Dear Tony:

Subject: Virginia Tech Contract # UCP-TS-C02-12
Commodity/Service: Email/Collaboration Services

This is to inform you that the subject contract expires on December 31, 2016. Since the university would like to renew the contract for an additional (1) one year, please advise concerning your intention by signing in the appropriate space listed below. A signed copy of this letter should be received in Information Technology Acquisitions no later than December 5, 2016.

In addition, review the attached form, which shows your company information as listed in the university’s vendor database. If any of this information has changed, make corrections directly on the form, and return with this letter. It is essential this information be accurate for payments to be processed in a timely manner.

Virginia Tech recommends that our vendors utilize the WellsOne AP Control Payment System for payment of all invoices and strongly encourages all vendors under contract with the university to participate in this program. If your firm is not enrolled in the program, refer to the Procurement Department’s website at: http://www.procurement.vt.edu/vendor/WellsOne.html or contact me directly for more information.

Sincerely,

Vicky Moore, CUPO, VCO
Senior Buyer
Telephone: (540) 231-7953

SADA Systems, Inc. agrees to renew the contract for an additional (1) one year under the terms and conditions of the subject contract.

Authorized Signature: Annie Safioian
Name: Annie Safioian
Title: CFO

We currently participate in the WellsOne Program.
We would like to participate in the WellsOne Program.

SADA Systems, Inc. does not agree to renew the contract for an additional (1) one year.

Authorized Signature: 
Name: 
Title: 

Approved: Patricia K. Branscome
Director of Information Technology Acquisitions
Date: 11/29/16

Invent the Future
### VENDOR INFORMATION FORM

--- for office use ---

**SADA Systems, Inc.**

<table>
<thead>
<tr>
<th>FULL LEGAL NAME</th>
<th>(Company Name as it appears with your Federal Taxpayer Number)</th>
</tr>
</thead>
<tbody>
<tr>
<td>95-4816919</td>
<td>FEDERAL TAXPAYER NUMBER</td>
</tr>
<tr>
<td>(Company name as it appears on your invoice)</td>
<td></td>
</tr>
</tbody>
</table>

**BUSINESS NAME/DBA NAME/TA NAME**

<table>
<thead>
<tr>
<th>FEDERAL TAXPAYER NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>(If different than ID# above)</td>
</tr>
</tbody>
</table>

**PURCHASE ORDER ADDRESS:**

5250 Vineland Avenue  
5250 Lankershim Blvd  
P O BOX ADDRESS 1  
Suite 620  
STREET ADDRESS 2  
North Hollywood  
CITY  
CA  
STATE  
91601  
ZIP CODE  
Tony Safoian, CEO  
CONTACT PERSON  
tony.safoian@sadasystems.com  
EMAIL

**PAYMENT ADDRESS:**

5250 Vineland Avenue  
5250 Lankershim Blvd  
PAYMENT P O BOX ADDRESS 1  
Suite 620  
PAYMENT STREET ADDRESS 2  
North Hollywood  
CITY  
CA  
STATE  
91601  
ZIP CODE  
818-766-2400  
PHONE NUMBER  
866-997-0000  
TOLL FREE NUMBER  
818-766-0090  
FAX NUMBER
Data Security Addendum for Inclusion in Contract #UCP-TS-C02-12 with Virginia Polytechnic Institute and State University ("Virginia Tech")

This Addendum supplements the above-referenced agreement between Virginia Tech and SADA Systems Inc. ("Selected Firm/Vendor") dated December 11, 201 and associated renewal Amendment #1 dated December 16, 2015 (the "Agreement"). It is applicable only in those situations where the Selected Firm/Vendor provides goods or services under a Purchase Order which necessitate that the Selected Firm/Vendor create, obtain, transmit, use, maintain, process, or dispose of University Data (as defined in the Definitions Section of this Addendum) in order to fulfill its obligations to Virginia Tech.

This Addendum sets forth the terms and conditions pursuant to which Virginia Tech Data will be protected by the Selected Firm/Vendor during the term of the Parties’ Agreement and after its termination.

1. Definitions
   a. "Brand Features" means the trade names, trademarks, service marks, logos, domain names, and other distinctive brand features of each party, respectively, as secured by such party from time to time.
   b. "End User" means the individuals authorized by the University to access and use the Services provided by the Selected Firm/Vendor under this Agreement.
   c. "Personally Identifiable Information" includes but is not limited to: personal identifiers such as name, address, phone number, date of birth, Social Security number, email address, student or personnel identification number, and non-directory information; "personal information" as defined in Virginia Code section 18.2-186.6 and/or any successor laws of the Commonwealth of Virginia; personally identifiable information contained in student education records as that term is defined in the Family Educational Rights and Privacy Act, 20 USC 1232g; "medical information" as defined in Virginia Code Section 32.1-127.1:05; "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers, access codes, driver’s license numbers; and state- or federal-identification numbers such as passport, visa or state identity card numbers.
   d. "Securely Destroy" means taking actions that render data written on media unrecoverable by both ordinary and extraordinary means. These actions must meet or exceed those sections of the National Institute of Standards and Technology (NIST) SP 800-88 guidelines relevant to data categorized as high security.
   e. "Security Breach" means a security-relevant event in which the security of a system or procedure used to create, obtain, transmit, maintain, use, process, store or dispose of data is breached, and in which University Data is exposed to unauthorized disclosure, access, alteration, or use.
   f. "Services" means any goods or services acquired by Virginia Tech from the Selected Firm/Vendor.
   g. "University Data" includes all Personally Identifiable Information and other information that is not intentionally made generally available by Virginia Tech on public websites, including but not limited to business, administrative and financial data, intellectual property, and patient, student and personnel data.
Rights and License in and to the University Data
The parties agree that as between them, all rights including all intellectual property rights in and to University Data shall remain the exclusive property of the University, and Selected Firm/Vendor has a limited, nonexclusive license to use these data as provided in this Agreement solely for the purpose of performing its obligations hereunder. This Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.

Intellectual Property Rights/Disclosure
a. Unless expressly agreed to the contrary in writing, all goods, products, materials, documents, reports, writings, video images, photographs or papers of any nature including software or computer images prepared or provided by Selected Firm/Vendor (or its subcontractors) for the University will not be disclosed to any other person or entity without the written permission of the University.
b. Selected Firm/Vendor warrants to the University that the University will own all rights, title and interest in any and all intellectual property rights created in the performance or otherwise arising from this Agreement and will have full ownership and beneficial use thereof, free and clear of claims of any nature by any third party including, without limitation, copyright or patent infringement claims. Selected Firm/Vendor agrees to assign and hereby assigns all rights, title, and interest in any and all intellectual property created in the performance or otherwise arising from this Agreement, and will execute any future assignments or other documents needed for the University to document, register, or otherwise perfect such rights.
c. Notwithstanding the foregoing, for research collaboration pursuant to subcontracts under sponsored research agreements administered by the University's Office of Sponsored Programs, intellectual property rights will be governed by the terms of the grant or contract to the University to the extent such grant or contract requires intellectual property terms to apply to subcontractors.

Data Privacy
a. Selected Firm/Vendor will use University Data only for the purpose of fulfilling its duties under this Agreement and will not share such data with or disclose it to any third party without the prior written consent of the University, except as required by this Agreement or as otherwise required by law.
b. University Data will not be stored outside the United States without prior written consent from the University.
c. Selected Firm/Vendor will provide access to University Data only to its employees and subcontractors who need to access the data to fulfill Selected Firm/Vendor obligations under this Agreement. Selected Firm/Vendor will ensure that employees who perform work under this Agreement have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of this Agreement. If Selected Firm/Vendor will have access to the University's "education records" as defined under the Family Educational Rights and Privacy Act (FERPA), the Selected Firm/Vendor acknowledges that for the purposes of this Agreement it will be designated as a "school official" with "legitimate educational interests" in the University education records, as those terms have been defined under FERPA and its implementing regulations, and the Selected Firm/Vendor agrees to abide by the limitations and requirements imposed on school officials. Selected Firm/Vendor will use the education records only for the purpose of fulfilling its duties under this Agreement for University's and its End User's benefit, and will not share such data with or disclose it to
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| 5 Data Security | a. Selected Firm/Vendor will store and process University Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Selected Firm/Vendor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, Selected Firm/Vendor warrants that all electronic University Data will be encrypted in transmission (including via web interface) and stored at no less than 128-bit level encryption.  

b. Selected Firm/Vendor will use industry-standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this Agreement. |
| 6 Employee Background Checks and Qualifications | a. Selected Firm/Vendor shall ensure that its employees have undergone appropriate background screening and possess all needed qualifications to comply with the terms of this agreement including but not limited to all terms relating to data and intellectual property protection.  
b. If the Selected Firm/Vendor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable information or financial or business data which has been identified to the Selected Firm/Vendor as having the potential to affect the accuracy of the University’s financial statements, Selected Firm/Vendor shall perform the following background checks on all employees who have potential to access such data in accordance with the Fair Credit Reporting Act: Social Security Number trace; seven (7) year felony and misdemeanor criminal records check of federal, state, or local records (as applicable) for job related crimes; Office of Foreign Assets Control List (OFAC) check; Bureau of Industry and Security List (BIS) check; and Office of Defense Trade Controls Debarred Persons List (DDTC). |
| 7 Data Authenticity and Integrity | Selected Firm/Vendor will take reasonable measures, including audit trails, to protect University Data against deterioration or degradation of data quality and authenticity. The selected Firm/Vendor shall be responsible for ensuring that University Data, per the Virginia Public Records Act, “is preserved, maintained, and accessible throughout their lifecycle, including converting and migrating electronic data as often as necessary so that information is not lost due to hardware, software, or media obsolescence or deterioration.” |
| 8 Security Breach | a. Response. Immediately upon becoming aware of a Security Breach, or of circumstances that could have resulted in unauthorized access to or disclosure of use of University Data, Selected Firm/Vendor will notify the University, fully investigate the incident, and cooperate fully with the University’s investigation of and response to the incident. Except as otherwise required by law, Selected Firm/Vendor will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the University.  
b. Liability. In addition to any other remedies available to the University under law or equity,
Selected Firm/Vendor will reimburse the University in full for all costs incurred by the University in investigation and remediation of such Security Breach, including but not limited to providing notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities as required by law or contract; providing one year’s credit monitoring to the affected individuals if the Personally Identifiable Information exposed during the breach could be used to commit financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Breach.

<table>
<thead>
<tr>
<th>9</th>
<th>Response to Legal Orders, Demands or Requests for Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Except as otherwise expressly prohibited by law, Selected Firm/Vendor will:</td>
</tr>
<tr>
<td></td>
<td>• immediately notify the University of any subpoenas, warrants, or other legal orders, demands or requests received by Selected Firm/Vendor seeking University Data;</td>
</tr>
<tr>
<td></td>
<td>• consult with the University regarding its response;</td>
</tr>
<tr>
<td></td>
<td>• cooperate with the University’s reasonable requests in connection with efforts by the University to intervene and quash or modify the legal order, demand or request; and</td>
</tr>
<tr>
<td></td>
<td>• upon the University’s request, provide the University with a copy of its response.</td>
</tr>
<tr>
<td>b.</td>
<td>If the University receives a subpoena, warrant, or other legal order, demand (including request pursuant to the Virginia Freedom of Information Act) or request seeking University Data maintained by Selected Firm/Vendor, the University will promptly provide a copy to Selected Firm/Vendor. Selected Firm/Vendor will promptly supply the University with copies of data required for the University to respond, and will cooperate with the University’s reasonable requests in connection with its response.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>10</th>
<th>Data Transfer Upon Termination or Expiration</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Upon termination or expiration of this Agreement, Selected Firm/Vendor will ensure that all University Data are securely returned or destroyed as directed by the University in its sole discretion. Transfer to the University or a third party designated by the University shall occur within a reasonable period of time, and without significant interruption in service. Selected Firm/Vendor shall ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of the University or its transferee, and to the extent technologically feasible, that the University will have reasonable access to University Data during the transition. In the event that the University requests destruction of its data, Selected Firm/Vendor agrees to Securely Destroy all data in its possession and in the possession of any subcontractors or agents to which the Selected Firm/Vendor might have transferred University data. The Selected Firm/Vendor agrees to provide documentation of data destruction to the University.</td>
</tr>
<tr>
<td>b.</td>
<td>Selected Firm/Vendor will notify the University of impending cessation of its business and any contingency plans. This includes immediate transfer of any previously escrowed assets and data and providing the University access to Selected Firm/Vendor’s facilities to remove and destroy University-owned assets and data. Selected Firm/Vendor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the University. Selected Firm/Vendor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the University. Selected Firm/Vendor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on the University, all such work to be coordinated and performed in advance of the formal, final transition date.</td>
</tr>
</tbody>
</table>
## Audits

a. The University reserves the right in its sole discretion to perform audits of Selected Firm/Vendor at the University’s expense to ensure compliance with the terms of this Agreement. The Selected Firm/Vendor shall reasonably cooperate in the performance of such audits. This provision applies to all agreements under which the Selected Firm/Vendor must create, obtain, transmit, use, maintain, process, or dispose of University Data.

b. If the Selected Firm/Vendor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information or financial or business data which has been identified to the Selected Firm/Vendor as having the potential to affect the accuracy of the University’s financial statements, Selected Firm/Vendor will at its expense conduct or have conducted at least annually:

- American Institute of CPAs Service Organization Controls (SOC) Type II audit, or other security audit with audit objectives deemed sufficient by the University, which attests the Selected Firm/Vendor’s security policies, procedures and controls;
- vulnerability scan, performed by a scanner approved by the University, of Selected Firm/Vendor’s electronic systems and facilities that are used in any way to deliver electronic services under this Agreement; and
- formal penetration test, performed by a process and qualified personnel approved by the University, of Selected Firm/Vendor’s electronic systems and facilities that are used in any way to deliver electronic services under this Agreement.

Additionally, the Selected Firm/Vendor will provide the University upon request the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations under this Agreement. The University may require, at University expense, the Selected Firm/Vendor to perform additional audits and tests, the results of which will be provided promptly to the University.

## Institutional Branding

Each party shall have the right to use the other party’s Brand Features only in connection with performing the functions provided in this Agreement. Any use of a party’s Brand Features will inure to the benefit of the party holding intellectual property rights in and to those features.

## Compliance

a. Selected Firm/Vendor will comply with all applicable laws and industry standards in performing services under this Agreement. Any Selected Firm/Vendor personnel visiting the University’s facilities will comply with all applicable University policies regarding access to, use of, and conduct within such facilities. The University will provide copies of such policies to Selected Firm/Vendor upon request.

b. Selected Firm/Vendor warrants that the service it will provide to the University is fully compliant with and will enable the University to be compliant with relevant requirements of all laws, regulation, and guidance applicable to the University and/or Selected Firm/Vendor, including but not limited to: the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Financial Modernization Act (GLB), Payment Card Industry Data Security Standards (PCI-DSS), Americans with Disabilities Act (ADA), and Federal Export Administration Regulations.
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| 14 | **Indemnity**  
Vendor shall indemnify, defend and hold Virginia Tech harmless from all claims, liabilities, damages, or judgments involving a third party, including Virginia Tech's costs and attorneys' fees, which arise as a result of Vendor's failure to meet any of its obligations under this Agreement. |
| 15 | **No End User Agreements**  
This Agreement is the entire agreement between the University (including University employees and other End Users) and the Selected Firm/Vendor. In the event that the Selected Firm/Vendor enters into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, with University employees or other End Users, such agreements shall be null, void and without effect, and the terms of this Agreement shall apply. |
| 16 | **Survival**  
The Selected Firm/Vendor's obligations under Section 10 shall survive termination of this agreement until all University Data has been returned or Securely Destroyed. |

IN WITNESS WHEREOF, this Addendum has been executed by an authorized representative of each party as of the date set forth beneath such party’s designated representative’s signature.

**SADA Systems Inc.**  
By:  
Title: CFO  
Date: 03/18/2016

**Virginia Tech**  
By:  
Title: Director, Information Technology Acquisitions  
Date: 3/18/16
COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT AMENDMENT

Contract Number: MCP-TS-C02-12
Amendment # 1

The above referenced contract is amended this 16th day of December, 2015 by SADA Systems Incorporated, hereinafter called the “Contractor” and the Commonwealth of Virginia, Virginia Polytechnic Institute and State University, hereinafter called “Virginia Tech”.

The parties hereby agree to extend the above referenced contract until December 31, 2016. This is the first of five optional one-year renewals.

All other terms and conditions remain in full force and effect.

The parties agree to execute this Contract Amendment by electronic means, via facsimile/scanned signatures.

By: Contractor Authorized Signature

By: Virginia Tech Authorized Signature

IN WITNESS WHEREOF, the parties have caused this Contract Amendment to be duly executed intending to be bound thereby.

Contractor:

Annie Safiian
Authorized Signature
Printed Name
CFO
Title

Virginia Tech

Patricia K. Branscome
Authorized Signature
Printed Name
Director – IT Acquisitions
Title

Invent the Future

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
An equal opportunity, affirmative action institution
COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract Number: UCP-TS-C02-12

This contract entered into this 15th day of December 2011 by SADA Systems Incorporated, hereinafter called “Contractor”, and the Commonwealth of Virginia, Virginia Polytechnic Institute and State University called “Virginia Tech”.

WITNESSETH that the Contractor and Virginia Tech, in consideration of the mutual covenants, promises, and agreements herein contained, agrees as follows:

SCOPE OF CONTRACT: The Contractor shall provide Email/Collaboration Services to Virginia Tech as set forth in the Contract Documents.


COMPENSATION AND METHOD OF PAYMENT: The Contractor shall be paid by Virginia Tech in accordance with the Contract Documents.

CONTRACT DOCUMENTS: The Contract Documents shall consist of:
- This signed Contract
- Attachment B – Proposal Submitted by Contractor for RFP 0016512 dated April 4, 2011
- Attachment C – Proposal Clarifications and Negotiations
- Attachment D – Agreements for Virginia Tech
- Attachment E – Agreement for Cooperative Use

All of which contract documents are incorporated herein.

The parties agree to execute this Contract by electronic means, via facsimile/scanned signatures.

By: ________________________________ By: ________________________________
Contractor Authorized Signature Virginia Tech Authorized Signature

In WITNESS WHEREOF, the parties have caused this Contract to be duly executed intending to be bound thereby.

Contractor:

By: ________________________________
Name: Tony Safion
Title: President, CEO

Virginia Tech:

By: ________________________________
Name: John D. Krallman
Title: Director of IT Business & Financial Affairs

Invent the Future

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
An equal opportunity, affirmative action institution
## Table of Contents for Contract Attachments

<table>
<thead>
<tr>
<th>Section</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contract</td>
<td>1</td>
</tr>
<tr>
<td>Attachment A – Request for Proposal (RFP) 0016512 dated March 3, 2011</td>
<td>3</td>
</tr>
<tr>
<td>Attachment B – Proposal Submitted by Contractor for RFP 0016512 dated April 4, 2011</td>
<td>34</td>
</tr>
<tr>
<td>Attachment C – Proposal Clarifications and Negotiations</td>
<td>120</td>
</tr>
<tr>
<td>Attachment D – Agreements for Virginia Tech Use: Master Professional Services Agreement, Maintenance and Support Agreement, Google Apps Customer Agreement</td>
<td>128</td>
</tr>
<tr>
<td>Attachment E – Agreements for Cooperative Use: Master Professional Services Agreement, Maintenance and Support Agreement, Google Apps Customer Agreement</td>
<td>153</td>
</tr>
</tbody>
</table>
Attachment A

Contract UCP-TS-C02-12

Request for Proposal # 0016512 dated March 3, 2011
Request for Proposal #0016512

for

E-mail/Collaboration Services

March 3, 2011
1. **QUESTIONS**: All inquiries for information regarding this solicitation should be directed to: Nancy Sterling, Phone: (540) 231-9517, e-mail: nancy.sterling@vt.edu. Questions will be received through March 28, 2011 at 3:00 PM.

   - **DUE DATE**: Sealed Proposals will be received until **April 4, 2011 at 3:00 PM**. Failure to submit proposals to the correct location by the designated date and hour will result in disqualification.

2. **ADDRESS**: Proposals should be mailed or hand delivered to: Virginia Polytechnic Institute and State University (Virginia Tech), Information Technology Acquisitions, 1700 Pratt Drive (0214), Blacksburg, Virginia 24061. Reference the Opening Date and Hour, and RFP Number in the lower left corner of the return envelope or package.

3. **PRE-PROPOSAL CONFERENCE**: See Section IX for information regarding a pre-proposal conference.

4. **TYPE OF BUSINESS**: (Please check all applicable classifications). If your classification is certified by the Virginia Department of Minority Business Enterprise, provide your certification number: _______________________________. For certification assistance, please visit: [http://www.dmbe.state.va.us/swamcert.html](http://www.dmbe.state.va.us/swamcert.html).

   - __X__ Large
   - __X__ Small business – An independently owned and operated business which, together with affiliates, has 250 or fewer employees or average annual gross receipts of $10 million or less averaged over the previous three years. Department of Minority Business Enterprise (DMBE) certified women-owned and minority-owned business shall also be considered small business when they have received DMBE small business certification.
   - __X__ Women-owned business – A business concern that is at least 51% owned by one or more women who are U. S. citizens or legal resident aliens, or in the case of a corporation, partnership, or limited liability company or other entity, at least 51% of the equity ownership interest is owned by one or more women who are citizens of the United States or non-citizens who are in full compliance with the United States immigration law, and both the management and daily business operations are controlled by one or more women who are U. S. citizens or legal resident aliens.
   - __X__ Minority-owned business – A business concern that is at least 51% owned by one or more minority individuals (see Section 2.2-1401, Code of Virginia) or in the case of a corporation, partnership, or limited liability company or other entity, at least 51% of the equity ownership interest in the corporation, partnership, or limited liability company or other entity is owned by one or more minority individuals and both the management and daily business operations are controlled by one or more minority individuals.

6. **COMPANY INFORMATION/SIGNATURE**: In compliance with this Request For Proposal and to all the conditions imposed therein and hereby incorporated by reference, the undersigned offers and agrees to furnish the goods and services in accordance with the attached signed proposal and as mutually agreed upon by subsequent negotiation.

<table>
<thead>
<tr>
<th>FULL LEGAL NAME (PRINT)</th>
<th>FEDERAL TAXPAYER NUMBER (ID#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SADA Systems, Inc.</td>
<td>95-4816919</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BUSINESS NAME/DBA NAME/TA NAME</th>
<th>FEDERAL TAXPAYER NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>(If different than the Full Legal Name)</td>
<td>(If different than ID# above)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BILLING NAME (Company name as it appears on your invoice)</th>
<th>FEDERAL TAXPAYER NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>SADA Systems, Inc.</td>
<td>(If different than ID# above)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PURCHASE ORDER ADDRESS</th>
<th>PAYMENT ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>5250 Lankershim Blvd. Suite 620</td>
<td>5250 Lankershim Blvd. Suite 620</td>
</tr>
<tr>
<td>North Hollywood, CA 91601</td>
<td>North Hollywood, CA 91601</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONTACT NAME/TITLE (PRINT)</th>
<th>SIGNATURE (IN INK)</th>
<th>DATE</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>E-MAIL ADDRESS</th>
<th>TELEPHONE NUMBER</th>
<th>TOLL FREE TELEPHONE NUMBER</th>
<th>FAX NUMBER TO RECEIVE E-PROCUREMENT ORDERS</th>
</tr>
</thead>
</table>

09/10
I. PURPOSE:

The purpose of this Request for Proposal (RFP) is to solicit sealed proposals to establish a contract through competitive negotiations for E-mail/Collaboration Services by Virginia Polytechnic Institute and State University (Virginia Tech), an agency of the Commonwealth of Virginia.

II. CONTRACT PERIOD:

The term of this contract is for three (3) years, or as negotiated. There will be an option for five (5) one-year renewals, or as negotiated.

III. BACKGROUND:

A. University Overview

Founded in 1872 as a land-grant college, Virginia Tech (www.vt.edu) is the most comprehensive university in the Commonwealth of Virginia and is among the top research universities in the nation. Virginia Tech’s nine colleges are dedicated to quality, innovation, and results through teaching, research, and outreach activities. At its 2,600 acre main campus located in Blacksburg and other campus centers in Northern Virginia, Southwest Virginia, Hampton Roads, Richmond, Southside, and Roanoke, Virginia Tech enrolls more than 28,000 undergraduate and graduate students from all 50 states and more than 100 countries in 180 academic degree programs.

Virginia Polytechnic Institute & State University operating as Virginia Tech (“Virginia Tech”) seeks proposals for comprehensive e-mail, calendaring, and collaboration services for their university employees and students. As detailed below, the requested services must be stable, secure, state of the art, feature rich, scalable, integrated, and available for installation, service, and maintenance on both a single institution and multi-institutional basis. Vendors shall specifically address all enumerated financial, administrative and technical requirements, but shall also discuss how their proposals might enable the collaborating institution to:

• **Increase efficiency through standardization.**
  Comment: Many of the services upon which Virginia Tech depends have standardized around architectures, operational practices, and core technologies. Nevertheless, the ongoing focus on department/campus level aggregation and provisioning produces fragmented environments with many customizations that add little value and also increase the costs of the service for each department/college. Through this RFP, we will explore aggregation/implementation above the level of the individual department/college, with the hope of leveraging standardization and benefitting operational efficiencies and the bottom line.

• **Increase interoperability and associated capacity for collaboration.**
  Comment: University researchers and scholars collaborate across global disciplinary communities as well as within their home institution. By aggregating demand and associated operations above the level of the individual department, or college, Virginia Tech seeks proposals that will enable a technical environment that is easier to navigate across the institution (e.g., sharing of institutional directories and shared capacities to create virtual collaboration groups and shared tools at an institutional level).

B. Current Campus IT Environments

Virginia Tech has a campus population in excess of 60,000 users, including faculty, students, staff, and affiliates. Typically Virginia Tech colleges and institution have heterogeneous computing environments and support the use of multiple Windows, Macintosh and Unix/Linux operating systems. (See VI.B.1.a)

C. Current E-mail Environments

Virginia Tech has approximately 100,000 e-mail users, including faculty, students, staff and affiliates. Most of these users use the central e-mail services (typically IMAP-based, but increasingly expanding to encompass Microsoft Exchange servers) provided by central IT, while others use services provided by their school or department (subunits of the institution). Shared access to e-mail folders is often used for delegating access and/or sharing data with individual users or groups of users (static and dynamic), or to facilitate group workflow. Centrally provided e-mail services are tightly integrated with campus directory (typically LDAP and AD) and authentication systems (typically LDAP, CAS, Shibboleth and/or AD). Existing quotas provided by the Virginia Tech range from 200 MB to 2 GB, or
are effectively unlimited, but with a 30 day retention period. Users access their e-mail through either a web interface or a native client application. (See VI.B.2.a) The Mac and Windows clients typically support synchronization with various handheld devices. (See VI.B.4.a)

D. **Current Calendar Environments**

Virginia Tech has approximately 6,000 calendar users, including faculty, students, staff and affiliates. Most of these users use the central calendar services provided by central IT within the institution (typically Microsoft Exchange), while others use services provided by their school or department (subunits of the institution). Shared access to calendar data is very important for many campus users, including the ability to delegate access and/or share data with individual users or groups of users (static and dynamic). Users access their calendar through either a web interface or a native client application. (See VI.B.2.a) The Mac and Windows clients typically support synchronization with various handheld devices. (See VI.B.4.a)

IV. **EVA BUSINESS-TO-GOVERNMENT ELECTRONIC PROCUREMENT SYSTEM**

The eVA Internet electronic procurement solution streamlines and automates government purchasing activities within the Commonwealth of Virginia. Virginia Tech, and other state agencies and institutions, have been directed by the Governor to maximize the use of this system in the procurement of goods and services. We are, therefore, requesting that your firm register as a trading partner within the eVA system.

There are registration fees and transaction fees involved with the use of eVA. These fees must be considered in the provision of quotes, bids and price proposals offered to Virginia Tech. Failure to register within the eVA system may result in the quote, bid or proposal from your firm being rejected and the award made to another vendor who is registered in the eVA system.

Registration in the eVA system is accomplished on-line. Your firm must provide the necessary information. Please visit the eVA website portal at [http://www.eva.virginia.gov/register/vendorreg.htm](http://www.eva.virginia.gov/register/vendorreg.htm) and register both with eVA and Ariba. This process needs to be completed before Virginia Tech can issue your firm a Purchase Order or contract. If your firm conducts business from multiple geographic locations, please register these locations in your initial registration.

For registration and technical assistance, reference the eVA website at: [eVACustomerCare@dgs.virginia.gov](mailto:eVACustomerCare@dgs.virginia.gov), or call 866-289-7367 or 804-371-2525.

V. **CONTRACT PARTICIPATION**

It is the intent of this solicitation and resulting contract to allow for cooperative procurement. Accordingly, any public body, public or private health or educational institutions, or Virginia Tech’s affiliated corporations and/or partnerships may access any resulting contract if authorized by the contractor.

Participation in this cooperative procurement is strictly voluntary. If authorized by the Contractor, the resultant contract may be extended to the entities indicated above to purchase at contract prices in accordance with contract terms. The Contractor shall notify Virginia Tech in writing of any such entities accessing the contract. No modification of this contract or execution of a separate contract is required to participate. The Contractor will provide semi-annual usage reports for all entities accessing the Contract. Participating entities shall place their own orders directly with the Contractor and shall fully and independently administer their use of the contract to include contractual disputes, invoicing and payments without direct administration from Virginia Tech. Virginia Tech shall not be held liable for any costs or damages incurred by any other participating entity as a result of any authorization by the Contractor to extend the contract. It is understood and agreed that Virginia Tech is not responsible for the acts or omissions of any entity, and will not be considered in default of the contract no matter the circumstances.
VI. STATEMENT OF NEEDS:

A. General Services Sought

Virginia Tech seeks a new central e-mail and calendaring solution for their students, faculty and staff. Such solution must achieve the standard of 99.99% availability for all centrally supported services, while providing a rich set of features across a wide range of client platforms, delivering: increased scalability, reliability, availability, and recoverability of e-mail and Calendaring Services. In brief, the successful vendor should provide:

- Integration with Virginia Tech’s existing directory, authentication and authorization systems, and with other campus messaging, scheduling and communications systems;
- Continued implementation and support for standard open protocols;
- Expanded opportunities for collaborative and unified messaging and communications;
- Increased User productivity through integrated scheduling and communications tools;
- A leveraged, long-lasting relationship between Vendor and Virginia Tech.

This RFP is intended to secure all labor, software, and services for proper deployment of this solution. Proposals shall identify all costs, enabling Virginia Tech to accurately assess its expenses. All proposals must be in accordance with the specifications and information contained herein, as well as any addenda. If the Vendor finds any of the system specifications or engineering assumptions outlined in this document in error or unwise, Vendor shall present a persuasive case to the contrary. Installation and Technical Assistance Support for all components are to come directly from Vendor unless otherwise specified by this RFP.

All components specified in any response to this RFP are assumed to have General Availability (GA) status. If any component does not have GA status, Vendor shall so state and clearly identify when and under what condition GA status will be reached. Unless otherwise specified, no Manufacturer Discontinued (MD) products will be considered.

All services provided as part of this RFP must be maintainable by the Vendor under contract. Additionally, Vendor is responsible for specifying and providing service support and upgrades for term of the contract.

B. Specific Technical Requirements

1. Supported Operating Systems

The following platforms and versions are widely utilized on the campus and as a minimum MUST be supported by the proposed solution:
   a) Windows XP, Vista, and 7; Mac OSX; and Linux, particularly Debian, Fedora, and Ubuntu.

2. Supported Native and Web Clients

The following clients and versions are widely utilized on the campus and as a minimum MUST be supported by the proposed solution:
   a) Eudora, Outlook/Outlook Express, Apple e-mail, Entourage, Gnome Evolution, Thunderbird.

3. Supported Web Browsers

User and administration web interfaces MUST be usable via the web browsers commonly used on campus, including as a minimum: Mozilla Foundation Firefox on Microsoft Windows (XP, Vista, and 7), Apple Mac OS X (10.3, 10.4, 10.5 and 10.6), and Linux and Unix clients, Microsoft Internet Explorer 6 and Internet Explorer 7 on Microsoft Windows (XP, Vista and 7), Apple Safari on Apple Mac OS X (10.3, 10.4, 10.5, 10.6), and Google Chrome. Vendor MUST provide support for new OS and Browser versions within 30 days of general availability to the public.

4. Supported Mobile Devices
The proposed solution MUST support a variety of operating systems: RIM Blackberry, Apple iPhone, Microsoft Windows Mobile, Palm WebOS, Android.

a) The proposed solution SHOULD also support IETF and OMA standards-compliant devices as e-mail and calendar clients. Appropriate push and/or pull synchronization, via a desktop client conduit or “over the air” of e-mail, calendar, contact and to-do data MUST be available for mobile devices.

5. Supported Protocols

The solution MUST comply with the following standards. In the case of IETF RFCs, “comply” means that the solution adheres to all requirements declared “MUST”, “REQUIRED”, “SHALL”, “MUST NOT” or “SHALL NOT”. Please note where the solution also complies with RFC requirements declared “SHOULD”, “RECOMMENDED”, “SHOULD NOT”, “NOT RECOMMENDED”.

a) IETF RFC 2426 - vCard MIME Directory Profile
b) IETF RFC 2445 - Internet Calendaring and Scheduling Core Object Specification
c) IETF RFC 2446 - iCalendar Transport-Independent Interoperability Protocol (iTIP) Scheduling Events, Busy Time, To-dos and Journal Entries
d) IETF RFC 2447 - iCalendar Message-Based Interoperability Protocol (iMIP)
e) IETF RFC 4791 - CalDAV support an extension to the HTTP and WebDAV protocols to enable interoperable distributed calendaring and scheduling
f) IETF RFC 2821 - Simple E-mail Transport Protocol
g) IETF RFC 2822 - Internet Message Format
h) IETF RFC 3207 - SMTP Service Extension for Secure SMTP over Transport Layer Security
i) IETF RFC 3501 - Internet Message Access Protocol - Version 4rev1
k) IETF RFC 4752 - The Kerberos V5 ("GSSAPI") Simple Authentication and Security Layer (SASL) Mechanism Internet E-mail Consortium, "vCard - The Electronic Business Card Version 2.1", OMA SyncML ADA Setion 508

6. Provisioning/Deprovisioning

Solution MUST provide an Application Programming Interface (API) allowing Virginia Tech to provision, deprovision, rename, suspend, unsuspend and adjust settings of individual User accounts

7. Support for Emergency Notification E-mailings

In the event of an emergency, the system SHOULD permit the broadcasting of e-mail by authorized Users to an entire campus population or to select subgroups. Appropriate infrastructure SHOULD be provided as part of the proposed solution to ensure that that messages sent as part of a designated Emergency Notification are guaranteed to be received in individual User e-mailboxes within five (5) minutes of transmission. A simple interface SHOULD provide authorized Users the option to select Emergency Notification recipients from among a series of pre-defined groupings (or dynamically provisioned groups based on LDAP characteristics). Proof of receipt or logs documenting transmission to each recipient SHOULD be provided for each Emergency Notification e-mailing.

8. Data Center Location

Virginia Tech data stored by the solution SHOULD be maintained in data centers situated in the continental United States, Alaska, or Hawaii.

9. E-discovery and Data Preservation

Solution SHOULD provide an Application Programming Interface (API) allowing Virginia Tech to search, access, and download individual User E-mail data without requiring the knowledge of, or changing, the User password.

10. Collaboration

a) Solution SHOULD provide ability to share data and files stored within the solution;
b) Solution SHOULD provide ability to have multiple Users work on common files at the same time from different or separate work groups or locations;
c) Solution SHOULD provide ability to collaborate with Users that are telecommuting or otherwise away from campus;
d) Solution SHOULD provide a Wiki-type solution for collaboration that allows changes to be tracked by User; and
e) Solution SHOULD provide ability to maintain version control (i.e., who, what, when).

11. Instant Messaging

a) Solution SHOULD have the capability to provide instant messaging capabilities for internal Users and with external (non-campus) Users.

12. Video Conferencing

a) Solution SHOULD provide ability to support one-to-one internal videoconferences;
b) Solution SHOULD provide ability to support external video conferencing participants;
c) Solution MAY provide ability to support multiple locations internally;
d) Solution MAY provide ability to use saved video files within office productivity tools;
e) Solution MAY provide a Real-time on-screen notation
f) Solution MAY provide a Remote Desktop Access/Control within video conferencing solution

C. Technical Discovery

1. Data Stewardship

Many individuals at Virginia Tech have been early adopters of cloud-based (often free) solutions to e-mail, calendaring, and collaboration tools. However, license terms associated with those cloud-based solutions do not necessarily address the complex issues of data stewardship as they relate to students, and especially to faculty and staff (e.g., issues of ownership and use of Customer and End User data, system and data security, and e-Discovery, to name a few).

a) Please describe the measures your organization and personnel will take to ensure that all data - message headers, contents, calendar events, contacts, logs and any personally identifiable information - received, stored, sent or tracked by or for Users of Virginia Tech remains the property of contracting institution and/or their Users. Please provide a copy of all related policies and procedures.

b) System Security and Data Protection. Please describe the measures your organization and personnel will take to ensure that all activities under this Agreement are performed in a sufficiently secure manner to protect against reasonably anticipated threats or hazards to the privacy, security, and integrity of Customer and End User Data, and to prevent unauthorized access to or use or alteration of those data. In particular:
   (1) What is your operating system and application vulnerability testing and patching methodology and frequency to ensure the system, application, and associated tools/protocols/utilities are kept up to date with all relevant security patches?
   (2) Do the servers employ a network- and/or host-based intrusion prevention system, and if so provide details? Describe all other network- and host-based firewalls, security appliances, and/or similar defenses in place to help ensure Customer data confidentiality and integrity, as well as availability of the services provided to the Customer under this Agreement.
   (3) Do the servers use clear-text passwords for any reason? (E.g., including SMTP authentication or remote login)
   (4) Do the servers run any network services that are unrelated to and unnecessary for delivery of the services provided to the Customer under this Agreement? (If so, please specify.)
   (5) Will data be encrypted during transmission between the server(s) and the web interface and/or native clients (see Section VI.B.)? Will data be encrypted at rest on the server? (In each case, specify encryption mechanisms and bit lengths)
   (6) Do your physical security controls include video monitoring, restricted access areas, mantraps, card access controls, or similar controls?
   (7) Do you conduct regular internal security tests and/or audits (including vulnerability scanning, application security assessment scanning, and penetration testing) conducted by personnel or
c) Data Retention. Describe how your solution will ensure retention of data or records in an End User’s account, including attachments, until the End User deletes them or for an alternative time period mutually agreed by the parties. Specifically:

(1) Describe your plan for backup and restoration of system data, including standard backup retention periods, multiple copies of data, and procedures for processing data for long-term archiving. Please describe how individual Users and administrators will be able to easily restore individual e-mailboxes from your backups.

(2) Is archiving configurable both on a per User and per group basis? Can data be archived based on content, sender, recipient, and/or other metadata with different archival periods per institutional policy or legal requirements? Can e-mail administrators view and perform all normal e-mail functions on archived e-mail without having to restore?

(3) Describe your method of securely destroying all deleted data and/or expired backups at the end of that time period and at Customer’s election.

(4) Describe your procedures for responding to Customer’s e-discovery needs and responsibilities, including where customer indicates that certain records may be relevant to litigation that Customer reasonably anticipates; describe your capability to place an immediate “hold” on the destruction of Customer or End User records that might otherwise occur under routine records destruction schedules. Discuss whether e-mail administrators will be able to retrieve or view archived e-Discovery data based on content, sender, recipient, and/or other metadata with different archival periods? Describe the formats in which e-mail administrators can export archived e-Discovery data. (See Special Term 27d)

(5) Can the proposed solution be implemented such that all storage of Customer and End User data remain within the United States? If not, where will Vendor store data and what security measures does Vendor have in place in those locations?

2. System Logging and Data Integrity

Please describe the measures your organization and personnel will take to ensure that you retain, and can provide to Customer on request, logs necessary for the investigation of security incidents and/or to address data integrity concerns, including describing:

a) Your data retention policy for authentication and other relevant system logs; what is the process and lead-time for providing access in response to a request by Customer’s authorized infrastructure and security personnel? (E.g., authentication logs maintained for 90 days and accessible with 24 hours upon valid request from Customer’s identified/authorized system administrator or security personnel.) (See Special Term 27c)

b) The requirements necessary to implement logging and monitoring on the system and how does the system log security/authorization changes as well as User and administrator security events (e.g., login failures, access denied, changes accepted)?

c) Whether the services generate or support an audit trail for each User and type of usage? Do available audit logs include login, logout, action performed and source IP address?

d) The system capability to log security/authorization changes as well as User and administrator security events (e.g., login failures, access denied, changes accepted), and all requirements necessary to implement logging and monitoring on the system.

e) How your solution protects Customer and End User Data against deterioration or degradation of data quality and authenticity? Do you perform regular data integrity audits, and if so, with what frequency?

3. Data Security and Breach Notification

Please describe the measures the organization and personnel take to mitigate risk and/or notify Users of data exposure, including describing:

a) How the organization and its personnel ensure the prompt discovery and response to publicly known software bugs or other security threats that may expose Customer and End User Data to risk of unauthorized access, alteration, or use.

b) All security breaches involving Customer and End User Data that you have experienced within the last 2 years, and your response including what steps you have taken to minimize the likelihood of recurrence.
c) The process whereby Customer is notified in the event of any security breaches or exposure of End User Data, and the process Vendor will utilize to inform to such End Users of said breach. (See Special Term 26a)

d) The facilities available in the system to provide separation of duties between security administration and system administration functions.

4. User Privacy and Confidentiality

Much of our data – including student information databases and much faculty and staff e-mail – constitutes "education records" for purposes of the Family Educational Rights and Privacy Act (FERPA) and therefore may be outsourced only to vendors that we have designated, and that are willing to accept designation, as "school officials" with "legitimate educational interests" in the data. In order to do that, we must ensure both that our definitions of those two terms in our FERPA annual notices are broad enough to cover outsourcing, and that the vendor will not use the data for any purpose other than providing the outsourced service (such as data mining for the vendor's own benefit) or re-disclose it to others without appropriate authorization. (See Special Terms 22 and 23)

a) Please describe the measures your organization and personnel will take to ensure that:

(1) Customer and End User Data are only accessed and used for the purpose of performing the activities that are the subject of this RFP, and will not be used for other purposes including targeted marketing purposes building an index of metadata, etc;

(2) Customer and End User Data are only accessed and used by those personnel within your organization, or approved subcontractors, who require access to perform activities that are the subject of this RFP;

(3) Customer and End User Data will not be disclosed to or shared with any third party except as required by state or federal law or a valid court order (and, when required in such cases under the Family Educational Rights and Privacy Act or other applicable law, with prior notice to the person or persons affected), or with prior written consent from Customer or, where applicable, the individual(s) whose personal records would be disclosed; and

(4) Your personnel and approved subcontractors understand, accept, and have received appropriate instruction regarding their obligations to handle Customer and End User Data with the proper security as described above, and all such personnel and subcontractors will have read, understood, accepted, and received appropriate instruction as to how to comply with, the data protection provisions reflected in this RFP and the ultimate agreement between your organization and Customer.

b) Please describe your familiarity with and understanding of the data privacy and security requirements of the following laws that may apply to Customer and End User Data: Health Insurance Portability and Accountability Act (HIPAA); Family Educational Rights and Privacy Act (FERPA); Financial Modernization Act of 199 (Gramm-Leach-Bliley); PCI-DSS, and/or any state data protection or breach notification requirements that you consider applicable. Describe how the proposed system tools and attributes can be used to comply with the requirements of these laws and regulations.

c) Please describe your procedures for responding to subpoenas for End User information within your solution. How will you notify the Customer of subpoena or other legal requests related to End User data, before complying with the request? How will you cooperate with Customer in the event Customer elects to contest certain requests for confidential End User data?

d) Please provide a copy of all policies and procedures within your organization that relate to the measures described in Section VI.C.4.b.

e) Please provide the name(s) and contact information for the person(s) responsible in your organization for electronic and paper records security.

D. Integration and Operational Issues

SaaS and cloud computing solutions provide great promise to the future of campus IT infrastructures, but they must be fully integrated with institutional identity management and directory systems, and should only be pursued with a clear understanding of the entry and exit conditions, including essential matters such as how the Customer and End User data will be provided (migrated) at the conclusion of the license term, if the vendor ceases to support the services, or when new technologies become available.

1. Service Entry Plan/Migration Strategy

Provide a high-level entry plan which provides for the successful and uninterrupted transfer to vendor of services under various migration scenarios. Include a timeline and estimated milestones for each scenario:
Implement a 1,000 User pilot solution and migrate all live and historical data (archive and backup) from Oracle OCUCS and MS Exchange 2007 system(s) migrated by June 2011.

b) Implement the entire solution and migrate all live and historical data (archive and backup) from Oracle OCUCS and MS Exchange 2007 system(s) migrated by August 2011.

c) Implement the entire solution without migrating historical data from existing e-mail.

2. Integration with Directory, Identity Management and Authentication Services

Provide your implementation plan for integration with institutional identity & access management. Specifically address the fact that Virginia Tech wants to maintain its directory (LDAP & AD) and authentication (CAS, Shibboleth, AD, LDAP) services, and seeks to avoid separate account provisioning and authentication/authorization requirements. Based on this assumption:

a) How will you integrate with an existing [OpenLDAP, Microsoft AD] directory service?

b) How will you integrate with an existing [CAS 3.0, Shibboleth (Saml 2.0), OpenLDAP, Microsoft AD] authentication system?

c) For web components, how will you integrate with an existing [Internet2 Shibboleth Web Single Sign-On, CAS WebAuth, OpenLDAP] authentication system?

d) Can you enforce password/passphrase aging requirements? Can you enforce password/passphrase complexity requirements? (If so, can you enforce such requirements differentially within the population based on LDAP attributes, e.g., students vs. faculty vs. clinical workers?).

3. Integration with Account Provisioning and Management Systems

Will your solution allow the system administrator(s) to set up Users and groups that are protected from one another, including enabling segregated management of groups by different administrators either intra-institutionally or inter-institutionally? What programmatic interface(s) are provided to university system administrators to enable automated creation, locking, unlocking, and deletion of accounts, and management of quotas, group membership, etc?

4. Integration with Other Systems or Applications

a) Does your solution support open standards based interoperability with content and document management systems, unified messaging systems (voice e-mail, instant messaging, VoIP, etc), emergency notification systems, and collaboration tools (wikis, blogs, etc)? Please specify which open standards are supported and specify whether the associated interoperability is included in the solution, or by other products separately available from the vendor.

b) Does your solution support standards-based programmatic interfaces for integrating with other scheduling products used on campus? Please specify which open standards are supported and specify whether the associated interoperability is included in the solution, or by other products separately available from the vendor.

c) Can your solution provide standards-based programmatic interfaces for integrating with Sakai, the open source enterprise teaching, learning and academic collaboration platform (see http://sakaiproject.org/)? Describe the level of integration your product has or can have with Sakai.

5. Service Termination Plan/Exit Strategy

In the event of a termination for whatever reason, how will you provide for the successful and uninterrupted transfer of each of the services and associated data (i.e. e-mail messages, calendar entries, address book contacts, documents, etc) from the vendor service to Virginia Tech or a third party provider designated by Virginia Tech? This exit strategy should address capacity planning, process planning, facilities planning, human resources planning, telecommunications planning, and migration schedules. In the event of a migration to a different solution, within 90 days of receiving written notification from Customer of successful migration, the vendor must ensure the destruction of all of Virginia Tech’s data utilizing US Department of Defense-compliant disk sanitation techniques. (See Special Term 28)

E. Functionalities

Basic e-mail functionality is now well understood and interoperability between servers and clients has become commonplace. Likewise, calendar functionality is becoming more standards based. Beyond the basic functionalities, Virginia Tech makes heavy use of certain features for workflow or delegation that are essential to any transition to
SaaS or cloud solutions. Other supplemental component functionality is desired beyond the primary target applications described in the body of this RFP and is detailed in VI.B.10-12

1. Interfaces and Platform Support

Virginia Tech has a diverse client environment including Windows, Macintosh and Unix/Linux operating systems.

a) Does the proposed solution support multiple client platforms (e.g., Windows XP and Vista, Mac OS X and Linux), native e-mail clients (e.g. Eudora, Outlook/Outlook Express, Apple e-mail (Mac Mail), Entourage, Gnome Evolution) and web-based clients (e.g., Thunderbird)? Specifically, does it support the operating systems and platforms detailed in VI.B.1.a and 2.a?

b) Describe how the proposed solution will provide a secure, robust, common web interface for accessing all components of the solution (e-mail, calendar, address book, task list, etc) from a variety of browsers, as detailed in VI.B.3. Will the web e-mail client allow Users to choose between at least plain text and HTML e-mail formats (indicate any other formats supported)? Specify any other formats supported, and describe whether the User is able to choose a default format, and override the default on a per-message basis.

c) Describe how you will support access from and synchronization with common mobile devices for all components of the solution (e-mail, calendar, address book, task list, etc), including but not limited to the devices detailed in VI.B.4. Can you offer a simplified web interface available for use with mobile devices not supported directly?

d) How will you handle interface issues, particularly in relation to compliance responsibilities (ADA section 508 and WC3 standards), presentation, and access to your system?

e) Will your system afford options for individualized institutional branding?

f) What aspects of the display will be User-customizable, including display as format (coloring, font styles, etc.) of calendar events, e-mail messages, contacts and tasks based on categorization, sender, recipient, etc.?

g) Can you offer campus and inter-institutional operability between native clients (e.g. Eudora, Outlook, Apple E-mail), such that features like calendar free/busy time and shared e-mail folders can be accessible among institutions? What is your end-User support model?

2. Specific Component Functionality

Provide details on how the proposed solution meets the following criteria:

a) E-mail. Describe how your product offers the following basic e-mail functionality:

1. Ability to send, receive, format and forward messages and attachments
2. Ability for Users to define and manage e-mail filter rules that run on the server to automatically delete, redirect or file messages into folders.
3. Ability to manage folders and copy, move, and store information to desktop or local storage.
4. Ability for Users to have two or more e-mail aliases in addition to their primary university provided ID, and to send e-mail from group accounts.
5. Ability for Users to restore deleted e-mail messages and folders directly and without intervention from the system administrator.
6. Other features you wish to highlight.

b) Personal Calendars and Task Lists. Provide details on how the proposed solution meets the following criteria:

1. Basic calendaring functionality, including but not limited to inviting Users, groups and resources to events. Users should be able to see the free/busy times for all invitees, including all the members of pre-existing and ad hoc groups (unless restricted by access controls). The system should be able to automatically schedule meetings, support a variety of types of recurring events, and permit the viewing or hiding of appointment details.
2. The calendar client(s) should provide daily, weekly and monthly views, and allow scrolling through and printing of calendars by day, week and month and the ability to view multiple calendars at the same time (both personal and global).
3. Ability to print calendar events such that all relevant information, including meeting location, conference call numbers, document links, etc. are included.
4. Ability to schedule resources, including but not limited to facilities, conference rooms, equipment and virtual venues (IM chat rooms, conference call bridges, etc); ability to support access controls for each type by Users or groups.
5. Ability to support task lists at multiple priority levels.

c) Address Book/Contact Management. Provide details on how the proposed solution meets the following criteria:
Basic contact management functionality, including but not limited to last name, first name, middle initial, department, title, phone number, fax number, e-mailing address, e-mail address, business address, contact log, notes, etc.

(2) Ability to synchronize contact information with desktop applications;

(3) Ability to share contact lists with other Users or groups.

3. Overall Solution Functionality and Interoperability

Provide details on how proposed solution meets the following criteria:

a) Delegation, Shared Use and Workflow. The system should provide a facility to delegate administration of User and group e-mailboxes, calendars, quotas, etc. to departmental administrators.

(1) Describe how the system supports the creation and management of shared e-mailboxes, calendars, address books, and task lists with multiple owners and access control lists that can include User’s ad hoc groups.

(2) Describe how the system supports the ability to delegate e-mail, calendar, tasks, and other functionality to another staff member (i.e., proxy assignments, including e-mail/phone, appointments, resources, reminder notes, tasks, etc.)

(3) Describe how the system supports the ability for User-controlled setting of proxy access limitations (e.g., Read/Write; Subscribe to Alarms and Appointments, Modify Options, Rules, and Folders).

(4) Describe how the system either supports multiple calendars, address books and task lists per User, or allows Users to categorize calendar events, contacts and tasks. In either case, the proposed solution should support sharing of these objects, with User configurable access controls.

b) Personal, Group and Global Address Books. Personal and group address books should all be available within the e-mail and calendaring functions to any authorized Users. A common global address book, bound to the university’s existing directory services, should also be available to all Users and accessible within the e-mail and calendar functions. Additionally, please describe whether your solution would enable Virginia Tech to share global address books inter-institutionally. Any clients delivered with the solution should provide auto-completion for common address book lookup fields, such as names and addresses.

c) Categorization/Tagging. A User should be able to apply multiple customizable categories or tags to e-mail messages, address book entries, and calendar events and tasks.

d) Searching and Sorting. Provide details on how the proposed solution meets the following criteria:

(1) The ability for Users to search messages, calendars and address books, either all at once or by selecting specific e-mail folders, calendars or address books.

(2) The ability for Users to specify multiple search criteria, including searching for resources using the metadata.

(3) The ability within the web e-mail interface for Users to sort folders by various criteria (sender, subject, date, etc.), and should support displaying messages in threads.

(4) The use of indexing or related technologies to accelerate e-mailbox and calendar searches.

4. Anti-spam, Virus Protection and Open Relays

Provide details on how the proposed solution meets the following criteria:

a) How will you enable filtering of incoming and outgoing e-mail through an anti-virus scanner capable of completely quarantining infected messages? Describe in detail the quarantine response employed by your solution (e.g., “messages flagged as suspicious are placed in a quarantine area for up to 14 days; daily or weekly e-mail notifications are sent to the User; and the User connects to a Web-based administration site to delete or release a message.) Are the scanner’s virus signatures updated at least daily? Does the solution allow the university to additionally route incoming messages through its own server, if desired, for additional filtering? Are the scanner’s virus signatures updated at least daily?

b) Provide details about what products you will use for spam filtering and give a detailed spam filtering options (e.g., “messages flagged as suspicious are, at the Users option, either deleted or placed into a separate folder for up to 14 days; and the User can set the sensitivity for spam rankings via settings in the LDAP directory.) Will the proposed solution work with the university’s existing anti-spam e-mail gateways (Mirapoint Junkmail Manager) and filter messages marked as spam by the university gateway into separate folders? How do you ensure that spam definitions are kept up to date?

c) Does the proposed solution allow administrators to define global filters that can be applied to all incoming or outgoing messages for all Users?

d) Does the proposed solution support white-lists, blacklists, and auto-deletion, controlled at the individual Users level and at the local system administrator level?
e) Does the proposed solution restrict open relaying, including multilevel relaying (i.e., it must not accept or deliver e-mail for non-local addresses, and must not accept non-local e-mail from another system which accepts e-mail from non-local clients)?

5. Protocols and Standards

Please list all e-mail protocols supported, including but not limited to IETF E-mail standards (RFC2821 - SMTP, RFC2822 – Internet Message Format, RFC4511 - LDAP). We seek standards-based solutions; therefore, please provide technical details identifying which protocols you can support and how, including those identified in VI.B.5 and any others relevant standards or protocols.

F. Service Levels

Institutional e-mail and calendar systems are expected to have high availability. In certain cases, faculty are also clinicians and service levels have direct bearing on clinical care capabilities. During campus emergencies rapid dissemination of e-mail is critical to campus safety plans. (See VI.B.7). Other core business functions are significantly impacted during e-mail and calendar outages.

1. Performance and Availability

What is your basic service model? If you believe you can offer better than industry-standard services, describe why and how.

a) The proposed solution should deliver individual e-mail within 7 days of contract signing.

b) What has been your system availability and how do you measure it (e.g., 99.9%, 99.99%, 99.999%, 99.995%) for all Users over the past three years (or the duration of its existence, if less than 3 years)? What would be the functional and financial effect of increasing or decreasing the system guarantee/reliability by "one 9" or "half a 9" of reliability, relative to the actual measured three year availability? (E.g., increasing from an actual measured performance of 99.9% to 99.95% or 99.99%; decreasing from an actual measured performance of 99.99% to 99.9% or 99.95%). Please provide uptimes for your system on a month-by-month basis over the past 12 months. What fault tolerance, failover or other measures do you offer that provide continuity and redundancy to ensure availability of services?

c) The proposed solution must support the peak User load 20,000 simultaneous sessions with no noticeable delay of any operation.

d) Describe your proposed incident response procedures, addressing specifically how you will manage unscheduled outages, interrupted services, or a customer's report of degradation in service. Include specifics as to how you will investigate and resolve service level interruptions.

e) Please describe the way in which feature enhancements are released to your product (e.g., separate beta testing vs. en-masse beta testing with the entire population). How will the Customer and End Users be notified of upcoming or released product features?

f) In the event of an unscheduled outage, please describe your process of informing Customer and End Users of root cause and preventative steps to avoid reoccurrence of similar outages.

g) Please list the primary metrics available for the e-mail and calendar applications.

h) Describe your maintenance plan for both hardware and software in non-emergency situations. How will you ensure minimal interference with our services? Will you coordinate all regular maintenance with customer scheduling and needs, including consideration of individual institution's academic calendar? If a delay is requested by a customer, are you prepared to advise us regarding the effect of any such delay will have on the services, services levels, and/or fees?

i) Please describe your change control procedures and how the Customer and End Users receive prior notification of scheduled downtime for maintenance or upgrades.

j) The proposed solution must support Virginia Tech’s emergency broadcast system as detailed in VI.B.7. Please provide specific information regarding your latencies, basic confirmations, and the SLA standards you can commit to in this area.

k) Please share your annual testing plan for Disaster Recovery and/or business continuity.

2. Storage, individual e-mail quotas, and scalability

What range of capacity can you deliver and at what cost? Specify costs if capacity were set at 2GB, 10GB, or at 25GB. Describe how your proposed solution will support archiving old inactive messages to a lower cost message store. Archiving should be configurable per User and group.
3. User Support Services

Describe in detail your end-User support services, including but not limited to,

a) telephone support;

b) online support;

c) campus training;

d) availability (e.g., 24-hour technical phone contact); and

e) when and how the campus Help Desk can escalate to you.

4. Documentation

Within one week of contract award, the Vendor shall supply Virginia Tech with complete documentation, service manuals, and appropriate system engineering bulletins for all components proposed in the response to this RFP, both hardware and software. Documentation must be received in machine readable form (e.g., on Compact Discs) and appropriate for loading on university-owned servers.

5. Training

Vendor should include online training materials, training for three (3) e-mail and calendar administrators, and “train the trainer” training for three (3) training professionals from Virginia Tech. If this training is offered as separate, off-site courses, Vendor should include course descriptions and schedule of offered courses thru 12/2011.

VII. PROPOSAL PREPARATION AND SUBMISSION:

A. General Requirements

1. RFP Response: In order to be considered for selection, Offerors must submit a complete response to this RFP. One (1) original, eight (8) copies and one (1) electronic media copy in generally used formats on CD, DVD, or USB Flash Drive media of each proposal must be submitted to:

Virginia Tech
Information Technology Acquisitions (0214)
1700 Pratt Drive
Blacksburg, VA 24061

Reference the Opening Date and Hour, and RFP Number in the lower left hand corner of the return envelope or package.

No other distribution of the proposals shall be made by the Offeror.

2. Proposal Preparation:

a) Proposals shall be signed by an authorized representative of the Offeror. All information requested should be submitted. Failure to submit all information requested may result in Virginia Tech requiring prompt submission of missing information and/or giving a lowered evaluation of the proposal. Proposals which are substantially incomplete or lack key information may be rejected by Virginia Tech at its discretion. Mandatory requirements are those required by law or regulation or are such that they cannot be waived and are not subject to negotiation.

b) Proposals should be prepared simply and economically providing a straightforward, concise description of capabilities to satisfy the requirements of the RFP. Emphasis should be on completeness and clarity of content.

c) Proposals should be organized in the order in which the requirements are presented in the RFP. All pages of the proposal should be numbered. Each paragraph in the proposal should reference the paragraph number of the corresponding section of the RFP. It is also helpful to cite the paragraph number, subletter, and repeat the text of the requirement as it appears in the RFP. If a response covers more than one page, the paragraph number and subletter should be repeated at the top of the next page. The proposal should contain a table of contents which cross references the RFP requirements. Information which the offeror desires to present that
does not fall within any of the requirements of the RFP should be inserted at an appropriate place or be attached at the end of the proposal and designated as additional material. Proposals that are not organized in this manner risk elimination from consideration if the evaluators are unable to find where the RFP requirements are specifically addressed.

d) Each copy of the proposal should be bound in a single volume where practical. All documentation submitted with the proposal should be bound in that single volume.

e) Ownership of all data, material and documentation originated and prepared for Virginia Tech pursuant to the RFP shall belong exclusively to Virginia Tech and be subject to public inspection in accordance with the Virginia Freedom of Information Act. Trade secrets or proprietary information submitted by an Offeror shall not be subject to public disclosure under the Virginia Freedom of Information Act. However, to prevent disclosure the Offeror must invoke the protections of Section 2.2-4342F of the Code of Virginia, in writing, either before or at the time the data or other materials is submitted. The written request must specifically identify the data or other materials to be protected and state the reasons why protection is necessary. The proprietary or trade secret material submitted must be identified by some distinct method such as highlighting or underlining and must indicate only the specific words, figures, or paragraphs that constitute trade secret or proprietary information. The classification of an entire proposal document, line item prices and/or total proposal prices as proprietary or trade secrets is not acceptable and may result in rejection of the proposal.

3. Oral Presentation: Offerors who submit a proposal in response to this RFP may be required to give an oral presentation of their proposal to Virginia Tech. This will provide an opportunity for the Offeror to clarify or elaborate on the proposal but will in no way change the original proposal. Virginia Tech will schedule the time and location of these presentations. Oral presentations are an option of Virginia Tech and may not be conducted. Therefore, proposals should be complete.

B. Specific Requirements

Proposals should be as thorough and detailed as possible so that Virginia Tech may properly evaluate your capabilities to provide the required goods and services. Offerors are required to submit the following information/items as a complete proposal:

1. A copy of your latest annual report.
2. Four (4) recent references, either educational or governmental, for whom you have provided the type of goods and services described herein. Include the date(s) the goods and services were furnished, the client name, address and the name and phone number of the individual Virginia Tech has your permission to contact.
3. Responses to the requirements as noted in Section VI formatted as noted above in Paragraph VII.A.2
4. Any proposed exceptions to the RFP terms and conditions.
5. Small, Women-owned and Minority-owned Business (SWAM) Utilization:

   If your business can not be classified as SWAM, describe your plan for utilizing SWAM subcontractors if awarded a contract. Describe your ability to provide reporting on SWAM subcontracting spend when requested. If your firm or any business that you plan to subcontract with can be classified as SWAM, but has not been certified by the Virginia Department of Minority Business Enterprise (DMBE), it is expected that the certification process will be initiated no later than the time of the award. If your firm is currently certified, you agree to maintain your certification for the life of the contract. For assistance with SWAM certification, visit the DMBE website at [www.dmbe.virginia.gov](http://www.dmbe.virginia.gov). Any questions relating to SWAM businesses or SWAM subcontracting opportunities can be directed to Mark Cartwright, the University’s Assistant Director for Supplier Diversity, at 540-231-3333 or mcartwright@vt.edu.

6. The return of the General Information Form and addenda, if any, signed and filled out as required.

VIII. SELECTION CRITERIA AND AWARD:

A. Selection Criteria
Proposals will be evaluated by Virginia Tech using the following:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Maximum Point Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Technical Requirements</td>
<td>23</td>
</tr>
<tr>
<td>2. Data Stewardship/User Privacy</td>
<td>9</td>
</tr>
<tr>
<td>3. Integration/Operation</td>
<td>16</td>
</tr>
<tr>
<td>4. Functionality/Service Levels</td>
<td>17</td>
</tr>
<tr>
<td>5. Pricing</td>
<td>25</td>
</tr>
<tr>
<td>6. SWAM Utilization</td>
<td>10</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

B. Award

Selection shall be made of two or more offerors deemed to be fully qualified and best suited among those submitting proposals on the basis of the evaluation factors included in the Request for Proposal, including price, if so stated in the Request for Proposal. Negotiations shall then be conducted with the offerors so selected. Price shall be considered, but need not be the sole determining factor. After negotiations have been conducted with each offeror so selected, Virginia Tech shall select the offeror which, in its opinion, has made the best proposal, and shall award the contract to that offeror. Virginia Tech may cancel this Request for Proposal or reject proposals at any time prior to an award. Should Virginia Tech determine in writing and in its sole discretion that only one offeror has made the best proposal, a contract may be negotiated and awarded to that offeror. The award document will be a contract incorporating by reference all the requirements, terms and conditions of this solicitation and the Contractor's proposal as negotiated. See Attachment B for sample contract form.

IX. OPTIONAL PRE-PROPOSAL CONFERENCE:

An optional pre-proposal conference will be held on March 16, 2011 at 10:00 AM in Room 208, 1700 Pratt Drive, Blacksburg, VA 24060. This is in the Corporate Research Center adjacent to the Virginia Tech campus, across from the Virginia Tech airport. The purpose of this conference is to allow potential Offerors an opportunity to present questions and obtain clarification relative to any facet of this solicitation.

While attendance at this conference will not be a prerequisite to submitting a proposal, offerors who intend to submit a proposal are encouraged to attend.

Bring a copy of this solicitation with you. Any changes resulting from this conference will be issued in a written addendum to this solicitation.

The pre-proposal conference site is off-campus and does not require a parking permit. If you choose to park on-campus, it is strongly recommended that you obtain a Virginia Tech parking permit for display on your vehicle prior to parking. Parking permits are available from the Virginia Tech Parking Services Department located at 455 Tech Center Drive, phone: (540) 231-3200, e-mail: parking@vt.edu.

We will offer a choice of in-person or pre-arranged teleconference attendance for the optional pre-proposal conference. All teleconference attendance requires advance arrangements; deadline March 14, 3:00 PM. Eastern time. See Attendance section below.

The format of the conference is to summarize background and procedural information, ask if there are follow-up questions to any Questions & Answers documents already posted to our department website (http://www2.itavt.edu/purchasing/index.html), receive any new questions, and close. Note that we do not plan to provide answers to questions immediately. For accuracy we plan to respond in writing in a document entitled
Questions & Answers Pre-Proposal Conference that will be posted within a few days as an addendum to the RFP on the above department website. Please contact Nancy Sterling if any questions arise.

Attendance:

**In-person attendance** – To attend in person, no pre-arrangement is necessary. However an email to Nancy Sterling with your company name and the number of people planning to attend does help with our planning. Information similar to the teleconference information will be taken at the meeting.

**Teleconference attendance** – To attend by teleconference, pre-arrangement is necessary. The deadline for receipt of the Teleconference Pre-Registration Form (See Attachment C) is March 14, at 3:00 PM Eastern time. The process requires contractors to complete Attachment C, including authorized signature confirming the requirements, and e-mail the completed form to Nancy Sterling (nancy.sterling@vt.edu). Virginia Tech will provide teleconference access information by March 15 at 3:00 P.M. Callers will pay their normal long distance fees, if applicable. Note that the maximum number of phone connections per company is two. For sound quality and least background noise, please call from a quiet room, use a hard-wired land line, and mute speakerphones when not addressing the conference.

X. **INVOICES:**

Invoices for goods or services provided under any contract resulting from this solicitation shall be submitted to:

Virginia Polytechnic Institute and State University  
Accounts Payable  
201 Southgate Center  
Blacksburg, VA 24061

XI. **ADDENDUM:**

Any **ADDENDUM** issued for this solicitation may be accessed at [http://www.ita.vt.edu/email-rfp.html](http://www.ita.vt.edu/email-rfp.html). Since a paper copy of the addendum will not be mailed to you, we encourage you to check the web site regularly.

XII. **CONTRACT ADMINISTRATION:**

A. Ron Jarrell, Technical Team Manager, NI&S Systems Support at Virginia Tech or his/her designee, shall be identified as the Contract Administrator and shall use all powers under the contract to enforce its faithful performance. All direct pre-award contact regarding any solicitations shall be solely through the Contract Officer, not the Contract Administrator.

B. The Contract Administrator, or his/her designee, shall determine the amount, quantity, acceptability, fitness of all aspects of the services and shall decide all other questions in connection with the services. The Contract Administrator, or his/her designee, shall not have authority to approve changes in the services which alter the concept or which call for an extension of time for this contract. Any modifications made must be authorized by the Virginia Tech Computer Purchasing Department through a written amendment to the contract.

XIII. **TERMS AND CONDITIONS:**

This solicitation and any resulting contract/purchase order shall be governed by the attached terms and conditions.

XIV. **ATTACHMENTS:**

Attachment A – Terms and Conditions  
Attachment B – Standard Contract Form  
Attachment C – Teleconference Pre-Registration Form
TERMS AND CONDITIONS

RFP General Terms and Conditions

http://www.purch.vt.edu/html.docs/terms/GTC_RFP_100110.pdf

Special Terms and Conditions

1. **AUDIT**: The Contractor hereby agrees to retain all books, records, and other documents relative to this contract for five (5) years after final payment, or until audited by the Commonwealth of Virginia, whichever is sooner. Virginia Tech, its authorized agents, and/or the State auditors shall have full access and the right to examine any of said materials during said period.

2. **AVAILABILITY OF FUNDS**: It is understood and agreed between the parties herein that Virginia Tech shall be bound hereunder only to the extent of the funds available or which may hereafter become available for the purpose of this agreement.

3. **CANCELLATION OF CONTRACT**: Virginia Tech reserves the right to cancel and terminate any resulting contract, in part or in whole, without penalty, upon 60 days written notice to the Contractor. In the event the initial contract period is for more than 12 months, the resulting contract may be terminated by either party, without penalty, after the initial 12 months of the contract period upon 60 days written notice to the other party. Any contract cancellation notice shall not relieve the Contractor of the obligation to deliver and/or perform on all outstanding orders issued prior to the effective date of cancellation.

4. **CONTRACT DOCUMENTS**: The contract entered into by the parties shall consist of the Request for Proposal including all modifications thereof, the proposal submitted by the Contractor, the written results of negotiations, the Commonwealth Standard Contract Form, all of which shall be referred to collectively as the Contract Documents.

5. **INSURANCE**: By signing and submitting a proposal under this solicitation, the Offeror certifies that if awarded the contract, it will have the following insurance coverage at the time the work commences. Additionally, it will maintain these during the entire term of the contract and that all insurance coverage will be provided by insurance companies authorized to sell insurance in Virginia by the Virginia State Corporation Commission.

During the period of the contract, Virginia Tech reserves the right to require the Contractor to furnish certificates of insurance for the coverage required.

**INSURANCE COVERAGES AND LIMITS REQUIRED**:

A. Worker's Compensation – Statutory requirements and benefits.
B. Employers Liability – $100,000.00
C. General Liability – $500,000.00 combined single limit. Virginia Tech and the Commonwealth of Virginia shall be named as an additional insured with respect to goods/services being procured. This coverage is to include Premises/Operations Liability, Products and Completed Operations Coverage, Independent Contractor's Liability, Owner's and Contractor's Protective Liability and Personal Injury Liability.
D. Automobile Liability – $50,000.00
E. Builders Risk – For all renovation and new construction projects under $100,000 Virginia Tech will provide All Risk – Builders Risk Insurance. For all renovation contracts, and new construction from $100,000 up to $500,000 the contractor will be required to provide All Risk – Builders Risk Insurance in the amount of the contract and name Virginia Tech as additional insured. All insurance verifications of insurance will be through a valid insurance certificate.

The contractor agrees to be responsible for, indemnify, defend and hold harmless Virginia Tech, its officers, agents and employees from the payment of all sums of money by reason of any claim against them arising out of any and all occurrences resulting in bodily or mental injury or property damage that may happen to occur in connection with and during the performance of the contract, including but not limited to claims under the Worker's Compensation Act. The contractor agrees that it will, at all times, after the completion of the work, be responsible for, indemnify, defend and hold harmless Virginia Tech, its officers, agents and employees from all liabilities resulting from bodily or mental injury or property damage directly or indirectly arising out of the performance or nonperformance of the contract.

6. **NOTICES**: Any notices to be given by either party to the other pursuant to any contract resulting from this solicitation shall be in writing, hand delivered or mailed to the address of the respective party at the following address:
7. **PROPOSAL ACCEPTANCE PERIOD**: Any proposal received in response to this solicitation shall be valid for (120) days. At the end of the (120) days the proposal may be withdrawn at the written request of the Offeror. If the proposal is not withdrawn at that time it remains in effect until an award is made or the solicitation is cancelled.

8. **CONTRACTOR RESPONSIBILITIES**: The Contractor shall be responsible for completely supervising and directing the work under this contract and all subcontractors that he may utilize, using his best skill and attention. Subcontractors who perform work under this contract shall be responsible to the Contractor. The Contractor agrees that he is as fully responsible for the acts and omissions of his subcontractors and of persons employed by them as he is for the acts and omissions of his own employees.

9. **PROPOSAL PRICES**: Proposal shall be in the form of a firm unit price for each item during the contract period.

10. **QUANTITIES**: Quantities set forth in this solicitation are estimates only, and the Contractor shall supply at proposal prices actual quantities as ordered, regardless of whether such total quantities are more or less than those shown.

11. **RENEWAL OF CONTRACT**: This contract may be renewed by Virginia Tech upon written agreement of both parties for five successive one year periods, or as negotiated under the terms of the current contract, and at a reasonable time (approximately 90 days) prior to the expiration.

12. **COMMUNICATIONS**: Communications regarding this Request for Proposals (RFP) shall be formal from the date of issue for this RFP, until either a Contractor has been selected or the Information Technology Acquisitions Office rejects all proposals. Formal communications will be directed to the Information Technology Acquisitions Office. Informal communications, including but not limited to request for information, comments or speculations regarding this RFP to any University employee other than an Information Technology Acquisitions Office representative may result in the offending Offeror’s proposal being rejected.

13. **RIGHT TO SELECT PROJECT PERSONNEL**: The University has the right to interview and select all of the Contractor’s personnel that will provide services under the Agreement.

14. **RIGHT TO REMOVE PROJECT PERSONNEL**: The University has the right to remove any of the selected Contractor’s personnel that will provide services under the Agreement.

15. **SUBCONTRACTS**: No portion of the work shall be subcontracted without prior written consent of Virginia Tech. In the event that the Contractor desires to subcontract some part of the work specified herein, the Contractor shall furnish Virginia Tech the names, qualifications and experience of their proposed subcontractors. The Contractor shall, however, remain fully liable and responsible for the work to be done by his subcontractor(s) and shall assure compliance with all requirements of the contract.

16. **ADVERTISING**: In the event a contract is awarded for supplies, equipment, or services resulting from this solicitation, no indication of such sales or services to Virginia Tech will be used in product literature or advertising without the prior written consent of Virginia Tech. The Contractor shall not state in any of the advertising or product literature that the Commonwealth of Virginia or any agency or institution of the Commonwealth has purchased or uses its products or services.

17. **CERTIFICATION TESTING AND ACCEPTANCE**: The system specified in the contract shall be considered ready for production testing upon receipt of documentation from the Contractor that a successful system audit or diagnostic test...
Attachment A - Terms and Conditions

21. **RIGHTS AND LICENSE IN AND TO CUSTOMER AND END USER DATA:**

The parties agree that as between them, all rights including all intellectual property rights in and to Customer and End User data shall remain the exclusive property of Customer, and Vendor has a limited, nonexclusive license to use these data as provided solely for the purpose of performing its obligations hereunder. Neither party has any rights, implied or
otherwise, to the other’s data, content, or intellectual property, except as the parties expressly agreed otherwise in writing.

22. DATA PRIVACY:
A. Vendor will use Customer Data and End User Data only for the purpose of fulfilling its duties hereunder and for Customer’s and its End User’s sole benefit, and will not share such data with or disclose it to any third party without the prior written consent of Customer or as otherwise required by law. By way of illustration and not of limitation, Vendor will not use such data for Vendor’s own benefit and, in particular, will not engage in “data mining” of Customer or End User Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by Customer.
B. Vendor will provide access to Customer and End User Data only those Vendor employees and subcontractors who need to access the data to fulfill Vendor’s obligations under this Agreement. Vendor will ensure that employees who perform work on the Vendor’s behalf have read, understood, and received appropriate instruction as to how to comply with the data protection provisions contained herein, and have undergone all background screening and possess all qualifications required by Customer prior to being granted access to the Data.

23. DATA SECURITY AND INTEGRITY:
A. All facilities used to store and process Customer and End User data will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Vendor’s own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, Vendor warrants that all Customer Data and End User Data will be encrypted in transmission (including via web interface) and storage at no less than 128-bit level, and that Vendor will comply with all other technical specifications of Customer. Vendor will comply with the requirements of FERPA, HIPAA, ITAR and FISMA. Vendor will use industry-standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services to Customer.
B. Vendor will configure the Services to filter spam while permitting communications from third-party Internet Protocol addresses identified by Customer as legitimate.
C. Vendor will at its expense conduct or have conducted at least annually:
   i. A SAS 70 audit of Vendor’s security policies, procedures and controls resulting in the issuance of a Service Auditor’s Report Type II;
   ii. a vulnerability scan, performed by a scanner approved by Customer, of Vendor’s systems and facilities that are used in any way to deliver Services; and a formal penetration test, performed by a process and qualified personnel approved by Customer, of Vendor’s systems and facilities that are used in any way to deliver services hereunder
   iii. Vendor will provide Customer upon request the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations to Customer and report on such. Customer may require, at its expense, Vendor to perform additional audits and tests, the results of which will be provided promptly to Customer.

24. DATA INTEGRITY:
Vendor will take commercially reasonable measures, including regular data integrity audits, to protect Customer and End User Data against deterioration or degradation of data quality and authenticity.

25. RESPONSE TO LEGAL ORDERS, DEMANDS OR REQUESTS FOR DATA:
A. Except as otherwise expressly prohibited by law, Vendor will:
   i. immediately notify Customer of any subpoenas, warrants, or other legal orders, demands or requests received by Vendor seeking Customer and/or End User Data;
   ii. consult with Customer regarding its response;
   iii. cooperate with Customer’s reasonable requests in connection with efforts by Customer to intervene and quash or modify the legal order, demand or request; and
   iv. upon Customer’s request, provide Customer with a copy of its response.
B. If Customer receives a subpoena, warrant, or other legal order, demand or request seeking Customer or End User Data maintained by Vendor, Customer will promptly provide a copy to Vendor. Vendor will promptly supply Customer with copies of data required for Customer to respond, and will cooperate with Customer’s reasonable requests in connection with its response.

26. DATA COMPROMISE RESPONSE:
Attachment A - Terms and Conditions

29. CHANGES TO SERVICE:
A. Operational at least 99.99% of the time in any given month during the term of this Agreement, meaning that the outage or downtime percentage will be not more than .01%. In the event of a Service outage, Vendor will promptly and at Vendor’s expense use commercial best efforts to restore the Services as soon as possible, and
i. unless the outage was caused by a force majeure event, refund or credit Customer, at Customer’s election, the pro-rated amount of fees corresponding to the time Services were unavailable. Neither party will be liable to the other for any failure or delay in performance to the extent said failures or delays are proximately caused.
by forces beyond that party’s reasonable control, provided that the party resumes performance as soon as it is reasonably able to do so.

B. From time to time it may be necessary or desirable for either the Customer or Vendor to propose changes in the Services provided. Automatic upgrades to any software used by Vendor to provide the Services that simply improve the speed, efficiency, reliability, or availability of existing Services and do not alter or add functionality, are not considered “changes to the Services” and such upgrades will be implemented by Vendor on a schedule no less favorable than provided by Vendor to any other customer receiving comparable levels of Services.

C. Vendor will provide Customer with a minimum of one (1) days’ prior notice of scheduled downtime in the provision of Services for maintenance or upgrades. To the extent possible, Vendor will schedule downtime during times of ordinarily low use by Customer. In the event of unscheduled and unforeseen downtime for any reason, except as otherwise prohibited by law Vendor will promptly notify Customer and cooperate with Customers’ reasonable requests for information regarding the downtime (including causes, effect on Services, and estimated duration).

D. Customer may suspend or terminate (or direct Vendor to suspend or terminate) an End User’s access to Services in accordance with Customer’s policies. Vendor may suspend access to Services by Customer or an End User immediately in response to an act or omission that reasonably appears to jeopardize the security or integrity of Vendor’s Services or the network(s) or facilities used to provide the Services. Suspension will be to the minimum extent, and of the minimum duration, required to prevent or end the security issue. Vendor may suspend Customer’s access to Services if, after at least thirty (30) days’ written notice to Customer and subsequent good-faith, commercially reasonable efforts to resolve the matter with Customer to the parties’ mutual satisfaction, Customer remains in material breach of the terms of an agreement between the parties. The suspension will be lifted immediately once the breach is cured. Vendor may suspend access to Services by an End User in response to (i) a material breach by End User of any terms of use s/he has agreed to in connection with receiving the Services. Vendor will notify Customer of any suspension of End User access to Services before suspension or, if notice before is not feasible, as soon as reasonably possible thereafter.

30. **INSTITUTIONAL BRANDING:** Vendor will provide reasonable and appropriate opportunities for Customer branding of Vendor services. Each party shall have the right to use the other party’s trademarks only in connection with performing the functions provided in this Agreement. Any use of a party’s trademarks will inure to the benefit of the party holding intellectual property rights in and to that trademark.

31. **EMERGENCY COMMUNICATIONS:** Vendor warrants that its Services are compatible with and will not interfere with Customer’s provision of emergency communications in compliance with applicable law and Customer policies. This includes enabling and supporting at least one (1) Customer simulations annually of emergency communications.

32. **WARRANTIES AND LIABILITY:**
   
   A. Vendor warrants that all services provided to Customer shall conform to and be performed in accordance with Vendor’s proposal and that Vendor’s services shall not infringe any third-party intellectual property rights.
   
   B. The Contractor agrees that the goods and services furnished under any award resulting from this solicitation shall be covered by the most favorable commercial warranties the contractor gives any customer for such goods and services and that the rights and remedies provided therein are in addition to and do not limit those available to Virginia Tech by any other clause of this solicitation. A copy of this warranty must be furnished with the proposal.
COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract Number: ____________________________

This contract entered into this ___ day of ___________ 20___, by ______________________, hereinafter called the "Contractor" and Commonwealth of Virginia, Virginia Polytechnic Institute and State University called "Virginia Tech".

WITNESSETH that the Contractor and Virginia Tech, in consideration of the mutual covenants, promises and agreements herein contained, agrees as follows:

SCOPE OF CONTRACT: The Contractor shall provide the ___________ to Virginia Tech as set forth in the Contract Documents.

PERIOD OF CONTRACT: From _________________________ through ________________________.

COMPENSATION AND METHOD OF PAYMENT: The Contractor shall be paid by Virginia Tech in accordance with the contract documents.

CONTRACT DOCUMENT: The contract documents shall consist of this signed contract, Request For Proposal Number ___________ dated __________, together with all written modifications thereof and the proposal submitted by the Contractor dated ___________ and the Contractor's letter dated ___________, all of which contract documents are incorporated herein.

In WITNESS WHEREOF, the parties have caused this Contract to be duly executed intending to be bound thereby.

Contractor: ____________________________
By: _________________________________
Title: ________________________________

Virginia Tech
By: _________________________________
Title: ________________________________
Attachment C - Teleconference Pre-Registration Form

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
RFP Number 0016512 - eMail / Collaboration Services

Teleconference Pre-Registration Form - Complete and e-mail this form to nancy.sterling@vt.edu
Conference Date: March 16, 2011, 9:00 AM Eastern
Pre-registration Teleconference Deadline: March 14, 2011, 3:00 PM Eastern

**PLEASE PRINT or TYPE**

Company Name: ________________________________________________________________

Mailing Address: ________________________________________________________________________________

<table>
<thead>
<tr>
<th>INDIVIDUAL NAME</th>
<th>TITLE</th>
<th>PHONE NUMBER</th>
<th>FAX NUMBER</th>
<th>E-MAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The authorized signature below confirms the following:
1) the above information is accurate - only those individuals named above will attend the teleconference
2) the company will honor the **limit of two phone connections** for their entire company
3) the company will minimize background noise during teleconference participation – suggestions: call from quiet room, use hard-wired land line, mute speakerphones
4) the company will not share the phone number and access code (provided later) with anyone beyond those named above

Authorized Signature for Company Named Above: _____________________________________________________

Printed/Typed Name and Title: ____________________________________________________________________
ADDENDUM # 1 TO RFP # 0016512
For
E-mail/Collaboration Services

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
INFORMATION TECHNOLOGY ACQUISITIONS (0214)
1700 PRATT DRIVE
BLACKSBURG, VA 24061

DATE
March 21, 2011

ORIGINAL DUE DATE AND HOUR
March 28, 2011 at 3:00 PM (not changed)

ADDRESS ALL INQUIRIES AND CORRESPONDENCE TO: John Krallman, Director of Information Technology Acquisitions
E-MAIL ADDRESS: john.krallman@vt.edu  TELEPHONE NUMBER (540) 231-6233
FAX NUMBER (540) 231-4110

Questions and Answers from the Pre-Proposal Conference through March 21, 2011

Q1. What platforms will be migrated? Does this include Exchange?
A1. Migration is mainly from a Sun-based hardware/software solution – JAVA. Some Exchange users may choose to migrate, but is not the primary thrust and will not be required. No plans for the proposed email solution to interface with Oracle.

Q2. Number of users being migrated?
A2. We’ve been trimming and expect the number to be 70-80,000. At this moment the count is about 78,000.

Q3. Size of mail storage repository?
A3. The mail store is 2 TB (terabytes). We have no quota, and we retain records for 62-days.

Q4. What archive solution is used?
A4. We have no archive solution. Methodology for individual end-users to store online may be provided in proposals (similar to .pst but different format).

Q5. What is the breakdown of supported clients?
A5. We encourage web-based interface. Proposals could provide the oldest and latest version of all clients the proposed system supports.

Q6. Do you need a Blackberry enterprise solution?
A6. We don’t have or need a Blackberry enterprise solution and don’t support them. The majority of Blackberry users are on Exchange and use ActiveSync or Goodlink.

Q7. Must, should, may – what is the intended difference?
A7. Shall and must items are essential to meet our system requirements. Should and may are identified features, and if the proposed solution has those features they ideally would be detailed in proposals.

Q8. How should pricing be presented?
A8. Ideally for scalability, cost could be provided per user, per year. Base solutions could include all ‘shall’ items, with other items priced as options.

Q9. How long should proposal pricing be valid?
A9. Six months is appropriate.

Q10. What is the timing to award?
A10. We are aiming for an award decision this summer, ideally to implement by mid-August.

Q11. What integration with vendor’s ID management solution is needed?
A11. We want to leverage our existing ID management, Open LDAP, as listed in the RFP.

Q12. What is needed for authentication?
A12. Describe all authentication solutions with which your proposed system can interact.

Q13. Will the migrating email need to support calendar and contacts?
A13. These will not be used or supported.

Q14. What is expected for system security data?
A14. Since this is a hosted solution, proposals should fully describe physical security, access control, patch and penetration test schedules, and other issues. See some relevant security URLs below. VT will enforce its own internal security policies.

Q15. Will the migration include multiple domains and name spaces? Are these all on the same platform?
A15. The initial migration will be only the main domain vt.edu. We’d like the option after initial migration to offer our sub-domain groups the ability to migrate as well (ex: xxx.vt.edu). VT is decentralized, so multiple platforms are used.

Q16. What groups of users will be migrating?
A16. Students, faculty, staff, retirees, and VT affiliates will be migrating. A handful of sponsored users are subject to ITAR and FISMA regulations and require hosting in US, and these may be migrating as a separate group depending on the proposed solution.

Q17. Will the solution need to display Free/Busy?
A17. No, this is outside the scope.

Q18. What is the last day for questions?
A18. March 28, 3pm is the last date for our office to receive questions. Addendums with questions and answers will be posted to the ITA and eVA websites listed in the RFP. We will not be extending the deadline.

Q19. Will the security requirements detailed in the RFP, such as HIPPA, apply to all users, or is this a segregated group?
A19. These requirements apply to all users.

Q20. Will you provide information on Graham-Leach-Bliley?
A20. That act relates to information privacy. Information is available at http://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act and other sources.

Q21. What level of support will be provided by VT’s internal IT?
A21. For implementation we have a project team in place representing critical aspects of the project; these people work with the current mail system. For system usage, VT will provide first-level help desk and VT will make any necessary contact with the service provider.

Q22. Are there other criteria or review groups or processes beyond the RFP?
A22. Selection will be based on the criteria in the RFP, including proposal responses, potential follow-up clarification questions and/or demonstrations. Student and Faculty/Staff representatives are included on the VT review team.

Below are security standard URLs related to this RFP.

sp800-53A-rev1-final.pdf

FEDERAL INFORMATION PROCESSING STANDARD (FIPS) 199, STANDARDS FOR SECURITY CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS

Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems

Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems
<table>
<thead>
<tr>
<th>FULL LEGAL NAME (PRINT)</th>
<th>FEDERAL TAXPAYER NUMBER (ID#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Company name as it appears with your Federal Taxpayer Number)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BUSINESS NAME/DBA NAME/TA NAME</th>
<th>FEDERAL TAXPAYER NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>(If different than the Full Legal Name)</td>
<td>(If different than ID# above)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BILLING NAME</th>
<th>FEDERAL TAXPAYER NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Company name as it appears on your invoice)</td>
<td>(If different than ID# above)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PURCHASE ORDER ADDRESS</th>
<th>PAYMENT ADDRESS</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>CONTACT NAME/TITLE (PRINT)</th>
<th>SIGNATURE (IN INK)</th>
<th>DATE</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>E-MAIL ADDRESS</th>
<th>TELEPHONE NUMBER</th>
<th>TOLL FREE TELEPHONE NUMBER</th>
<th>FAX NUMBER TO RECEIVE E-PROCUREMENT ORDERS</th>
</tr>
</thead>
</table>
Questions and Answers through March 30, 2011

Q1) How many users require archiving and e-discovery (e.g. everybody, faculty only, etc)? Question #1 is designed to determine if ALL users require archiving and e-discovery. If only some require this service, we will consider providing appropriate scenarios (with corresponding pricing options) in the proposal.

A1) Only a subset of users require archiving and e-discovery; those are principally senior administrators, who are also generally users of our Exchange system, and may be getting archiving services there. It's is perfectly acceptable to bid archiving/e-discovery as an optional per-user component.

Q2) How many internal IT resources does VirginiaTech plan to assign to this project? Does VirginiaTech require that the successful vendor handle all aspects of a start-to-finish implementation, or is self-service an option where a designated sub-group of users would be implemented by vendor, training on the process provided to VirginiaTech personnel, who would then handle the remaining mailboxes (with vendor support available when required)? Question #2 is designed to determine if VirginiaTech might be interested in a ‘self-service’ option as outlined in the question.

A2) The Internal IT group is familiar with email migrations, and recently migrated alumni users off of our central systems to a Google solution. A project team has already been formed with key representatives from all the appropriate internal groups prepared to handle implementation. We require the successful bidder to provide at a minimum appropriate engineering/technical contacts inside the organization able to perform effective corrective measures as needed, and provide necessary documentation and accesses required for Virginia Tech to successfully implement the transition, and are prepared to do the work in preparing our provisioning system, creating users, migrating e-mail if needed, etc. Bidders can provide proposals for higher levels of implementation if such configuration services are an available offering.

Q3) What is the exact version of the Oracle OCUCS mail server, and is that simply a rename of the previous Sun One Messaging server. …i.e. did you upgrade the Sun One server to Oracle (and what Oracle version), or is it still just Sun One renamed to Oracle and what Sun One version?

A3) Sun Java(tm) System Messaging Server 6.3-5.02 (built Oct 12 2007; 32bit). Oracle OCUCS is simply the name it's currently marketed under.
<table>
<thead>
<tr>
<th><strong>FULL LEGAL NAME (PRINT)</strong></th>
<th><strong>FEDERAL TAXPAYER NUMBER (ID#)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>(Company name as it appears with your Federal Taxpayer Number)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>BUSINESS NAME/DBA NAME/TA NAME</strong></th>
<th><strong>FEDERAL TAXPAYER NUMBER</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>(If different than the Full Legal Name)</td>
<td>(If different than ID# above)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>BILLING NAME</strong></th>
<th><strong>FEDERAL TAXPAYER NUMBER</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>(Company name as it appears on your invoice)</td>
<td>(If different than ID# above)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>PURCHASE ORDER ADDRESS</strong></th>
<th><strong>PAYMENT ADDRESS</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>CONTACT NAME/TITLE (PRINT)</strong></th>
<th><strong>SIGNATURE (IN INK)</strong></th>
<th><strong>DATE</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>E-MAIL ADDRESS</strong></th>
<th><strong>TELEPHONE NUMBER</strong></th>
<th><strong>TOLL FREE TELEPHONE NUMBER</strong></th>
<th><strong>FAX NUMBER TO RECEIVE E-PROCUREMENT ORDERS</strong></th>
</tr>
</thead>
</table>
Attachment B

Contract UCP-TS-C02-12

Proposal submitted by Contractor for RFP 0016512 dated April 4, 2011
This proposal valid for 180 days post April 4th, 2011 submission.
RFP 0016512

GENERAL INFORMATION FORM

1. QUESTIONS: All inquiries for information regarding this solicitation should be directed to: Nancy Sterling, Phone: (540) 231-9517, e-mail: nancy.sterling@vt.edu. Questions will be received through March 28, 2011 at 3:00 PM.

   - DUE DATE: Sealed Proposals will be received until April 4, 2011 at 3:00 PM. Failure to submit proposals to the correct location by the designated date and hour will result in disqualification.

2. ADDRESS: Proposals should be mailed or hand delivered to: Virginia Polytechnic Institute and State University (Virginia Tech), Information Technology Acquisitions, 1700 Pratt Drive (0214), Blacksburg, Virginia 24061. Reference the Opening Date and Hour, and RFP Number in the lower left corner of the return envelope or package.

3. PRE-PROPOSAL CONFERENCE: See Section IX for information regarding a pre-proposal conference.

4. TYPE OF BUSINESS: (Please check all applicable classifications). If your classification is certified by the Virginia Department of Minority Business Enterprise, provide your certification number: _______________________________. For certification assistance, please visit: http://www.dmbe.state.va.us/swamcert.html.

   - Large
   - X Small business – An independently owned and operated business which, together with affiliates, has 250 or fewer employees or average annual gross receipts of $10 million or less averaged over the previous three years. Department of Minority Business Enterprise (DMBE) certified women-owned and minority-owned business shall also be considered small business when they have received DMBE small business certification.

   - X Women-owned business – A business concern that is at least 51% owned by one or more women who are U. S. citizens or legal resident aliens, or in the case of a corporation, partnership, or limited liability company or other entity, at least 51% of the equity ownership interest is owned by one or more women who are citizens of the United States, who are in full compliance with the United States immigration law, and both the management and daily business operations are controlled by one or more women who are U. S. citizens or legal resident aliens.

   - Minority-owned business – A business concern that is at least 51% owned by one or more minority individuals (see Section 2.2-1401, Code of Virginia) or in the case of a corporation, partnership, or limited liability company or other entity, at least 51% of the equity ownership interest in the corporation, partnership, or limited liability company or other entity is owned by one or more minority individuals and both the management and daily business operations are controlled by one or more minority individuals.

6. COMPANY INFORMATION/SIGNATURE: In compliance with this Request For Proposal and to all the conditions imposed therein and hereby incorporated by reference, the undersigned offers and agrees to furnish the goods and services in accordance with the attached signed proposal and as mutually agreed upon by subsequent negotiation.

<table>
<thead>
<tr>
<th>FULL LEGAL NAME (PRINT)</th>
<th>(Company name as it appears with your Federal Taxpayer Number)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SADA Systems, Inc.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BUSINESS NAME/DBA NAME/TA NAME</th>
<th>(If different than the Full Legal Name)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BILLING NAME</th>
<th>(Company name as it appears on your invoice)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SADA Systems, Inc.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PURCHASE ORDER ADDRESS</th>
<th>PAYMENT ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>5250 Vineland Avenue</td>
<td>5250 Vineland Avenue</td>
</tr>
<tr>
<td>North Hollywood, CA 91601</td>
<td>North Hollywood, CA 91601</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONTACT NAME/TITLE (PRINT)</th>
<th>CONTACT NAME/TITLE (PRINT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tony Safoian, CEO</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E-MAIL ADDRESS</th>
<th>TELEPHONE NUMBER</th>
<th>TOLL FREE TELEPHONE NUMBER</th>
<th>FAX NUMBER TO RECEIVE E-PROCUREMENT ORDERS</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:tony.safoian@sadasystems.com">tony.safoian@sadasystems.com</a></td>
<td>818.766.2400</td>
<td>866.997.0000</td>
<td>818.766.0090</td>
</tr>
</tbody>
</table>

SIGNATURE (IN INK) 4/4/2011

Contract UCP-TS-C02-12      Page 36 of 177
This proposal valid for 180 days post April 4th, 2011 submission.
This proposal valid for 180 days post April 4th, 2011 submission.

Table of Contents

Section I – Purpose .............................................................................................................. 3
Section II – Contract Period ............................................................................................. 3
Section III – Background .................................................................................................... 3
Section IV – EVA Business-to-Government Electronic Procurement System ............... 5
Section V – Contract Participation .................................................................................... 5
Section VI – Statement of Needs ....................................................................................... 6
  Section VI.A – General Services Sought ........................................................................ 6
  Section VI.B – Specific Technical Requirements ............................................................. 6
  Section VI.C – Technical Discovery ............................................................................... 14
  Section VI.D – Integration and Operational Issues ......................................................... 41
  Section VI.E – Functionalities ....................................................................................... 49
  Section VI.F – Service Levels ......................................................................................... 61
  Section VI.G – Additional SADA Offerings ................................................................... 68
  Section VI.H – Cost ....................................................................................................... 71
  Section VI.I – Additional Relevant Information .............................................................. 73
Section VII – Proposal Preparation and Submission .......................................................... 73

All responses are noted by the following heading in black text immediately after the question it is responding to in grey text:

SADA SYSTEMS:

[Proposers Answer]
I. PURPOSE:

The purpose of this Request for Proposal (RFP) is to solicit sealed proposals to establish a contract through competitive negotiations for E-mail/Collaboration Services by Virginia Polytechnic Institute and State University (Virginia Tech), an agency of the Commonwealth of Virginia.

II. CONTRACT PERIOD:

The term of this contract is for three (3) years, or as negotiated. There will be an option for five (5) one-year renewals, or as negotiated.

III. BACKGROUND:

A. University Overview

Founded in 1872 as a land-grant college, Virginia Tech (www.vt.edu) is the most comprehensive university in the Commonwealth of Virginia and is among the top research universities in the nation. Virginia Tech’s nine colleges are dedicated to quality, innovation, and results through teaching, research, and outreach activities. At its 2,600 acre main campus located in Blacksburg and other campus centers in Northern Virginia, Southwest Virginia, Hampton Roads, Richmond, Southside, and Roanoke, Virginia Tech enrolls more than 28,000 undergraduate and graduate students from all 50 states and more than 100 countries in 180 academic degree programs.

Virginia Polytechnic Institute & State University operating as Virginia Tech (“Virginia Tech”) seeks proposals for comprehensive e-mail, calendaring, and collaboration services for their university employees and students. As detailed below, the requested services must be stable, secure, state of the art, feature rich, scalable, integrated, and available for installation, service, and maintenance on both a single institution and multi-institutional basis. Vendors shall specifically address all enumerated financial, administrative and technical requirements, but shall also discuss how their proposals might enable the collaborating institution to:

• Increase efficiency through standardization.
Comment: Many of the services upon which Virginia Tech depends have standardized around architectures, operational practices, and core technologies.

Nevertheless, the ongoing focus on department/campus level aggregation and provisioning produces fragmented environments with many customizations that add little value and also increase the costs of the service for each department/college. Through this RFP, we will explore aggregation/implementation above the level of the individual department/college, with the hope of leveraging standardization and benefitting operational efficiencies and the bottom line.

• Increase interoperability and associated capacity for collaboration.
Comment: University researchers and scholars collaborate across global disciplinary communities as well as within their home institution. By aggregating demand and associated operations above the level of the individual department, or college, Virginia Tech seeks proposals that will enable a technical environment that is easier to navigate across the institution (e.g., sharing of institutional directories and shared capacities to create virtual collaboration groups and shared tools at an institutional level).

B. Current Campus IT Environments

Virginia Tech has a campus population in excess of 60,000 users, including faculty, students, staff, and affiliates. Typically Virginia Tech colleges and institution have heterogeneous computing environments and support the use of multiple Windows, Macintosh and Unix/Linux operating systems. (See VI.B.1.a)
C.  Current E-mail Environments

Virginia Tech has approximately 100,000 e-mail users, including faculty, students, staff and affiliates. Most of these users use the central e-mail services (typically IMAP-based, but increasingly expanding to encompass Microsoft Exchange servers) provided by central IT, while others use services provided by their school or department (subunits of the institution). Shared access to e-mail folders is often used for delegating access and/or sharing data with individual users or groups of users (static and dynamic), or to facilitate group workflow. Centrally provided e-mail services are tightly integrated with campus directory (typically LDAP and AD) and authentication systems (typically LDAP, CAS, Shibboleth and/or AD). Existing quotas provided by the Virginia Tech range from 200 MB to 2 GB, or are effectively unlimited, but with a 30 day retention period. Users access their e-mail through either a web interface or a native client application. (See VI.B.2.a) The Mac and Windows clients typically support synchronization with various handheld devices. (See VI.B.4.a)

D.  Current Calendar Environments

Virginia Tech has approximately 6,000 calendar users, including faculty, students, staff and affiliates. Most of these users use the central calendar services provided by central IT within the institution (typically Microsoft Exchange), while others use services provided by their school or department (subunits of the institution). Shared access to calendar data is very important for many campus users, including the ability to delegate access and/or share data with individual users or groups of users (static and dynamic). Users access their calendar through either a web interface or a native client application. (See VI.B.2.a) The Mac and Windows clients typically support synchronization with various handheld devices. (See VI.B.4.a)

IV.  EVA BUSINESS-TO-GOVERNMENT ELECTRONIC PROCUREMENT SYSTEM:

The eVA Internet electronic procurement solution streamlines and automates government purchasing activities within the Commonwealth of Virginia. Virginia Tech, and other state agencies and institutions, have been directed by the Governor to maximize the use of this system in the procurement of goods and services. We are, therefore, requesting that your firm register as a trading partner within the eVA system.

There are registration fees and transaction fees involved with the use of eVA. These fees must be considered in the provision of quotes, bids and price proposals offered to Virginia Tech. Failure to register within the eVA system may result in the quote, bid or proposal from your firm being rejected and the award made to another vendor who is registered in the eVA system.

Registration in the eVA system is accomplished on-line. Your firm must provide the necessary information. Please visit the eVA website portal at http://www.eva.virginia.gov/register/vendorreg.htm and register both with eVA and Ariba. This process needs to be completed before Virginia Tech can issue your firm a Purchase Order or contract. If your firm conducts business from multiple geographic locations, please register these locations in your initial registration.

For registration and technical assistance, reference the eVA website at: eVACustomerCare@dgs.virginia.gov, or call 866-289-7367 or 804-371-2525.

V.  CONTRACT PARTICIPATION:

It is the intent of this solicitation and resulting contract to allow for cooperative procurement. Accordingly, any public body, public or private health or educational institutions, or Virginia Tech’s affiliated corporations and/or partnerships may access any resulting contract if authorized by the contractor.

Participation in this cooperative procurement is strictly voluntary. If authorized by the Contractor, the resultant contract may be extended to the entities indicated above to purchase at contract prices in accordance with contract terms. The Contractor shall notify Virginia Tech in writing of any such entities accessing the contract. No modification
of this contract or execution of a separate contract is required to participate. The Contractor will provide semi-annual usage reports for all entities accessing the Contract. Participating entities shall place their own orders directly with the Contractor and shall fully and independently administer their use of the contract to include contractual disputes, invoicing and payments without direct administration from Virginia Tech. Virginia Tech shall not be held liable for any costs or damages incurred by any other participating entity as a result of any authorization by the Contractor to extend the contract. It is understood and agreed that Virginia Tech is not responsible for the acts or omissions of any entity, and will not be considered in default of the contract no matter the circumstances.

Use of this contract does not preclude any participating entity from using other contracts or competitive processes as the need may be.

VI. STATEMENT OF NEEDS:

A. General Services Sought

Virginia Tech seeks a new central e-mail and calendaring solution for their students, faculty and staff. Such solution must achieve the standard of 99.99% availability for all centrally supported services, while providing a rich set of features across a wide range of client platforms, delivering: increased scalability, reliability, availability, and recoverability of e-mail and Calendaring Services. In brief, the successful vendor should provide:

- Integration with Virginia Tech’s existing directory, authentication and authorization systems, and with other campus messaging, scheduling and communications systems;
- Continued implementation and support for standard open protocols;
- Expanded opportunities for collaborative and unified messaging and communications;
- Increased User productivity through integrated scheduling and communications tools;
- A leveraged, long-lasting relationship between Vendor and Virginia Tech.

This RFP is intended to secure all labor, software, and services for proper deployment of this solution. Proposals shall identify all costs, enabling Virginia Tech to accurately assess its expenses. All proposals must be in accordance with the specifications and information contained herein, as well as any addenda. If the Vendor finds any of the system specifications or engineering assumptions outlined in this document in error or unwise, Vendor shall present a persuasive case to the contrary. Installation and Technical Assistance Support for all components are to come directly from Vendor unless otherwise specified by this RFP.

All components specified in any response to this RFP are assumed to have General Availability (GA) status. If any component does not have GA status, Vendor shall so state and clearly identify when and under what condition GA status will be reached. Unless otherwise specified, no Manufacturer Discontinued (MD) products will be considered.

All services provided as part of this RFP must be maintainable by the Vendor under contract. Additionally, Vendor is responsible for specifying and providing service support and upgrades for term of the contract.

SADA Systems:

Acknowledged.

B. Specific Technical Requirements

1. Supported Operating Systems

The following platforms and versions are widely utilized on the campus and as a minimum MUST be supported by the proposed solution:
This proposal valid for 180 days post April 4th, 2011 submission.

2. Supported Native and Web Clients

The following clients and versions are widely utilized on the campus and as a minimum MUST be supported by the proposed solution:

   a) Eudora, Outlook/Outlook Express, Apple e-mail, Entourage, Gnome Evolution, Thunderbird.

   **SADA Systems:**

   One of the benefits of a cloud-based solution is that Google Apps natively supports any client platform (e.g. Windows XP and Vista, Mac OS X, Linux) which supports a modern browser (e.g. Internet Explorer, Firefox, Google Chrome, Safari); this also extends to thin clients.


   Google Apps also supports integration with a wide variety of desktop IMAP clients including:

   - Outlook Express, 2003, 2007 (Windows)
   - Apple Mail 2, 3, 4
   - Windows Mail
   - Thunderbird 2, 3
   - Entourage
   - Eudora
   - Gnome Evolution

3. Supported Web Browsers

User and administration web interfaces MUST be usable via the web browsers commonly used on campus, including as a minimum: Mozilla Foundation Firefox on Microsoft Windows (XP, Vista, and 7), Apple Mac OS X (10.3, 10.4, 10.5 and 10.6), and Linux and Unix clients, Microsoft Internet Explorer 6 and Internet Explorer 7 on Microsoft Windows (XP, Vista and 7), Apple Safari on Apple Mac OS X (10.3, 10.4, 10.5, 10.6), and Google Chrome. Vendor MUST provide support for new OS and Browser versions within 30 days of general availability to the public.

   **SADA Systems:**

   You can use any of these browsers to access Google Apps:

   - Internet Explorer 7.0 and later on Windows
   - Firefox 3.0 and later on Windows, Mac, and Linux
   - Safari 3.0 and later on Mac
   - Google Chrome 4.0 and later on Windows
4. Supported Mobile Devices

The proposed solution MUST support a variety of operating systems: RIM Blackberry, Apple iPhone, Microsoft Windows Mobile, Palm WebOS, Android.

**SADA Systems:**

Google Apps supports the following mobile device operating systems:

- Android
- iPhone
- BlackBerry
- Palm webOS
- Symbian
- Windows Mobile 5
- Windows Mobile 6
- SnapperMail

4a) The proposed solution SHOULD also support IETF and OMA standards-compliant devices as e-mail and calendar clients. Appropriate push and/or pull synchronization, via a desktop client conduit or “over the air” of e-mail, calendar, contact and to-do data MUST be available for mobile devices.

**SADA Systems:**

Google supports synchronization with email and calendar clients using industry best practices and non-proprietary standards. Users are able to Over-the-air (OTA) sync their email, calendar, and contact information via the methods outlined below.

Google Apps aims to provide users with secure, more secure access to information regardless of location or device. Google Apps supports access to Gmail, Google Calendar, Docs, and Contacts from most common types of mobile devices. More information about accessing Google Apps from mobile devices and the specific Apps that can be accessed from each type of device can be found at [http://www.google.com/apps/intl/en/business/mobile.html](http://www.google.com/apps/intl/en/business/mobile.html). Further information regarding specific syncing capabilities is outlined below:

**BES:**

Google Apps Connector for Blackberry Enterprise Server allows for the synchronization of Mail, Calendar and Contacts. For enterprises, Gmail works with BlackBerry Mobile phones through the use of the Google Apps Connector for Blackberry Enterprise Server.

**Features**

- Push email delivery and send Messages sent from and received in your Gmail inbox are automatically pushed to your BlackBerry device within 60 seconds, keeping both inboxes up-to-date.
- Read/delete synchronization Emails read or deleted on your BlackBerry device are marked as read or deleted in your Gmail inbox, and vice-versa.
This proposal valid for 180 days post April 4th, 2011 submission.

- Folder/label synchronization: Select folders on your BlackBerry device to synchronize with labels in your Gmail interface.
- Global address lookup: Search for and access email addresses and phone numbers for other users on your company domain.
- Calendar access: View your Google Calendar events and schedule from the native BlackBerry application, with two-way synchronization from your Google Calendar to BlackBerry device.
- Contacts synchronization: Contacts in your BlackBerry address book and in your Gmail account are automatically synchronized. Information added to Gmail is pushed to your BlackBerry device within 5 minutes, and vice-versa.
- Hosting Support: Support multiple Google Apps domains on a single BlackBerry Enterprise Server. This enables our partners to offer hosted services for supporting BlackBerry devices by sharing a single BlackBerry Enterprise Server across multiple Google Apps customers.
- Availability: Google Apps Connector for BlackBerry Enterprise Server is available at no charge to Google Apps Premier and Google Apps Education Edition customers.

Google Sync for iPhone, iPad, iPod Touch and Windows Mobile:

Google Sync lets your users synchronize their mail, contacts and calendars to their mobile devices. This means that your users will have access (viewing and editing) to their inbox, address books and calendar events at any time. They can also get alerts (sound or vibration) for upcoming meetings and incoming messages. Google Sync works for both iPhone and Windows Mobile devices. These services are still in beta. Google Sync offers two-way synchronization between your calendar, contacts and email on a myriad of mobile devices. Updates are done automatically. Whether you update appointments and contacts from your mobile device or from your computer, you always have access to up-to-date information. Google Sync also offers controls for administrators to help ensure corporate policy enforcement across a range of mobile devices.

Android:

On some Android-powered devices, Google applications, such as Gmail, Google Calendar, Google Talk and Contacts come pre-installed. Access these apps by tapping their icons. When setting up the phone, make sure to log in using the username and password for your domain, and your content will be automatically synced on the go. Gmail, Google Calendar and Google Docs in the mobile browser are also available in a single, streamlined web interface, where you can seamlessly switch between applications. Bookmark http://www.google.com/m/a/example.com from your browser and add a shortcut icon to your homescreen by long-pressing and selecting the 'shortcut' then 'bookmark' options. But don't forget, you'll have to replace "example.com" with your actual domain name.

Palm webOS:

Instructions on configuring a Palm webOS device to access Gmail can be found at https://mail.google.com/support/bin/answer.py?hl=en&answer=150695.

5. Supported Protocols

The solution MUST comply with the following standards. In the case of IETF RFCs, “comply” means that the solution adheres to all requirements declared “MUST”, “REQUIRED”, “SHALL”, “MUST NOT” or “SHALL NOT”. Please note where the solution also complies with RFC requirements declared “SHOULD”, “RECOMMENDED”, “SHOULD NOT”, “NOT RECOMMENDED”.

a) IETF RFC 2426 - vCard MIME Directory Profile
**SADA Systems:**

Complies. Google builds the product using industry best practices and non-proprietary standards. You can import vCard files from applications like Outlook and Mac Address Book. Instructions can be found at http://mail.google.com/support/bin/answer.py?hl=en&answer=183711.

**b)** IETF RFC 2445 - Internet Calendaring and Scheduling Core Object Specification

**SADA Systems:**

Complies.

**c)** IETF RFC 2446 - iCalendar Transport-Independent Interoperability Protocol (iTIP) Scheduling Events, Busy Time, To-dos and Journal Entries

**SADA Systems:**

Complies. Google supports iCalendar data exchange with industry best practices and non-proprietary standards.

**d)** IETF RFC 2447 - iCalendar Message-Based Interoperability Protocol (iMIP)

**SADA Systems:**

Complies. Google supports iCalendar data exchange with industry best practices and non-proprietary standards.

**e)** IETF RFC 4791 - CalDAV support an extension to the HTTP and WebDAV protocols to enable interoperable distributed calendaring and scheduling

**SADA Systems:**


**f)** IETF RFC 2821 - Simple E-mail Transport Protocol

**SADA Systems:**

Complies.

**g)** IETF RFC 2822 - Internet Message Format

**SADA Systems:**

Complies.

**h)** IETF RFC 3207 - SMTP Service Extension for Secure SMTP over Transport Layer Security

**SADA Systems:**

Complies. Google supports SMTP over TLS with industry best practices and non-proprietary standards.

**i)** IETF RFC 3501 - Internet Message Access Protocol - Version 4rev1
**SADA Systems:**

Complies. Google supports IMAP with industry best practices and non-proprietary standards.


**SADA Systems:**

Complies. Google has the ability to interact with any standard LDAP (including Microsoft Active Directory, Lotus Domino, and most generic Open LDAP servers) using our Google Apps Directory Sync tool. The Google Apps Directory Sync tool has read-only ability when interacting with an LDAP, so data in the LDAP will be maintained. More information about Google Apps Directory Sync can be found at [http://www.google.com/support/a/bin/answer.py?hl=en&answer=106368](http://www.google.com/support/a/bin/answer.py?hl=en&answer=106368).

* IETF RFC 4752 - The Kerberos V5 ("GSSAPI") Simple Authentication and Security Layer (SASL) Mechanism
* Internet E-mail Consortium, "vCard - The Electronic Business Card Version 2.1", OMA SyncML ADA Section 508

**SADA Systems:**

Complies. Google integrates via SAML to the institution's SSO, which then would integrate directly with Kerberos within the University's identity management system.

Security Assertion Markup Language (SAML) is an XML standard that allows secure web domains to exchange user authentication and authorization data. Using SAML, an online service provider can contact a separate online identity provider to authenticate users who are trying to access secure content.

Google Apps offers a SAML-based Single Sign-On (SSO) service that provides partner companies with full control over the authorization and authentication of hosted user accounts that can access web-based applications like Gmail or Google Calendar. Using the SAML model, Google acts as the service provider and provides services such as Gmail and Start Pages. Google partners act as identity providers and control usernames, passwords and other information used to identify, authenticate and authorize users for web applications that Google hosts. There are a number of existing open source and commercial identity provider solutions that can help you implement SSO with Google Apps.

The Google Apps SSO service is based on the SAML v2.0 specifications. SAML v2.0 is supported by several widely known vendors. For more information on SAML support for your SSO and Kerberos System, please visit: [http://code.google.com/googleapps/domain/sso/saml_reference_implementation.html](http://code.google.com/googleapps/domain/sso/saml_reference_implementation.html)

6. Provisioning/Deprovisioning

Solution MUST provide an Application Programming Interface (API) allowing Virginia Tech to provision, deprovision, rename, suspend, unsuspend and adjust settings of individual User accounts

**SADA Systems:**

This is possible through the use of the Google Apps Directory Sync Tool or the Provisioning API.

Virginia Tech can use the Provisioning API to automate account and mailbox creation. The same API allows for renaming usernames. More info on the Provisioning API here: [http://code.google.com/googleapps/domain/gdata_provisioning_api_v2.0_reference.html](http://code.google.com/googleapps/domain/gdata_provisioning_api_v2.0_reference.html)
7. Support for Emergency Notification E-mailings

In the event of an emergency, the system SHOULD permit the broadcasting of e-mail by authorized Users to an entire campus population or to select subgroups. Appropriate infrastructure SHOULD be provided as part of the proposed solution to ensure that that messages sent as part of a designated Emergency Notification are guaranteed to be received in individual User e-mailboxes within five (5) minutes of transmission. A simple interface SHOULD provide authorized Users the option to select Emergency Notification recipients from among a series of pre-defined groupings (or dynamically provisioned groups based on LDAP characteristics). Proof of receipt or logs documenting transmission to each recipient SHOULD be provided for each Emergency Notification e-mailing.

**SADA Systems:**

Gmail allows the sending of mass emails within the domain. Senders are limited to only 2000 messages per day external to the domain, to prevent spam and prevent abuse per this article: [http://mail.google.com/support/bin/answer.py?answer=22839](http://mail.google.com/support/bin/answer.py?answer=22839)

Mass message sending can be handled via creating a group in Google Groups that includes all vt.edu email users or selected subgroups. Sending messages to be distributed to this group can be restricted to specific individuals. A custom footer for all messages sent from this group can be specified per this article: [http://groups.google.com/support/bin/answer.py?hl=en&answer=4637](http://groups.google.com/support/bin/answer.py?hl=en&answer=4637)

8. Data Center Location

Virginia Tech data stored by the solution SHOULD be maintained in data centers situated in the continental United States, Alaska, or Hawaii.

**SADA Systems:**

Your data will be stored in Google's network of data centers. Google maintains a number of geographically distributed data centers throughout the world, the locations of which are kept discreet for security purposes. Google's computing clusters are designed with resiliency and redundancy in mind, eliminating any single point of failure and minimizing the impact of common equipment failures and environmental risks.

9. E-discovery and Data Preservation

Solution SHOULD provide an Application Programming Interface (API) allowing Virginia Tech to search, access, and download individual User E-mail data without requiring the knowledge of, or changing, the User password.

**SADA Systems:**

The Google Apps Audit API allows Google Apps administrators to audit a user's email, email drafts, and archived chats. In addition, a domain administrator can retrieve account login information and download a user's mailbox.

[http://code.google.com/googleapps/domain/audit/docs/1.0/audit_developers_guide_protocol.html](http://code.google.com/googleapps/domain/audit/docs/1.0/audit_developers_guide_protocol.html)

10. Collaboration

   a) Solution SHOULD provide ability to share data and files stored within the solution;
**SADA Systems:**

The ability to share data and files is fundamental to Google Apps. Google Docs allows users to share materials with colleagues easily and efficiently. You may share both Google-specific docs as well as traditional office documents, and additionally, just about any file type.

b) Solution SHOULD provide ability to have multiple Users work on common files at the same time from different or separate work groups or locations;

**SADA Systems:**

Google Docs is a fully-featured suite of office productivity tools that provide a real-time, simultaneous editing experience for multiple users collaborating on documents, spreadsheets, or a presentations. Collaborators accesses the same online copy of the file in Google Docs, so there are no attachment compatibility problems, inbox storage quota issues, or versions to reconcile. When the group is done editing, the file can be stored in Google Docs, or exported back to the original format.

Google Sites is included with Google Apps and provides Wiki-like capability to your users. Changes, by user, are tracked automatically. Effective collaboration has become a key driver to improve team productivity. Project teams, often located across disparate locations and time zones, produce and distribute content in different formats and platforms. Teams need to consolidate relevant information in one place that's easy to navigate. Contributors and reviewers have specific needs to manage the creative process, maintain the project plan and keep all stakeholders informed.

c) Solution SHOULD provide ability to collaborate with Users that are telecommuting or otherwise away from campus;

**SADA Systems:**

Google Apps allows local, remote and offsite users to have the ability to collaborate with one another just as effectively as they can when on site. In addition, instead of consuming bandwidth through a corporate Internet link, mobile or telecommuting users only use their own local Internet connection.

d) Solution SHOULD provide a Wiki-type solution for collaboration that allows changes to be tracked by User; and

**SADA Systems:**

With Google Doc users can collaborate on a document with other users online in real-time without sending attachments back-and-forth and without requiring expensive client applications. Google Apps maintains a running version history of each edit, each editor, and when the file was edited. These common files can be shared in real time with multiple users allowing them to collaborate while maintaining a continuous, running revision history of all the changes to the files starting with the very first edit. The version control gives users the ability to literally step back through every change in the file by author or time, and restore a previous version, if necessary.

e) Solution SHOULD provide ability to maintain version control (i.e., who, what, when).

**SADA Systems:**

Google Docs gives users version control ability to literally step back through every change in the file by author or time, and restore a previous version, if necessary.
11. Instant Messaging

a) Solution SHOULD have the capability to provide instant messaging capabilities for internal Users and with external (non-campus) Users.

**SADA Systems:**

Google Chat supports the ability to chat across internal and external domains.

12. Video Conferencing

a) Solution SHOULD provide ability to support one-to-one internal videoconferences;

**SADA Systems:**

Video and voice are built into the Google Chat applications.

b) Solution SHOULD provide ability to support external video conferencing participants;

**SADA Systems:**

Administrators may choose to restrict video chat to users in the same domain or to allow chat to external users.

c) Solution MAY provide ability to support multiple locations internally;

**SADA Systems:**

Video chat capabilities are available for all users of Google Apps, provided they have the necessary equipment to engage in video communications.

d) Solution MAY provide ability to use saved video files within office productivity tools;

**SADA Systems:**

Saved video files can be linked from the Google Apps office productivity tools, and embedded directly in presentations and blogs.

e) Solution MAY provide a Real-time on-screen notation

**SADA Systems:**

Google Apps allows users to create a Google Doc that can be edited while a video chat is occurring, thereby allowing one or multiple users to

f) Solution MAY provide a Remote Desktop Access/Control within video conferencing solution

**SADA Systems:**

Google Apps does not allow Remote Desktop Access at this time.

C. Technical Discovery

1. Data Stewardship
Many individuals at Virginia Tech have been early adopters of cloud-based (often free) solutions to e-mail, calendaring, and collaboration tools. However, license terms associated with those cloud-based solutions do not necessarily address the complex issues of data stewardship as they relate to students, and especially to faculty and staff (e.g., issues of ownership and use of Customer and End User data, system and data security, and e-Discovery, to name a few).

**a)** Please describe the measures your organization and personnel will take to ensure that all data - message headers, contents, calendar events, contacts, logs and any personally identifiable information - received, stored, sent or tracked by or for Users of Virginia Tech remains the property of contracting institution and/or their Users. Please provide a copy of all related policies and procedures.

**SADA Systems:**

To put it simply, Google does not own your data. Google does not take a position on whether the data belongs to the institution signing up for Apps, or the individual user.

The data which you put into our systems is yours, and Google believes it should stay that way. Google thinks that means three key things.

1. Google will not share your data with others except as noted in our Privacy Policy (http://www.google.com/privacy/privacy-policy.html).
2. Google keeps your data as long as we require us to keep it.
3. Finally, you should be able to take your data with you if you choose to use external services in conjunction with Google Apps or stop using our services altogether (http://www.google.com/support/a/bin/answer.py?hl=en&answer=100458).

**b)** System Security and Data Protection. Please describe the measures your organization and personnel will take to ensure that all activities under this Agreement are performed in a sufficiently secure manner to protect against reasonably anticipated threats or hazards to the privacy, security, and integrity of Customer and End User Data, and to prevent unauthorized access to or use or alteration of those data. In particular:

1. **What is your operating system and application vulnerability testing and patching methodology and frequency to ensure the system, application, and associated tools/protocols/utilities are kept up to date with all relevant security patches?**

**SADA Systems:**

Google runs its data centers using custom hardware running a custom OS and filesystem. Each of these systems has been optimized for security and performance. The Google Security Team is working with external parties to constantly test and enhance security infrastructure to ensure it is impervious to external attackers. And because Google controls the entire stack running our systems, we are able to quickly respond to any threats or weaknesses that may emerge.

2. **Do the servers employ a network- and/or host-based intrusion prevention system, and if so provide details? Describe all other network- and host-based firewalls, security appliances, and/or similar defenses in place to help ensure Customer data confidentiality and integrity, as well as availability of the services provided to the Customer under this Agreement.**

**SADA Systems:**

Firewalls and Intrusion Detection.
Google employs multiple layers of network devices and intrusion detection to ensure that our external attack surface is protected.

Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Many companies make extensive use of third-party technologies (e.g., Network Intrusion Detection Systems - NIDS, Host-based Intrusion Detection Systems - HIDS) to look for known attacks against commonly-installed software, and Security Operations Centers (SOCs) to respond when they arise. We take a different approach by:

- Tightly controlling the size and make-up of our attack surface through preventative measures;
- Employing intelligent detect controls at data entry points; and
- Employing technologies that automatically remedy dangerous situations.

Most of our Internet-exposed attack surface is comprised of Google-created software and the environment involves a large number of servers. Traditional IDS products are not economical, efficient or useful in these situations and we rely on smarter methods of detecting exploitation.

When we approach intrusion detection concepts, we break down our attack surface according to anticipated input vectors (i.e., how hackers will attempt to break in). Google’s hosting infrastructure is custom-built so we have the ability to tightly define our perimeter and the entrance points into our network. The major areas of coverage that achieve the goals above are as follows:

- As mentioned previously, the OS on every system is stripped down, modified, and hardened to minimize third party vulnerabilities on running systems;
- All IP traffic is routed through custom front end servers that detect and stop malicious requests;
- Traffic is examined for exploitation of programming errors via methods such as cross-site scripting, and high priority alerts are generated when such an exploit is found;
- To prevent buffer overflow attacks, all open source software that is Internet facing or that processes external data goes through several levels of code review, audit, and modification before allowed into production. All changes are contributed back to the open source community.
- Systems are checked continually for binary modifications, and any unrecognized modifications are purged;
- Router ACLs are used to provide perimeter defense, and an internally routable IP space is used to make sure external connections are never made to internal systems;
- Layer 3 filtering is used to mitigate packet-level attacks. Google, an established provider of web-based services has gone to great lengths to protect against threats. Google runs its data centers using custom hardware running a custom OS and filesystem. Each of these systems has been optimized for security and performance. The Google Security Team is working with external parties to constantly test and enhance security infrastructure to ensure it is impervious to external attackers. And because Google controls the entire stack running our systems, we are able to quickly respond to any threats or weaknesses that may emerge.

Data is chunked and replicated over multiple systems, so that no one system is a single point of failure. There are "virtual" firewalls protecting one user’s data from another user’s data. A user has to authenticate to unlock their access to their data. Data from one domain is not available via another domain. To compromise Google’s data, a malicious individual or hacker would need to
know the specific systems that house the target data and would need to attack all of them to compromise a single user’s information.

Google believes its security model is much more secure than tradition, on-premise based systems for these reasons.

3) Do the servers use clear-text passwords for any reason? (E.g., including SMTP authentication or remote login)

SADA Systems:

Google servers do not use clear-text passwords. The layers of the Google application and storage stack require that requests coming from other components are authenticated and authorized. Service-to-service authentication is based on a security protocol that relies on a Google system to broker authenticated channels between application services. Trust between instances of this authentication broker is derived from x509 host certificates that are issued to each Google production host by a Google-internal certificate authority.

For example, a Gmail web front-end service would make a remote procedure call to a Gmail back-end service to request a message from a particular user’s Inbox. The Gmail back-end would authenticate and process this request only if the requester is indeed a service running under a service identity that is allowed to access all back-ends. The Gmail back-end would in turn authenticate in order to access files in the Google distributed file system, and if successful, would only be granted access in accordance with file access control lists (ACLs).

Also, data for end user authentication and API calls are transferred via HTTPS.

4) Do the servers run any network services that are unrelated to and unnecessary for delivery of the services provided to the Customer under this Agreement? (If so, please specify.)

SADA Systems:

No, only authorized network services that are required for the delivery of Google Apps services are permitted. Unauthorized packets are automatically dropped.

5) Will data be encrypted during transmission between the server(s) and the web interface and/or native clients (see Section VI.B.)? Will data be encrypted at rest on the server? (In each case, specify encryption mechanisms and bit lengths)

SADA Systems:

All Google Apps services provide the ability to access all data using encryption and customers can choose to require this option for their users. This helps ensure that no one except the user has access to his or her data. This is true for access to our mail, calendar, video, and chat data via our web applications. The mobile email client also uses encrypted access to ensure the privacy of communications. We do not offer encryption on the Start Page service at this time. We also require encryption for access to your mail data by third party clients.

SSL (Secure Sockets Layer) is a protocol that provides secure communications on the Internet for such things as web browsing, e-mail, instant messaging and other data transfers. If you enable SSL connections, Google will force HTTPS (Hypertext Transfer Protocol Secure) when your users access most services in Google Apps. SSL varies by service and is available for email, chat, calendar, docs, and sites.
In order to build a performance-oriented cloud offering while at the same time provide robust
security for data at rest, Google chose not to encrypt Apps data in the traditional sense. Rather,
Google Apps data (e.g., each individual email message and file) is "chunked" and distributed over
multiple servers/disks such that no one server/disk contains a data element in its entirety. Data
chunks are given random 64-bit names and are not stored in clear text so they are not humanly
readable. This storage design makes it very difficult to attack a specific user or any one customer's
data, as it is intermingled with millions of other user's data in a non-human readable form.

The best analogy to our data "obfuscation" approach is to imagine that each email message or file
is put through a paper shredder (chunked), each shred is dipped in dark colored ink (non-readable),
and subsequently all shreds are scattered across all waste baskets throughout all office buildings in
lower Manhattan (distributed).

(6) Do your physical security controls include video monitoring, restricted access areas, mantraps,
card access controls, or similar controls?

**SADA Systems:**

Google data centers employ electronic card key and biometric access control system that are linked
to a system alarm. The access control system monitors and records individuals' access to perimeter
doors, shipping/receiving, the raised floor, and other critical areas. Unauthorized activity and failed
access attempts are logged by the access control system, investigated as appropriate, and reported
to the security manager. The security manager reviews and approves these reports. Authorized
access throughout the business operations and data centers is restricted based on zones and
individuals' job responsibilities.

All entrants to the data centers must pass through a mantrap. The mantrap is designed to
physically limit access to one person at a time (floor sensors and automatic 180 degree turnstile)
and prohibits the “handing off” of a badge back to a secondary person.

The fire doors at the data centers are alarmed and can only be opened from the inside. The fire
doors are fitted with push bars [redacted] there is a specified delay on the push bar unless a fire
alarm has been activated. If a person tries to exit the building through a fire door without a fire
alarm having been triggered, an alarm would register in the security operations center.

CCTV cameras are in operation both inside and outside the data centers. The positioning of the
cameras has been designed to cover strategic areas including, among others, the perimeter, doors
to the data center building, shipping/receiving and the raised floor.

Security operations personnel manage the CCTV monitoring, recording and control equipment. The
CCTV equipment is connected by secure cables throughout the data centers. Cameras record on
site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained
for 60-90 days based on activity.

(7) Do you conduct regular internal security tests and/or audits (including vulnerability scanning,
application security assessment scanning, and penetration testing) conducted by personnel or
contractors with appropriate expertise? Please describe. Has your system ever undergone a SAS 70
Type II audit, and if so, are you willing to provide your customers with access to the results?

**SADA Systems:**
Google uses a combination of well-known third-party and proprietary tools to scan its external perimeter on a quarterly basis for network vulnerabilities and configuration errors; these tools are also applied internally on systems containing highly sensitive information. Google undergoes annual third-party penetration testing by a qualified vendor for both its external networks and financial-related applications.

Google has obtained SAS 70 Type II audit for Google Apps, conducted by Grant Thornton LLP, a firm with which Google had no prior relationship. The Google Apps SAS 70 Type II has far more controls and we have added new controls over time. Google engages an external auditor annually to review the confidentiality, integrity and availability controls that are in place for Google Apps. A summary of our SAS 70 report may be made available for review on a restricted basis, upon request, and under NDA. A full SAS 70 report is available after a Services Contract is in place, again on a restricted basis under NDA (additional Terms and Conditions may apply).

More information on security in Google Apps is available here: http://googleenterprise.blogspot.com/2010/06/security-first-protecting-your-data_04.html

(8) Will we be notified of major changes to your environment that could affect our security posture, and if so, how?

SADA Systems:

Google is committed to transparency, accountability, and maintaining your trust. Google often discloses security breaches, but does not have a blanket policy to do so. All of the information on security incidents may be found here:

http://googleonlinesecurity.blogspot.com/

If there is a security breach of the clients data, or a suspected security breach, Google will respond in the most expedient time possible under the circumstances, without unreasonable delay, consistent with the legitimate needs of applicable law enforcement, and after taking any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. Events that directly impact customers are treated with the highest priority. An individual or team is dedicated to remediating the problem and enlisting the help of product and subject experts as appropriate. Other responsibilities are deferred until the issue is resolved.

Google’s security incident management program is structured around the NIST guidance on handling incidents (NIST SP800-51). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities.

For more information on these and other risk mitigation measures, see the Google Apps Messaging and Collaboration Security Whitepaper:


c) Data Retention. Describe how your solution will ensure retention of data or records in an End User’s account, including attachments, until the End User deletes them or for an alternative time period mutually agreed by the parties. Specifically:
(1) Describe your plan for backup and restoration of system data, including standard backup retention periods, multiple copies of data, and procedures for processing data for long-term archiving. Please describe how Individual Users and administrators will be able to easily restore individual e-mailboxes from your backups.

**SADA Systems:**

Google Apps Education Edition allows users to exclusively govern when data is deleted. Email retention settings are not available for the purpose of establishing a corporate-wide policy on retention. However, complementary archiving capabilities (for extended retention) are available with the Google Message Discovery (GMD) add-on service.

The Google Apps RPO design target is zero, and the RTO design target is instant failover. Google's uptime service-level agreement is 99.9% calculated monthly, which equates to a total downtime of well under an hour per month.

Google achieves this through live or synchronous replication: every action a user takes in Gmail is simultaneously replicated in two data centers at once, so that if one data center fails, Google nearly instantly transfer the user's data over to the other one that's also been reflecting their actions.

These data center will be in different geographic disaster zones. Our Data Centers are redundant and can shift to a user’s secondary data center. To minimize service interruption due to hardware failure, natural disaster, or other catastrophe, Google implemented comprehensive disaster recovery program at all of its data centers. This program includes multiple components to eliminate single point-of-failure, including the following:

- Distributed data center architecture Google operates a geographically distributed set of datacenters ensure swift failover. Management of the data centers is also distributed to provide location-independent, around-the-clock coverage, and system administration.

- Data replication and backup To help ensure availability in the event of a disaster, all of the client’s data is replicated to separate systems in different data centers.

If a disaster occurred that effected one data center, the client’s data will be served from the secondary data center. The data between a user’s primary data center and their secondary data center is constantly replicated in “real time”.

There is nothing that Virginia Tech or a Virginia Tech user needs to do to act upon to invoke this. We have built monitoring tools that help look for a malfunction or even slowness in a data center and automatically, push users to their secondary data center. The only requirement is that client still have internet access.

In addition to the redundancy of data and no single point of failure model for our data centers We have also have a business continuity plan for our corporate office in Mountain View, CA. We have a plan that accounts for having suffered a major calamity, and people and services in are unavailable for 30+ days. This plan insures continued operations or our services to our customers.

And it's not just to preserve your Gmail accounts. Organizations get the same level of data replication for all the other major applications in the Apps suite: Google Calendar, Google Docs, and Google Sites.
The most up-to-date and detailed description of the SLA are available at http://www.google.com/apps/intl/en/terms/sla.html

(2) Is archiving configurable both on a per User and per group basis? Can data be archived based on content, sender, recipient, and/or other metadata with different archival periods per institutional policy or legal requirements? Can e-mail administrators view and perform all normal e-mail functions on archived e-mail without having to restore?

**SADA Systems:**

The Google Message Discovery (GMD) add-on archiving service allows you to group users into organization containers where each container may have a different email retention policy in the separate archive store. A user may only belong to one organization in the service but an organization may have a single user, allowing for maximum flexibility. All of that user's email (regardless of content or addresses/senders) will be subject to the same retention policy. All message parts are indexed for use in e-discovery searches. Messages that match a set of search criteria may have a hold record placed on them to override and extend the retention period as you deem appropriate.

Google Message Discovery (GMD) captures email as it is being sent and received which is before the email system would have an end-user attribute such as a label attached to it. An authorized administrator would be able to search and view the responsive email content in the archive system, name the saved search results and apply a litigation hold on that search set which would override the system retention period for as long as the hold record exists. The search results can be exported from the archive system in a PST or MBox file format.

(3) Describe your method of securely destroying all deleted data and/or expired backups at the end of that time period and at Customer’s election.

**SADA Systems:**

After a Google Apps user or Google Apps administrator deletes a message, account, user, or domain, and confirms deletion of that item (e.g., empties the Trash), the data in question is removed and no longer accessible from that user’s Google Apps interface. The data is then deleted from Google’s active servers and replication servers. Pointers to the data on Google’s active and replication servers are removed. De-referenced data will be overwritten with other customer data over time.

When retired from Google’s systems, disks containing customer information are subjected to a data destruction process before leaving Google’s premises:

(1) Policy requires the disk to be logically wiped by authorized individuals. The erasure consists of a full write of the drive with all zeroes (0x00) followed by a full read of the drive to ensure that the drive is blank.

(2) Another authorized individual is required to perform a second inspection to confirm that the disk has been successfully wiped. These erase results are logged by the drive’s serial number for tracking.

(3) The erased drive is released to inventory for reuse and redeployment. If the drive cannot be erased due to hardware failure, it must be securely stored until it can be destroyed. Each facility is audited on a weekly basis to monitor compliance with the disk erase policy.
(4) Describe your procedures for responding to Customer’s e-discovery needs and responsibilities, including where customer indicates that certain records may be relevant to litigation that Customer reasonably anticipates. Describe your capability to place an immediate “hold” on the destruction of Customer or End User records that might otherwise occur under routine records destruction schedules. Discuss whether e-mail administrators will be able to retrieve or view archived e-Discovery data based on content, sender, recipient, and/or other metadata with different archival periods? Describe the formats in which e-mail administrators can export archived e-Discovery data. (See Special Term 27d)

**SADA Systems:**

Google Message Discovery (GMD) includes the following search panels into which administrators can enter criteria to retrieve archived messages:

- Email Search panel: provides fields that let administrators enter criteria to find archived email messages by sender, recipient, "has attachment", body, data range search, match all or any included or excluded word combination.
- Boolean Search panel: lets administrators enter their own query strings, using the Apache Lucerne query syntax. This syntax supports Boolean operators, wildcards, fuzzy matches, and proximity matches, allowing users to create more-complex or targeted search queries.

Administrators can set up investigat[masked] and organize their search criteria and results, so they don't have to redo them later on. Searches may be span multiple inboxes or be restricted to a single sender or recipient.

Google also provides an audit API at no additional charge. The Google Apps Audit API allows Google Apps administrators to audit a user's email, email drafts, and archived chats. In addition, a domain administrator can retrieve account login information and download a user’s mailbox.

(5) Can the proposed solution be implemented such that all storage of Customer and End User data remain within the United States? If not, where will Vendor store data and what security measures does Vendor have in place in those locations?

**SADA Systems:**

Your data will be stored in Google's network of data centers. Google maintains a number of geographically distributed data centers, the locations of which are kept discreet for security purposes. Google’s computing clusters are designed with resiliency and redundancy in mind, eliminating any single point of failure and minimizing the impact of common equipment failures and environmental risks.

Access to data centers is very limited to only authorized select Google personnel.

2. System Logging and Data Integrity

Please describe the measures your organization and personnel will take to ensure that you retain, and can provide to Customer on request, logs necessary for the investigation of security incidents and/or to address data integrity concerns, including describing:

- Your data retention policy for authentication and other relevant system logs; what is the process and lead-time for providing access in response to a request by Customer’s authorized infrastructure and security personnel? (E.g., authentication logs maintained for 90 days and accessible with 24 hours
SADA Systems:

System logs are maintained for an appropriate period of time and are reviewed on an as-needed basis. For example, on our consumer and enterprise services, we anonymize users’ IP addresses in our server logs after nine months, but retain the anonymized logs indefinitely. From an internal perspective, logs are stored for a period of time considered to be useful to investigate a security incident that may be discovered in the future.

To support customer requests for information regarding their Google Apps domain accounts, the Reporting API is available for on-demand reporting. If a customer has a data request beyond the scope of the Reporting API, the customer may open a case with Google Support and document the request/rationale. The availability and associated provisioning time for the requested information may only be assessed on a case-by-case basis.

Greater customer control over tracking/auditing system access may be achieved through an external authentication server which communicates with Google Apps via the open SAML 2.0 standard for “single sign-on” (SSO).

b) The requirements necessary to implement logging and monitoring on the system and how does the system log security/authorization changes as well as User and administrator security events (e.g., login failures, access denied, changes accepted)?

SADA Systems:

Google Apps includes logging capabilities as part of the core product suite for account monitoring purposes. Google Apps Administrators may download an encrypted file of a domain account and log-in information for audit purposes using the Audit API. This type of extract includes time-stamp, event, and IP address. Complete documentation on the Audit API is found here:

http://code.google.com/googleapps/domain/audit/docs/1.0/audit_developers_guide_protocol.html

More granular tracking/auditing of security and authorization changes as well as user administration and security events may be achieved through an external authentication server which communicates with Google Apps via the open SAML 2.0 standard for “single sign-on” (SSO).

While a SAML SSO solution may also be used to extend alerts to a customer’s security team for monitoring purposes, note that Google also provides security warnings direct to the end-user when suspicious activity is detected. For example, Gmail displays a warning to users in the form of a banner message that states "Warning: We believe your account was last accessed from…[location and IP address]" to indicate location/geographic region where the account was accessed when unusual activity is detected. If you always log in from the same country and suddenly there is a log-in from halfway around the world, that would qualify as suspicious. After receiving the warning banner, users may click a "Details" link to obtain more information and may reset their password from that window.

c) Whether the services generate or support an audit trail for each User and type of usage? Do available audit logs include login, logout, action performed and source IP address?

SADA Systems:
When you use Gmail, Google's servers automatically record certain information about your use of Gmail. Similar to other web services, Google records information such as account activity (including storage usage, number of log-ins), data accessed or clicked on (including UI elements, ads, links); and other log information (including browser type, IP-address, date and time of access, cookie ID, and referrer URL).

d) The system capability to log security/authorization changes as well as User and administrator security events (e.g., login failures, access denied, changes accepted), and all requirements necessary to implement logging and monitoring on the system.

**SADA Systems:**

Google Apps includes logging capabilities as part of the core product suite for account monitoring purposes. Google Apps Administrators may download an encrypted file of a domain account and log-in information for audit purposes using the Audit API. This type of extract includes time-stamp, event, and IP address. Complete documentation on the Audit API is found here:

[http://code.google.com/googleapps/domain/audit/docs/1.0/audit_developers_guide_protocol.html](http://code.google.com/googleapps/domain/audit/docs/1.0/audit_developers_guide_protocol.html)

More granular tracking/auditing of security and authorization changes as well as user administration and security events may be achieved through an external authentication server which communicates with Google Apps via the open SAML standard for “single sign-on” (SSO).

While a SAML SSO solution may also be used to extend alerts to a customer's security team for monitoring purposes, note that Google also provides security warnings direct to the end-user when suspicious activity is detected. For example, Gmail displays a warning to users in the form of a banner message that states "Warning: We believe your account was last accessed from [location and IP address]" to indicate location/geographic region where the account was accessed when unusual activity is detected. If you always log in from the same country and suddenly there is a log-in from halfway around the world, that would qualify as suspicious. After receiving the warning banner, users may click a "Details" link to obtain more information and may reset their password from that window.

e) How your solution protects Customer and End User Data against deterioration or degradation of data quality and authenticity? Do you perform regular data integrity audits, and if so, with what frequency?

**SADA Systems:**

The Google cloud infrastructure demonstrates the qualities essential for supporting large-scale data processing workloads on commodity hardware. Our system protects customer and end-user data against deterioration or degradation of data quality and authenticity through constant monitoring, replicating crucial data, and fast and automatic recovery. Replication (six copies of data at any given time spread over a minimum of two data centers) allows us to tolerate server/disk failures. The frequency of these failures motivated a novel online repair mechanism that regularly and transparently audits/repairs the damage and compensates for lost replicas in real-time.

Automated data integrity audits are performed continuously using checksumming to detect corruption of stored data. Each server independently verifies the integrity of its own copy of data by maintaining checksums. Checksums are stored persistently with logging, separate from user data. Servers verify the checksum of data blocks before returning any data, thereby ensuring corruption will not propagate to other machines. If a block does not match the recorded checksum, the server returns an error to the requestor and reports the mismatch to the master. In response, the requestor will read from other
replicas, while the master will clone the data from another replica. After a valid new replica is in place, the master instructs the server that reported the mismatch to delete its replica.

3. Data Security and Breach Notification

Please describe the measures the organization and personnel take to mitigate risk and/or notify Users of data exposure, including describing:

   a) How the organization and its personnel ensure the prompt discovery and response to publicly known software bugs or other security threats that may expose Customer and End User Data to risk of unauthorized access, alteration, or use.

   SADA Systems:

   The Google Security Team actively scans for security threats using commercial tools, intensive automated and manual penetration efforts, quality assurance (QA) processes, software security reviews, and external audits. Google’s Vulnerability Management team monitors mailing lists, vendor errata notices, blogs, etc to identify when new security vulnerabilities and fixes are necessary. They also ensure that appropriate administrators are applying security fixes to their systems and have the resources they need to do so.

   Google employs a number of approaches to further reduce the incidence of implementation-level security vulnerabilities in its products and services:

   - Implementation-level security reviews: Conducted by members of the Google Security Team, typically in later stages of product development, implementation-level security reviews aim to validate that a software artifact has indeed been developed to be robust against relevant security threats. Such reviews typically consist of a re-evaluation of threats and countermeasures identified during security design review, targeted security reviews of security-critical code, selective code reviews to assess code quality from a security perspective, and targeted security testing.

   - Automated testing for flaws in certain relevant vulnerability classes. We use both in-house developed tools and some commercially available tools for this testing.

   - Security testing performed by Software Quality Engineers in the context of the project’s overall software quality assessment and testing efforts.

   - Google maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at http://www.google.com/intl/en/corporate/security.html

   b) All security breaches involving Customer and End User Data that you have experienced within the last 2 years, and your response including what steps you have taken to minimize the likelihood of recurrence.

   SADA Systems:

   Google is committed to transparency, accountability, and maintaining your trust. Google often discloses security breaches, but does not have a blanket policy to do so. All of the information on security incidents may be found here:

   http://googleonlinesecurity.blogspot.com/
This proposal valid for 180 days post April 4th, 2011 submission.

26

RFP #0016512

C) The process whereby Customer is notified in the event of any security breaches or exposure of End User Data, and the process Vendor will utilize to inform to such End Users of said breach. (See Special Term 26a)

**SADA Systems:**

Google complies with all laws and regulations including applicable security breach notification law. Google will notify Virginia Tech of a security breach, following the discovery or notification of such security breach, in the most expedient time possible under the circumstances, without unreasonable delay, consistent with the legitimate needs of applicable law enforcement, and after taking any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

d) The facilities available in the system to provide separation of duties between security administration and system administration functions.

**SADA Systems:**

The Google Apps Control Panel (CPanel) is used to perform administrative functions and set security policy. While enhancements to the native CPanel will provide separation of security and system administration functions in the future, solutions are available today from the Google Apps Marketplace that provide role-based security and management tasks. Through the Google Apps Marketplace, software vendors help us build a rich ecosystem of integrated apps that work seamlessly with Google Apps, allowing IT administrators to leverage the benefits of cloud computing and extend Google Apps to meet more of their business requirements.

4. User Privacy and Confidentiality

Much of our data – including student information databases and much faculty and staff e-mail – constitutes "education records" for purposes of the Family Educational Rights and Privacy Act (FERPA) and therefore may be outsourced only to vendors that we have designated, and that are willing to accept designation, as "school officials" with "legitimate educational interests" in the data. In order to do that, we must ensure both that our definitions of those two terms in our FERPA annual notices are broad enough to cover outsourcing, and that the vendor will not use the data for any purpose other than providing the outsourced service (such as data mining for the vendor’s own benefit) or re-disclose it to others without appropriate authorization. (See Special Terms 22 and 23)

a) Please describe the measures your organization and personnel will take to ensure that:

(1) Customer and End User Data are only accessed and used for the purpose of performing the activities that are the subject of this RFP, and will not be used for other purposes including targeted marketing purposes building an index of metadata, etc;

**SADA Systems:**

Google and SADA employees will access your account data only when an administrator from your domain grants Google employees explicit permission to do so for troubleshooting purposes. During the course of troubleshooting an issue or other investigation, the Google Support team may ask for the creation of a test administrator account, solely to be used to resolve the particular issue at hand.
In order to provide some of the core features in Google Apps products, our automated systems will scan and index some user data. For example:

- Email is scanned so we can perform spam filtering and virus detection.
- Email is scanned so we can display contextually relevant advertising in some circumstances. (Note that there is no ad-related scanning or processing in Google Apps for Education or Business with ads disabled)
- Some user data, such as documents and email messages, are scanned and indexed so your users can privately search for information in their own Google Apps accounts.

In other words, we only scan or index user content in Google Apps in order to provide features that will directly benefit users, or to help us maintain the safety and security of our systems. Except when your users choose to publish information publicly, Google Apps data is not part of the general google.com index.

It's important to note that our scanning and indexing procedures are 100% automated and involve no human interaction.

(2) Customer and End User Data are only accessed and used by those personnel within your organization, or approved subcontractors, who require access to perform activities that are the subject of this RFP;

**SADA Systems:**

Google and SADA employees will access your account data only when an administrator from your domain grants Google employees explicit permission to do so for troubleshooting purposes. During the course of troubleshooting an issue or other investigation, the Google Support team may ask for the creation of a test administrator account, solely to be used to resolve the particular issue at hand.

(3) Customer and End User Data will not be disclosed to or shared with any third party except as required by state or federal law or a valid court order (and, when required in such cases under the Family Educational Rights and Privacy Act or other applicable law, with prior notice to the person or persons affected), or with prior written consent from Customer or, where applicable, the individual(s) whose personal records would be disclosed; and

**SADA Systems:**

Google complies with valid legal process. It is Google's policy to notify users before turning over their data whenever possible and legally permissible.

Google employees may not access end-user accounts except as described in Google's Privacy Policy (http://www.google.com/privacy.html).

(4) Your personnel and approved subcontractors understand, accept, and have received appropriate instruction regarding their obligations to handle Customer and End User Data with the proper security as described above, and all such personnel and subcontractors will have read, understood, accepted, and received appropriate instruction as to how to comply with, the data protection provisions reflected in this RFP and the ultimate agreement between your organization and Customer.

**SADA Systems:**
Google and SADA employees will access your account data only when an administrator from your domain grants Google employees explicit permission to do so for troubleshooting purposes. During the course of troubleshooting and/or investigation, the Google Support team may ask for the creation of a test administrator account, solely to be used to resolve the particular issue at hand.

b) Please describe your familiarity with and understanding of the data privacy and security requirements of the following laws that may apply to Customer and End User Data: Health Insurance Portability and Accountability Act (HIPAA); Family Educational Rights and Privacy Act (FERPA); Financial Modernization Act of 199 (Gramm-Leach-Bliley); PCI-DSS, and/or any state data protection or breach notification requirements that you consider applicable. Describe how the proposed system tools and attributes can be used to comply with the requirements of these laws and regulations.

**SADA Systems:**

Google complies with applicable US privacy law, and the Google Apps Terms of Service can specifically detail our obligations and compliance with FERPA (Family Educational Rights and Privacy Act) regulations.

Google’s security and compliance services, powered by Postini, offer capabilities (GME – Encryption) that many businesses use to satisfy their compliance requirements with a variety of regulations, such as HIPAA/FERPA, among others. Generally, an organization must decide whether its use of our products is compliant with any regulations the company may be subject to.

c) Please describe your procedures for responding to subpoenas for End User information within your solution. How will you notify the Customer of subpoena or other legal requests related to End User data, before complying with the request? How will you cooperate with Customer in the event Customer elects to contest certain requests for confidential End User data?

**SADA Systems:**

Google complies with valid legal process. It is Google’s policy to notify users before turning over their data whenever possible and legally permissible.

d) Please provide a copy of all policies and procedures within your organization that relate to the measures described in Section VI.C.4.b.

**SADA Systems:**

Google complies with applicable US privacy law, and the Google Apps Terms of Service can specifically detail our obligations and compliance with FERPA (Family Educational Rights and Privacy Act) regulations.

Google’s security and compliance services, powered by Postini, offer capabilities (GME – Encryption) that many businesses use to satisfy their compliance requirements with a variety of regulations, such as HIPAA/FERPA, among others. Generally, an organization must decide whether its use of our products is compliant with any regulations the company may be subject to.
This Privacy Policy applies to all of the products, services and websites offered by Google Inc. or its subsidiaries or affiliated companies except Postini (Postini Privacy Policy). Sometimes, we may post product specific privacy notices or Help Center materials to explain our products in more detail.

If you have any questions about this Privacy Policy, please feel free to contact us through our website or write to us at

Privacy Matters
c/o Google Inc.
1600 Amphitheatre Parkway
Mountain View, California, 94043
USA

Information we collect and how we use it

We may collect the following types of information:

- **Information you provide** – When you sign up for a Google Account, we ask you for personal information. We may combine the information you submit under your account with information from other Google services or third parties in order to provide you with a better experience and to improve the quality of our services. For certain services, we may give you the opportunity to opt out of combining such information.

  Use the Google Dashboard to learn more about the information associated with your Account. If you are using Google services in conjunction with your Google Apps Account, Google provides such services in conjunction with or on behalf of your domain administrator. Your administrator will have access to your account information including your email. Consult your domain administrator’s privacy policy for more information.

- **Cookies** – When you visit Google, we send one or more cookies to your computer or other device. We use cookies to improve the quality of our service, including for storing user preferences, improving search results and ad selection, and tracking user trends, such as how people search. Google also uses cookies in its advertising services to help advertisers and publishers serve and manage ads across the web and our services.

- **Log information** – When you access Google services via a browser, application or other client our servers automatically record certain information. These server logs may include information such as your web request, your interaction with a service, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser or your account.

- **User communications** – When you send email or other communications to Google, we may retain those communications in order to process your inquiries, respond to your requests and improve our services. When you send and receive SMS messages to or from one of our services that provides SMS functionality, we may collect and maintain information associated with those messages, such as the phone number, the wireless carrier associated with the phone number, the content of the message, and the date and time of the transaction. We may use your email address to communicate with you about our services.

- **Affiliated Google Services on other sites** – We offer some of our services on or through other websites. Personal information that you provide to those sites may be sent to Google in order to deliver the service. We process such information under this Privacy Policy.
Third Party Applications – Google may make available third party applications, such as gadgets or extensions, through its services. The information collected by Google when you enable a third party application is processed under our Privacy Policy. Information collected by the third party application provider is governed by their privacy policies.

Location data – Google offers location-enabled services, such as Google Maps and Latitude. If you use those services, Google may receive information about your actual location (such as GPS signals sent by a mobile device) or information that can be used to approximate a location (such as a cell ID).

Unique application number – Certain services, such as Google Toolbar, include a unique application number that is not associated with your account or you. This number and information about your installation (e.g., operating system type, version number) may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers (for example, to request automatic updates to the software).

Other sites – This Privacy Policy applies to Google services only. We do not exercise control over the sites displayed as search results, sites that include Google applications, products or services, or links from within our various services. These other sites may place their own cookies or other files on your computer, collect data or solicit personal information from you.

In addition to the above, we use the information we collect to:

- Provide, maintain, protect, and improve our services (including advertising services) and develop new services; and

- Protect the rights or property of Google or our users.

If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use.

Google processes personal information on our servers in the United States of America and in other countries. In some cases, we process personal information outside your own country.

Choices

You can use the Google Dashboard to review and control the information stored in your Google Account.

Most browsers are initially set up to accept cookies, but you can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some Google features and services may not function properly if your cookies are disabled.

Google uses the DoubleClick advertising cookie on AdSense partner sites and certain Google services to help advertisers and publishers serve and manage ads across the web. You can view and manage your ads preferences associated with this cookie by accessing the Ads Preferences Manager. In addition, you may choose to opt out of the DoubleClick cookie at any time by using DoubleClick’s opt-out cookie.

Information sharing

Google only shares personal information with other companies or individuals outside of Google in the following limited circumstances:
• We have your consent. We require opt-in consent for the sharing of any sensitive personal information.

• We provide such information to our subsidiaries, affiliated companies or other trusted businesses or persons for the purpose of processing personal information on our behalf. We require that these parties agree to process such information based on our instructions and in compliance with this Privacy Policy and any other appropriate confidentiality and security measures.

• We have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law.

If Google becomes involved in a merger, acquisition, or any form of sale of some or all of its assets, we will ensure the confidentiality of any personal information involved in such transactions and provide notice before personal information is transferred and becomes subject to a different privacy policy.

**Information security**

We take appropriate security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data. These include internal reviews of our data collection, storage and processing practices and security measures, including appropriate encryption and physical security measures to guard against unauthorized access to systems where we store personal data.

We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it on our behalf. These individuals are bound by confidentiality obligations and may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations.

**Accessing and updating personal information**

When you use Google services, we make good faith efforts to provide you with access to your personal information and either to correct this data if it is inaccurate or to delete such data at your request if it is not otherwise required to be retained by law or for legitimate business purposes. We ask individual users to identify themselves and the information requested to be accessed, corrected or removed before processing such requests, and we may decline to process requests that are unreasonably repetitive or systematic, require disproportionate technical effort, jeopardize the privacy of others, or would be extremely impractical (for instance, requests concerning information residing on backup tapes), or for which access is not otherwise required. In any case where we provide information access and correction, we perform this service free of charge, except if doing so would require a disproportionate effort. Because of the way we maintain certain services, after you delete your information, residual copies may take a period of time before they are deleted from our active servers and may remain in our backup systems. Please review the service Help Centers for more information.

**Enforcement**

Google adheres to the US Safe Harbor Privacy Principles of Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement, and is registered with the U.S. Department of Commerce’s Safe Harbor Program.
Google regularly reviews its compliance with this Privacy Policy. When we receive formal written complaints, it is Google’s policy to contact the complaining user regarding his or her concerns. We will cooperate with the appropriate regular authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that cannot be resolved between Google and an individual.

**Changes to this Privacy Policy**

Please note that this Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any Privacy Policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes). We will also keep prior versions of this Privacy Policy in an archive for your review.

**Google Apps Terms of Service for Google Apps for Education**

Go to the Additional Terms for services made available with the new accounts infrastructure

This Google Apps for Education Agreement (the "Agreement") is entered into by and between Google Inc. ("Google"), with offices at 1600 Amphitheatre Parkway, Mountain View, California 94043 and ENTER CUSTOMER'S FULL LEGAL NAME, with an address at ENTER CUSTOMER ADDRESS ("Customer"). This Agreement governs Customer's access to and use of the Services and will be effective as of the Effective Date.

1. **Services.**

   o 1.1 **Facilities and Data Transfer.** All facilities used to store and process Customer Data will adhere to reasonable security standards no less protective than the security standards at facilities where Google stores and processes its own information of a similar type. Google has implemented at least industry standard systems and procedures to ensure the security and confidentiality of Customer Data, protect against anticipated threats or hazards to the security or integrity of Customer Data, and protect against unauthorized access to or use of Customer Data. As part of providing the Services, Google may transfer, store and process Customer Data in the United States or any other country in which Google or its agents maintain facilities. By using the Services, Customer consents to this transfer, processing and storage of Customer Data.

   o 1.2 **Modifications.**

     ▪ a. **To the Services.** Google may make commercially reasonable changes to the Services from time to time. If Google makes a material change to the Services, Google will inform Customer, provided that Customer has subscribed with Google to be informed about such material change.

     ▪ b. **To URL Terms.** Google may make commercially reasonable changes to the URL Terms from time to time. If Google makes a material change to the URL Terms, Google will inform Customer by either sending an email to the Notification Email Address or alerting Customer via the Admin Console. If the change has a material adverse impact on Customer and Customer does not agree to the change, Customer must so notify Google via the Help Center within thirty days after
This proposal valid for 180 days post April 4th, 2011 submission.

1.3 Aliases. Customer is solely responsible for monitoring, responding to, and otherwise processing emails sent to the "abuse" and "postmaster" aliases for Customer Domain Names but Google may monitor emails sent to these aliases for Customer Domain Names to allow Google to identify Services abuse.

1.4 Ads.

a. Default. The default setting for the Services is one that does not allow Google to serve Ads. Customer may change this setting in the Admin Console, which constitutes Customer’s authorization for Google to serve Ads. If Customer enables the serving of Ads, it may revert to the default setting at any time and Google will cease serving Ads.

b. Selectively Showing Ads. Notwithstanding Section 1.4(a), if Customer separates different classifications of End Users by domain or Google provides the capability for Customer to show Ads only to particular sets of End Users within the same domain, then Customer must enable the serving of Ads to End Users who are alumni.

c. Selectively Showing Ads. If Customer chooses to separate different classifications of End Users by domain, then Customer must enable the serving of Ads to Alumni. If Google provides the capability for Customer to show Ads only to particular sets of End Users, then Customer must enable Google’s serving of Ads to End Users who are not Students or Staff.

1.5 End User Accounts. Customer is solely responsible for monitoring, responding to, and otherwise processing emails sent to the “abuse” and “postmaster” aliases for Customer Domain Names but Google may monitor emails sent to these aliases for Customer Domain Names to allow Google to identify Services abuse.

2. Customer Obligations.

2.1 Permitted Uses. The Services are permitted for use only by (a) non-profit educational institutions and (b) other non-profit entities (as defined under the relevant state statutes) with 3,000 or less End User Accounts.

2.2 Compliance. Customer will use the Services in accordance with the Acceptable Use Policy. Google may make new applications, features or functionality for the Services available from time to time, the use of which may be contingent upon Customer’s agreement to additional terms. In addition, Google will make other Non-Google Apps Products (beyond the Services) available to Customer and its End Users in accordance with the Non-Google Apps Product Terms and the applicable product-specific Google terms of service. If Customer does not desire to enable any of the Non-Google Apps Products, Customer can enable or disable them at any time through the Admin Console.

2.3 Customer Administration of the Services. Customer may specify one or more Administrators through the Admin Console who will have the rights to access Admin.
Account(s) and to administer the End User Accounts. Customer is responsible for: (a) maintaining the confidentiality of the password and Admin Account(s); (b) designating those individuals who are authorized to access the Admin Account(s); and (c) ensuring that all activities that occur in connection with the Admin Account(s) comply with the Agreement. Customer agrees that Google’s responsibilities do not extend to the internal management or administration of the Services for Customer and that Google is merely a data-processor.

2.4 End User Consent. Customer’s Administrators may have the ability to access, monitor, use, or disclose data available to End Users within the End User Accounts. Customer will obtain and maintain all required consents from End Users to allow: (i) Customer’s access, monitoring, use and disclosure of this data and Google providing Customer with the ability to do so and (ii) Google to provide the Services.

2.5 Unauthorized Use. Customer will use commercially reasonable efforts to prevent unauthorized use of the Services and to terminate any unauthorized use. Customer will promptly notify Google of any unauthorized use of, or access to, the Services of which it becomes aware.

2.6 Restrictions on Use. Unless Google specifically agrees in writing, Customer will not, and will use commercially reasonable efforts to make sure a third party does not: (a) sell, resell, lease, or the functional equivalent, the Services to a third party (unless expressly authorized in this Agreement); (b) attempt to reverse engineer the Services or any component; (c) attempt to create a substitute or similar service through use of, or access to, the Services; (d) use the Services for High Risk Activities; or (e) use the Services to store or transfer any Customer Data that is controlled for export under Export Control Laws.

2.7 Third Party Requests. Customer is responsible for responding to Third Party Requests. Google will, to the extent allowed by law and by the terms of the Third Party Request: (a) promptly notify Customer of its receipt of a Third Party Request; (b) comply with Customer’s reasonable requests regarding its efforts to oppose a Third Party Request; and (c) provide Customer with the information or tools required for Customer to respond to the Third Party Request. Customer will first seek to obtain the information required to respond to the Third Party Request on its own, and will contact Google only if it cannot reasonably obtain such information.


3.1 By Customer. Customer will, at its own expense, respond to questions and complaints from End Users or third parties relating to Customers’ or End Users’ use of the Services. Customer will use commercially reasonable efforts to resolve support issues before escalating them to Google.

3.2 By Google. If Customer cannot resolve a support issue consistent with the above, then Customer may escalate the issue to Google in accordance with the TSS Guidelines. Google will provide TSS to Customer in accordance with the TSS Guidelines.

4. Suspension.

4.1 Of End User Accounts by Google If Google becomes aware of an End User’s violation of the Agreement, then Google may specifically request that Customer Suspend the applicable End User Account. If Customer fails to comply with Google’s request to Suspend
an End User Account, then Google may do so. The duration of any Suspension by Google will be until the applicable End User has cured the breach, which caused the Suspension.

4.2 Emergency Security Issues. Notwithstanding the foregoing, if there is an Emergency Security Issue, then Google may automatically Suspend the offending use. Suspension will be to the minimum extent and of the minimum duration required to prevent or terminate the Emergency Security Issue. If Google Suspends an End User Account for any reason without prior notice to Customer, at Customer’s request, Google will provide Customer the reason for the Suspension as soon as is reasonably possible.

5. Confidential Information.

5.1 Obligations. Each party will: (a) protect the other party’s Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to Affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential. Each party (and any Affiliates, employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill its obligations under this Agreement, while using reasonable care to protect it. Each party is responsible for any actions of its Affiliates, employees and agents in violation of this Section.

5.2 Exceptions. Confidential Information does not include information that: (a) the recipient of the Confidential Information already knew; (b) becomes public through no fault of the recipient; (c) was independently developed by the recipient; or (d) was rightfully given to the recipient by another party.

5.3 Required Disclosure. Each party may disclose the other party’s Confidential Information when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.

5.4 FERPA. The parties acknowledge that (a) Customer Data may include personally identifiable information from education records that are subject to FERPA (“FERPA Records”); and (b) to the extent that Customer Data includes FERPA Records, Google will be considered a “School Official” (as that term is used in FERPA and its implementing regulations) and will comply with FERPA.


6.1 Intellectual Property Rights. Except as expressly set forth herein, this Agreement does not grant either party any rights, implied or otherwise, to the other’s content or any of the other’s intellectual property. As between the parties, Customer owns all Intellectual Property Rights in Customer Data, and Google owns all Intellectual Property Rights in the Services.

6.2 Display of Brand Features. Google may display only those Customer Brand Features authorized by Customer (such authorization is provided by Customer uploading its Brand Features into the Services), and only within designated areas of the Services Pages. Customer may specify the nature of this use using the Admin Console. Google may also display Google Brand Features on the Services Pages to indicate that Google provides the Services. Neither party may display or use the other party’s Brand Features beyond what is allowed in this Agreement without the other party’s prior written consent.
6.3 **Brand Features Limitation.** Any use of a party’s Brand Features will inure to the benefit of the party holding Intellectual Property Rights in those Brand Features. A party may revoke the other party’s use of its Brand Features pursuant to this Agreement with written notice to the other and a reasonable period to stop the use.

7. **Publicity.** Neither party may make any public statement regarding the relationship contemplated by this Agreement without the other party’s prior written consent. Notwithstanding the foregoing, (a) Customer is permitted to state publicly that it is a customer of the Services, consistent with the Trademark Guidelines, and (b) Customer consents to Google’s use of Customer’s name in a general customer list, but only if Customer is not the only Customer appearing on the list. For clarification, Customer does not need to seek approval from Google if Customer is repeating a public statement that is substantially similar to a public statement that has been previously approved by Google in accordance with the provisions of this Agreement.

8. **Representations, Warranties and Disclaimers.**

   - **8.1 Representations and Warranties.** Each party represents that it has full power and authority to enter into the Agreement. Each party warrants that it will comply with all laws and regulations applicable to its provision, or use, of the Services, as applicable (including applicable security breach notification law). Google warrants that it will provide the Services in accordance with the applicable SLA. Customer acknowledges and agrees that it is solely responsible for compliance with the Children's Online Privacy Protection Act of 1998, including, but not limited to, obtaining parental consent concerning collection of students' personal information used in connection with the provisioning and use of the Services by the Customer and End Users.

   - **8.2 Disclaimers.** TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS EXPRESSLY PROVIDED FOR HEREIN, NEITHER PARTY MAKES ANY OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE AND NONINFRINGEMENT. GOOGLE MAKES NO REPRESENTATIONS ABOUT ANY CONTENT OR INFORMATION MADE ACCESSIBLE BY OR THROUGH THE SERVICES. CUSTOMER ACKNOWLEDGES THAT THE SERVICES ARE NOT A TELEPHONY SERVICE AND THAT THE SERVICES ARE NOT CAPABLE OF PLACING OR RECEIVING ANY CALLS, INCLUDING EMERGENCY SERVICES CALLS, OVER PUBLICLY SWITCHED TELEPHONE NETWORKS. THE SERVICES ARE NEITHER DESIGNED NOR INTENDED FOR HIGH RISK ACTIVITIES.

9. **Term; No Fees.**

   - **9.1 Term.** This Agreement will remain in effect for the Term.

   - **9.2 Auto Renewal.** At the end of the Initial Term and each renewal term, the Services will automatically renew for an additional term of twelve months. If either party does not want the Services to renew, then it must notify the other party in writing at least 15 days prior to the end of the then current term. This notice of non-renewal will be effective upon the conclusion of the then current term.

   - **9.3 No Fees.** During the Initial Term, Google will not charge Customer fees for the Services. Upon the parties’ mutual written agreement, (a) Google may charge Customer fees for the Services after the Initial Term and (b) Google may charge Customer fees for a premium
version of the Services or for optional functionality or enhancements that may be added to
the Services by Google.

- 9.4 Services Use. Customer has no obligation to use the Services and may cease using the
Services at any time for any reason (or no reason).

10. Termination.

- 10.1 Termination for Breach. Either party may suspend performance or terminate this
Agreement if: (i) the other party is in material breach of the Agreement and fails to cure
that breach within thirty days after receipt of written notice; (ii) the other party ceases its
business operations or becomes subject to insolvency proceedings and the proceedings are
not dismissed within ninety days; or (iii) the other party is in material breach of this
Agreement more than two times notwithstanding any cure of such breaches.

- 10.2 Other Termination. Customer may terminate this Agreement for any reason (or no
reason) with thirty days prior written notice to Google.

- 10.3 Effects of Termination. If this Agreement terminates, then: (i) the rights granted by
one party to the other will cease immediately (except as set forth in this Section); (ii)
Google will provide Customer access to, and the ability to export, the Customer Data for a
commercially reasonable period of time at Google’s then-current rates, if applicable, for
the Services; (iii) after a commercially reasonable period of time, Google will delete
Customer Data by removing pointers to it on Google’s active and replication servers and
overwriting it over time; and (iv) upon request each party will promptly use commercially
reasonable efforts to return or destroy all other Confidential Information of the other
party.

11. Indemnification.

- 11.1 By Google. Google will indemnify, defend, and hold harmless Customer from and
against all liabilities, damages, and costs (including settlement costs and reasonable
attorneys’ fees) arising out of a third party claim that Google’s technology used to provide
the Services or any Google Brand Feature infringe or misappropriate any patent, copyright,
trade secret or trademark of such third party. Notwithstanding the foregoing, in no event
shall Google have any obligations or liability under this Section arising from: (i) use of the
Services or Google Brand Features in a modified form or in combination with materials not
furnished by Google, and (ii) any content, information or data provided by Customer, End
Users or other third parties.

- 11.2 Possible Infringement.

  a. Repair, Replace, or Modify. If Google reasonably believes the Services infringe a
third party's Intellectual Property Rights, then Google will: (a) obtain the right for
Customer, at Google's expense, to continue using the Services; (b) provide a non-
infringing functionally equivalent replacement; or (c) modify the Services so that
they no longer infringe.

  b. Suspension or Termination. If Google does not believe the foregoing options are
commercially reasonable, then Google may suspend or terminate Customer’s use
of the Services with a minimum of six months written notice to Customer, unless
prohibited by a court of competent jurisdiction.
11.3 **General.** Customer will promptly notify Google of the claim and cooperate with Google in defending the claim. Google has full control and authority over the defense, except that: (a) any settlement requiring Customer to admit liability or to pay any money will require Google’s prior written consent, such consent not to be unreasonably withheld or delayed; and (b) Customer may join in the defense with its own counsel at its own expense. THE INDEMNITY ABOVE IS CUSTOMER’S ONLY REMEDY UNDER THIS AGREEMENT FOR VIOLATION BY GOOGLE OF A THIRD PARTY’S INTELLECTUAL PROPERTY RIGHTS.

12. **Limitation of Liability.**

12.1 **Limitation on Indirect Liability.** NEITHER PARTY WILL BE LIABLE UNDER THIS AGREEMENT FOR LOST REVENUES OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES, EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN THAT SUCH DAMAGES WERE POSSIBLE AND EVEN IF DIRECT DAMAGES DO NOT SATISFY A REMEDY.

12.2 **Limitation on Amount of Liability.** NEITHER PARTY MAY BE HELD LIABLE UNDER THIS AGREEMENT FOR MORE THAN THE AMOUNT PAID BY CUSTOMER TO GOOGLE DURING THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO LIABILITY.

12.3 **Exceptions to Limitations.** These limitations of liability apply to the fullest extent permitted by applicable law, but do not apply to breaches of confidentiality obligations, violations of a party’s Intellectual Property Rights by the other party, or indemnification obligations.

13. **Miscellaneous.**

13.1 **Notices.** Unless specified otherwise herein: (a) all notices must be in writing and addressed to the attention of the other party’s legal department and primary point of contact; and (b) notice will be deemed given: (i) when verified by written receipt if sent by personal courier, overnight courier, or when received if sent by mail without verification of receipt; or (ii) when verified receipt or electronic logs if sent by facsimile or email.

13.2 **Assignment.** Neither party may assign or transfer any part of this Agreement without the written consent of the other party, except to an Affiliate, but only if: (a) the assignee agrees in writing to be bound by the terms of this Agreement; and (b) the assigning party remains liable for obligations incurred under the Agreement prior to the assignment. Any other attempt to transfer or assign is void.

13.3 **Change of Control.** Upon a change of control (for example, through a stock purchase or sale, merger, or other form of corporate transaction): (a) the party experiencing the change of control will provide written notice to the other party within thirty days after the change of control; and (b) the other party may immediately terminate this Agreement any time between the change of control and thirty days after it receives the written notice in subsection (a).

13.4 **Force Majeure.** Neither party will be liable for inadequate performance to the extent caused by a condition (for example, natural disaster, act of war or terrorism, riot, labor condition, governmental action, and Internet disturbance) that was beyond the party’s reasonable control.
13.5 **No Waiver.** Failure to enforce any provision of this Agreement will not constitute a waiver.

13.6 **Severability.** If any provision of this Agreement is found unenforceable, the balance of the Agreement will remain in full force and effect.

13.7 **No Agency.** The parties are independent contractors, and this Agreement does not create an agency, partnership or joint venture.

13.8 **No Third-Party Beneficiaries.** There are no third-party beneficiaries to this Agreement.

13.9 **Equitable Relief.** Nothing in this Agreement will limit either party's ability to seek equitable relief.

13.10 **Governing Law.**

   - **For State and City Government Entities.** If Customer is a city or state government entity, then the parties agree to remain silent regarding governing law and venue.

   - **For All other Entities.** If Customer is any entity not set forth in Section 13.10(a) then the following applies: This Agreement is governed by California law, excluding that state’s choice of law rules. FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS AGREEMENT, THE PARTIES CONSENT TO PERSONAL JURISDICTION IN, AND THE EXCLUSIVE VENUE OF, THE COURTS IN SANTA CLARA COUNTY, CALIFORNIA.

13.11 **Amendments.** Any amendment must be in writing and expressly state that it is amending this Agreement.

13.12 **Survival.** The following Sections will survive expiration or termination of this Agreement: 5 (Confidential Information), 7.1 (Intellectual Property Rights), 11.3 (Effects of Termination), 12 (Indemnification), 13 (Limitation of Liability), 14 (Miscellaneous) and 15 (Definitions).

13.13 **Entire Agreement.** This Agreement, and all documents referenced herein, is the parties’ entire agreement relating to its subject and supersedes any prior or contemporaneous agreements on that subject. If Customer is presented with a similar agreement on the same subject matter upon its log in to use the Services, this Agreement supersedes and replaces that agreement. The terms located at a URL and referenced in this Agreement are hereby incorporated by this reference.

13.14 **Interpretation of Conflicting Terms.** If there is a conflict between this Agreement and the URL Terms, this Agreement will control.

13.15 **Counterparts.** The parties may enter into this Agreement in counterparts, including facsimile, PDF or other electronic copies, which taken together will constitute one instrument.

14. **Definitions.**
o "Acceptable Use Policy" means the acceptable use policy for the Services available at http://www.google.com/a/help/intl/en/admins/use_policy.html or such other URL as may be provided by Google.

o "Admin Account(s)" means the administrative account(s) provided to Customer by Google for the purpose of administering the Services. The use of the Admin Account(s) requires a password, which Google will provide to Customer.

o "Admin Console" means the online tool provided by Google to Customer for use in reporting and certain other administration functions.

o "Administrators" mean the Customer-designated technical personnel who administer the Services to End Users on Customer's behalf.

o "Ads" means online advertisements displayed by Google to End Users.

o "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a party.

o "Agreement" means this Google Apps for Education Agreement.

o "Brand Features" means the trade names, trademarks, service marks, logos, domain names, and other distinctive brand features of each party, respectively, as secured by such party from time to time.

o "Confidential Information" means information disclosed by a party to the other party under this Agreement that is marked as confidential or would normally be considered confidential under the circumstances. Customer Data is Customer's Confidential Information.

o "Customer Data" means data, including email, provided, generated, transmitted or displayed via the Services by Customer or End Users.

o "Customer Domain Names" means the following domain names owned or controlled by Customer, which will be used in connection with the Services: ENTER CUSTOMER ADDRESS. Customer may provide the Services to any of its sub-domains (for example, if Customer Domain Name is “edu.com”, a sub-domain may include “alumni.edu.com”) without written approval from Google.

o "Effective Date" means the date this Agreement is countersigned.

o "Emergency Security Issue" means either: (a) Customer’s use of the Services in violation of the Acceptable Use Policy, which could disrupt: (i) the Services; (ii) other customers’ use of the Services; or (iii) the Google network or servers used to provide the Services; or (b) unauthorized third party access to the Services.

o "End Users" means the individuals Customer permits to use the Services.

o "End User Account" means a Google-hosted account established by Customer through the Services for an End User.

o "Export Control Laws" means all applicable export and re-export control laws and regulations, including the Export Administration Regulations (“EAR”) maintained by the
U.S. Department of Commerce, trade and economic sanctions maintained by the Treasury Department’s Office of Foreign Assets Control, and the International Traffic in Arms Regulations ("ITAR") maintained by the Department of State.

- "FERPA" means the Family Educational Rights and Privacy Act (20 U.S.C. 1232g) and the Family Educational Rights and Privacy Act Regulations (34 CFR Part 99), as amended or otherwise modified from time to time.

- "Help Center" means the Google help center accessible at http://www.google.com/support/ or other such URL as Google may provide.

- "High Risk Activities" means uses such as the operation of nuclear facilities, air traffic control, or life support systems, where the use or failure of the Services could lead to death, personal injury, or environmental damage.

- "Intellectual Property Rights" means current and future worldwide rights under patent law, copyright law, trade secret law, trademark law, moral rights law, and other similar rights.

- "Initial Term" means the term that begins on the Effective Date and continues for 1 year.

- "Non-Google Apps Products" means Google products which are not part of the Services, but which may be accessed by End Users using their End User Account login and password. The Non-Google Apps Products are set forth at the following URL: http://www.google.com/support/a/bin/answer.py?hl=en&answer=181865, or such other URL as Google may provide.

- "Non-Google Apps Product Terms" means the terms found at the following URL: http://www.google.com/apps/intl/en/terms/additional_services.html, or such other URL as Google may provide from time to time.

- "Notification Email Address" means the email address designated by Customer to receive email notifications from Google. Customer may change this email address through the Admin Console.

- "Service Pages" mean the web pages displaying the Services to End Users.

- "Service" means the Google Apps for Education Services provided by Google and used by Customer under this Agreement. The Services are described here: http://www.google.com/a/help/intl/en/users/user_features.html, or such other URL as Google may provide.

- "SLA" means the Services Level Agreement located here: http://www.google.com/a/help/intl/en/admins/sla.html or other such URL as Google may provide.

- "Suspend" means the immediate disabling of access to the Service, or components of the Service, as applicable, to prevent further use of the Service.

- "Term" means the term of this Agreement, which begins on the Effective Date and continues until the earlier of: (a) the end of the applicable term for the Services or (b) the Agreement is terminated as set forth herein.
- "Trademark Guidelines" means Google’s Guidelines for Third Party Use of Google Brand Features, located at the following URL: http://www.google.com/permissions/guidelines.html, or other such URL as Google may provide.

- "Third Party Request" means a request from a third party for records relating to an End User’s use of the Services. Third Party Requests can be a lawful search warrant, court order, subpoena, other valid legal order, or written consent from the End User permitting the disclosure.

- "TSS" means the technical support services provided by Google to the Administrators during the Term pursuant to the TSS Guidelines.

- "TSS Guidelines" means Google's technical support services guidelines then in effect for the applicable Services. TSS Guidelines are at the following URLs: http://www.google.com/a/help/intl/en/admins/tssg.html or such other URL as Google may provide.

- "URL Terms" means the Acceptable Use Policy, the SLA, and the TSS Guidelines.

Please provide the name(s) and contact information for the person(s) responsible in your organization for electronic and paper records security.

**SADA Systems:**

Annie Safoian, CFO SADA Systems, Inc.
Address: 5250 Vineland Avenue, North Hollywood, CA 91601
Phone: (818) 766-2400

**D. Integration and Operational Issues**

SaaS and cloud computing solutions provide great promise to the future of campus IT infrastructures, but they must be fully integrated with institutional identity management and directory systems, and should only be pursued with a clear understanding of the entry and exit conditions, including essential matters such as how the Customer and End User data will be provided (migrated) at the conclusion of the license term, if the vendor ceases to support the services, or when new technologies become available.

**1. Service Entry Plan/Migration Strategy**

Provide a high-level entry plan which provides for the successful and uninterrupted transfer to vendor of services under various migration scenarios. Include a timeline and estimated milestones for each scenario:

- **Implement a 1,000 User pilot solution and migrate all live and historical data (archive and backup) from Oracle OCUCS and MS Exchange 2007 system(s) migrated by June 2011**

**SADA Systems:**

The SADA team will collaborate with the University IT team to assess technical requirements, use cases, and other considerations prior to the pilot. The specific methodology depends on the University's IT environment, but generally, Google first-party tools can be used to provision users from an existing LDAP directory and migrate historical mail, calendar, and contacts data from a Microsoft Exchange or IMAP server into the pilot users' Google Apps accounts. Live mail will be directed to Google Apps by
means of split or dual delivery through an MX record change or mail forwarding rule on the legacy mail server.

Since every pilot has different objectives, our recommendation would be that each university decide what would be unnecessary for a pilot and then shorten timeline according to the goals, objectives and success criteria of their own particular pilot. Then, using the plan listed below, a university could opt out of doing some of the more formal steps required of a full-blown implementation and thus shorten the time frame according to its own needs.

The level of technical integration may vary depending on the university's specific requirements and environment, but doesn't depend significantly on the number of participants. The timeline can be as little as 30 days with data migration, depending on the university's egress bandwidth and availability of university technical resources. Milestones might include: deployment planning workshop (week 1), formulation of a data migration and mail delivery strategy (week 2), cutover of mail delivery to Google Apps (week 3), and phased migration of user data (week 3-4). The timeline may vary according to the goals, scope/objectives and success criteria of the university's particular pilot.

This plan assumes there is no disruption of service.

b) Implement the entire solution and migrate all live and historical data (archive and backup) from Oracle OCUCS and MS Exchange 2007 system(s) migrated by August 2011.

*SADA Systems:*

Implementing Google Apps with complete data migration is a slightly more complex way to implement Google Apps. It is important to note that there are many other factors that affect the timeframe and level of effort. Those factors can be broken up into a technical design category to include; SSO integration, Blackberry BES Integration, Directory Services, Calendar Free-Busy integration; an end user training and change management category and lastly, a resourcing category; what level of effort and expertise are able to expend on the project.

Post-pilot, a university will have validated that tools and methodologies to migrate to Google Apps for Education are functional and successful in their specific environment. Depending on the number of users needed to be provisioned and migrated, the university can work with SADA, to define a realistic timeline and milestones based on best practices known at the time of implementation. Once tools have been validated in a particular environment, the migration timeline will vary upon the university's availability of technical resources, computational resources, and egress bandwidth.

These criteria affect the timeline, scope, risk and cost of your project, but you may definitely assume that if you are migrating data your implementation will be slightly longer and more complex than if you opt not to.

A realistic timeline for migration of all data from the existing system will also vary based on the number of users and complexity of technical integration. A 10,000 user migration might take 12-16 weeks for all historical data to be migrated, but users could be fully provisioned and online with Google Apps in 30-60 days first.

Below is a standard, 6-week, Google Apps best practices implementation plan for higher educational institutions:

Step 1 - Building a Plan & Setting Goals (6 weeks to deployment)
1. Participate in a kick-off meeting with your Project Team (manager, technical, marketing, etc)
2. See what other schools have done by browsing customer testimonials
3. Sign up for Google Apps account at http://www.google.com/a/cpanel/education/new
4. Develop scheme and dates for technical requirements
5. Sign up with partners to assist with technical requirements. This is optional.

Step 2 - Testing the Product (5 weeks to deployment)

1. Get acquainted with services (calendar, docs, sites, start page, email)
2. Test Email Migration
3. Test Single Sign On Implementation (If applicable)
4. Test Directory Services Integration or alternately Provisioning API (If applicable)

Step 3 - Testing the Product (4 weeks to deployment)

1. Test Mail Delivery Setup (Recommended on the test domain)
2. Check in with your Project Team

Step 4 - Customizing and Modifying (3 weeks to deployment)

1. Customize account with information unique to your school
2. Make Modifications on technical requirements

Step 5 - Implementing the Plan (2 weeks to deployment)

1. Implement Single Sign On
2. Implement Email Migration
3. Implement Marketing Plan
4. Check in with Project Team
5. Setup your Help Desk Operations

Step 6 - Ignite (1 week to deployment)

1. Complete Marketing Plan
2. Complete provisioning
3. Choose date/time of day to change live domain’s MX records (mail delivery) to Google

This plan assumes there is no disruption of service.

c) Implement the entire solution without migrating historical data from existing e-mail.

**SADA Systems:**

Implementing Google Apps without migrating any data is the least complex way to implement Google Apps, carries the lowest risk and will result in the lowest cost transition. It is important to note that there are still factors that affect the timeframe. Those factors can be broken up into a technical design category to include; SSO integration, Blackberry BES Integration, Directory Services, Calendar Free-Busy integration; an end user training and change management category and lastly, a resourcing category; what level of effort and expertise are able to expend on the project.

Post-pilot, a university will have validated that tools and methodologies to migrate to Google Apps for Education are functional and successful in their specific environment. Depending on the number of
users needed to be provisioned and migrated, the university can work with SADA, to define a realistic timeline and milestones based on best practices known at the time of implementation.

These decisions affect the timeline, scope, risk and cost of your project, but you may definitely assume that if you are not migrating data your implementation will be simpler, shorter, cost less and have a higher likelihood of success. The migration timeline will vary depending on the number of users needed to be provisioned and technical integration with existing systems. Without data migration, an entire campus could be online with Google Apps within 30-60 days.

Below is a standard, 6-week, Google Apps best practices implementation plan for higher educational institutions:

Step 1 - Building a Plan & Setting Goals (6 weeks to deployment)

1. Participate in a kick-off meeting with your Project Team (manager, technical, marketing, etc)
2. See what other schools have done by browsing customer testimonials
3. Sign up for Google Apps account at http://www.google.com/a/cpanel/education/new
4. Develop scheme and dates for technical requirements
5. Sign up with partners to assist with technical requirements. This is optional.

Step 2 - Testing the Product (5 weeks to deployment)

1. Get acquainted with services (calendar, docs, sites, start page, email)
2. Test Email Migration (NOT APPLICABLE)
3. Test Single Sign On Implementation (If applicable)
4. Test Directory Services Integration or alternately Provisioning API (If applicable)

Step 3 - Testing the Product (4 weeks to deployment)

1. Test Mail Delivery Setup (Recommended on the test domain)
2. Check in with your Project Team

Step 4 - Customizing and Modifying (Deployment)

1. Customize account with information unique to your school
2. Make Modifications on technical requirements

Step 5 - Implementing the Plan (2 weeks to deployment)

1. Implement Single Sign On
2. Implement Email Migration (NOT APPLICABLE)
3. Implement Marketing Plan
4. Check in with Project Team
5. Setup your Help Desk Operations

Step 6 - Ignite (1 week to deployment)

1. Complete Marketing Plan
2. Complete provisioning
3. Choose date/time of day to change live domain's MX records (mail delivery) to Google

This plan assumes there is no disruption of service.
2. Integration with Directory, Identity Management and Authentication Services

Provide your implementation plan for integration with institutional identity & access management. Specifically address the fact that Virginia Tech wants to maintain its directory (LDAP & AD) and authentication (CAS, Shibboleth, AD, LDAP) services, and seeks to avoid separate account provisioning and authentication/authorization requirements. Based on this assumption:

a) How will you integrate with an existing [OpenLDAP, Microsoft AD] directory service?

**SADA Systems:**

Google provides Google Apps Directory Sync (GADS) so that you can maintain your corporate directory in your current LDAP system and sync user account and groups to Google. Additionally, you may maintain your identity management directly within Google Apps and lastly, Google can integrate with any SAML 2.0-compliant identity management system.

Administrators can manage user identity and account information directly in Google Apps or can continue to manage users in the organization’s existing directory (LDAP) system and automatically synchronize that with Google Apps using Google Apps Directory Sync (GADS).

b) How will you integrate with an existing [CAS 3.0, Shibboleth (Saml 2.0), OpenLDAP, Microsoft AD] authentication system?

**SADA Systems:**

With Google Apps Directory Sync (provided at no additional cost), you can automatically provision users, groups and non-employee contacts based on the user data in your LDAP server, such as Microsoft Active Directory or similar directory service. Google Apps Directory Sync connects to your Google Apps directory and adds/deletes user accounts to match your existing organizational schema. Google Apps Directory Sync supports LDAP v3, which supports SASL.

Google Apps provides a SAML 2.0 integration point for external authentication services (see [http://code.google.com/googleapps/saml_reference_implementation.html](http://code.google.com/googleapps/saml_reference_implementation.html) for further information). For information on how to leverage this for Shibboleth integration, see [http://code.google.com/apis/apps/articles/shibboleth2.0.html](http://code.google.com/apis/apps/articles/shibboleth2.0.html).

Google Apps can be integrated with Kerberos 5 via Web SSO solutions which support it.

For more information on how Google Apps supports authentication standards such as OpenSSO, OpenID, and OAuth, see [http://code.google.com/apis/apps/open_source_projects.html](http://code.google.com/apis/apps/open_source_projects.html) and [http://code.google.com/googleapps/domain/sso/openid_reference_implementation.html](http://code.google.com/googleapps/domain/sso/openid_reference_implementation.html).

Google Apps supports SAML 2.0-based SSO, compatible with Shibboleth. Many schools have used this service with Shibboleth. More information here: [http://code.google.com/googleapps/domain/sso/saml_reference_implementation.html](http://code.google.com/googleapps/domain/sso/saml_reference_implementation.html).

c) For web components, how will you integrate with an existing [Internet2 Shibboleth Web Single Sign-On, CAS WebAuth, OpenLDAP] authentication system?

**SADA Systems:**

Customer administrators and IT architects have choices with respect to end-user authentication and Google Apps. Customer organizations can choose to use the native Google Apps username, password
and multi-factor authentication (if enabled by the administrator) to gain access to Google Apps services or can implement the SAML (V2.0) SSO API where user authentication responsibility is transparently sent to the customer infrastructure. Using the SAML SSO approach, customer organizations can enforce custom authentication methods to include multi-factor authentication. Customers using SAML SSO can, therefore, include support for solutions like SecurID, Arcot, biometric devices, smartcards, etc.

\textbf{d)} Can you enforce password/passphrase aging requirements? Can you enforce password/passphrase complexity requirements? (If so, can you enforce such requirements differentially within the population based on LDAP attributes, e.g., students vs. faculty vs. clinical workers?).

\textbf{SADA Systems:}

In the Google Apps Control Panel, Administrators can set password length requirements, and view password strength indicators (which identify passwords that meet the length requirement but may still not be strong enough).

The password strength indicators can assess password strength in real-time and help administrators spot passwords that were relatively secure when chosen, but have become more vulnerable to the latest patterns of attacks.

If your Active Directory / LDAP ID Management server will remain in place, you can also manage and restrict passwords as you do today since these passwords will sync with your Google Apps domain using SSO and password sync.

3. Integration with Account Provisioning and Management Systems

Will your solution allow the system administrator(s) to set up Users and groups that are protected from one another, including enabling segregated management of groups by different administrators either intra-institutionally or inter-institutionally? What programmatic interface(s) are provided to university system administrators to enable automated creation, locking, unlocking, and deletion of accounts, and management of quotas, group membership, etc?

\textbf{SADA Systems:}

Google Apps provides API's for provisioning, including creating/updating/renameing/deleting/suspending user accounts, and for managing group membership (see http://code.google.com/googleapps/domain/gdata_provisioning_api_v2.0_reference.html for further information).

Google Apps also provides API's to manage administrative settings and retrieve information such as the maximum and current number of users (see http://code.google.com/googleapps/domain/admin_settings/docs/1.0/admin_settings_developers_guide_protocol.html for further information); each user gets 7.4 GB of email and IM storage, so administrators no longer have to manage individual storage quotas.

4. Integration with Other Systems or Applications

\textbf{a)} Does your solution support open standards based interoperability with content and document management systems, unified messaging systems (voice e-mail, instant messaging, VoIP, etc), emergency notification systems, and collaboration tools (wikis, blogs, etc)? Please specify which open
standards are supported and specify whether the associated interoperability is included in the solution, or by other products separately available from the vendor.

**SADA Systems:**

Google’s mission is to make the world’s information universally accessible and useful. Google Apps reflects our belief that communications should be accessible and useful as well. We’re committed to open communications standards, and want to offer Google Apps users and users of other service providers alike the flexibility to choose which clients, service providers, and platforms they use for their communication and collaboration needs.

Google Apps natively provides many of the capabilities of unified messaging without the need for additional solutions:

- Google chat supports the ability to chat internally and externally. Administrators may choose to restrict chat to users in the same domain or to allow chat to external users. In addition to restricting IM use to internal users, administrators may disable IM altogether.
- Presence is built into GMail, Calendar, Chat, Docs and Spreadsheets.
- Administrators may force all IM to be "on the record", resulting in the chat history to be recorded in the user's mailbox. It must be noted that this archive is not intended to be used for eDiscovery purposes.
- Video and voice are built into chat applications
- Users may place phone calls directly from the chat interface
- Gmail comes with a media player to play voice mail messages from phone systems

The Google Apps unified messaging experience is also available on mobile devices such as Android, including mail, calendar, contacts, and voice

Google Apps natively provides many of the capabilities of collaboration tools such as wikis and blogs without the need for additional solutions:

- Google Docs eliminates the need for serial collaboration with attachments. Employees can share files with colleagues for collaborative editing. Everyone accesses the same online copy of the file in Google Docs, so there are no attachment compatibility problems, inbox storage quota issues, or versions to reconcile. When the group is done editing, you can keep the file in Google Docs, or export it back to the original format.
- Sharing knowledge is simple with Google Sites. Free-form text, file attachments, videos, photos, and other types of information can be organized all together. It's so intuitive that every user can contribute; no special technical skills are required so colleagues can create rich sites without burdening IT for support. Best of all, Google search is built-in, so users can find company information instantaneously.
- Sites File Storage automatically versions uploaded documents and indexes all their contents.
- Videos can be more personal and impactful than traditional office documents. Users can use Google Video to securely share and watch internal videos with no special hardware or software.
- Google Apps provides native access to Blogger and other collaboration and social tools such as Orkut right from the menu
Google Apps also supports rapid integration with Google Maps and Google Search, as well as with databases, web applications, web services, and XML feeds, providing the user with a coherent, unified experience.

Google Apps provides a complete suite of both application/service-level APIs, as well as administrative APIs for programmatic integration with existing 3rd party systems and administrative processes. All Google APIs are based on industry standards such as HTTP, SMTP, ATOM/RSS, OpenID/OAuth, SAML, and XMPP. The Google Apps APIs generally fall into two categories: application/service, and domain administration. Through these APIs, it’s possible for Google Apps to interoperate with third party systems such as document management systems, unified messaging systems, emergency notification systems and collaboration tools. Messages from third party systems can be distributed by Google Apps.

Finally, there are many existing third party products that extend Google Apps, provide additional functionality, and provide interoperability with other systems using the Google Apps APIs. Partners such as Esnatech provide products which include additional integration with traditional telecommunications services such as faxes, voicemail, and telephone calls.

In addition to the Google Talk client, there are many other clients out there that provide a great communications experience. We believe users should have choice in which clients they use to connect to the Google Talk service and we want to encourage the developer community to create new and innovative applications that leverage our service. To enable this, Google Talk uses the standard XMPP protocol for authentication, presence, and messaging. Google can talk to any client that supports Jabber/XMPP can connect to the Google Talk service. Here’s a list of popular clients:

http://www.google.com/talk/otherclients.html

As long as you adhere to the requirements of the XMPP specs, you will be able to connect to the Google Talk service. The service is hosted at talk.google.com on port 5222 over TLS. Google Talk uses extensions to XMPP for voice/video signaling and peer-to-peer communication. Currently, Google Talk’s implementation differs slightly from the draft XMPP Jingle specifications. However, Google Talk is in the process of being updated to be in full compliance with the Jingle specifications. Details on the voice and video signaling used by Google are available in the Google Talk Call Signaling document. Additionally, the open source libjingle library is provided to make it easy to implement voice/video interoperability with Google Talk. Today, Google Talk supports the following standard voice codecs:

- PCMA
- PCMU
- G.722
- GSM
- iLBC
- Speex

We also support the following codecs from Global IP Sound: ISAC, IPCMWB, EG711U, EG711A.

Google Talk supports the following video codecs:

- H.264/SVC
- H.264
- H.263-1998

Support for the Google VP8 codec is in process.
b) Does your solution support standards-based programmatic interfaces for integrating with other scheduling products used on campus? Please specify which open standards are supported and specify whether the associated interoperability is included in the solution, or by other products separately available from the vendor.

**SADA Systems:**

Google Apps Calendar supports standard programmatic interfaces for its calendar such as iCal and CalDav, included, at no cost, to every customer. Google Calendar includes a robust, data API supporting the following industry standards: .NET, Java, JavaScript, PHP, Python.

c) Can your solution provide standards-based programmatic interfaces for integrating with Sakai, the open source enterprise teaching, learning and academic collaboration platform (see http://sakaiproject.org/)? Describe the level of integration your product has or can have with Sakai.

**SADA Systems:**

Rsmart's 2.7.1 release of the Sakai collaborative learning environment includes new Google Apps functionality. Sharing a Google Doc in Sakai now lets Sakai handle which users have access – often a volatile course roster as students drop and add classes – without having to manage a separate list of usernames with Google.

5. Service Termination Plan/Exit Strategy

In the event of a termination for whatever reason, how will you provide for the successful and uninterrupted transfer of each of the services and associated data (i.e. e-mail messages, calendar entries, address book contacts, documents, etc) from the vendor service to Virginia Tech or a third party provider designated by Virginia Tech? This exit strategy should address capacity planning, process planning, facilities planning, human resources planning, telecommunications planning, and migration schedules. In the event of a migration to a different solution, within 90 days of receiving written notification from Customer of successful migration, the vendor must ensure the destruction of all of Virginia Tech’s data utilizing US Department of Defense-compliant disk sanitation techniques. (See Special Term 28)

**SADA Systems:**

Google offers convenient migration options to transfer mail service and data to another service via open standards. The Data Liberation Front (http://www.dataliberation.org) and this article detail the process: http://www.google.com/support/a/bin/answer.py?hl=en&answer=100458

Google does not impose any additional costs or penalties for cessation of a contract. Moreover, Google provides a number of free tools, managed by the Google Data Liberation Front team, for migration away from Google Apps. The Google Data Liberation Front is an engineering team at Google whose singular goal is to make it easier for users to move their data in and out of Google products. We do this because we believe that you should be able to export any data that you create in (or import into) a product. We help and consult other engineering teams within Google on how to "liberate" their products. This is their mission statement: Users should be able to control the data they store in any of Google's products. The DLF team's goal is to make it easier to move data in and out. To that end, we have a rich set of API's and tools to allow you to move your data out of Google and to other platforms; either cloud-based or hosted. A list of APIs is here:

http://code.google.com/googleapps/docs
Additionally, we support standard email protocols such as POP, IMAP and MAPI that making moving your data to and from Google simple. We haven't seen instances of customers moving from one hosted system to another, but it's technically possible and support for protocols would be the mechanism by which this would be accomplished. The migration tools provided by Google have no cost and customers can work with a Google Partner to implement the migration processes.

E. Functionalities

Basic e-mail functionality is now well understood and interoperability between servers and clients has become commonplace. Likewise, calendar functionality is becoming more standards based. Beyond the basic functionalities, Virginia Tech makes heavy use of certain features for workflow or delegation that are essential to any transition to SaaS or cloud solutions. Other supplemental component functionality is desired beyond the primary target applications described in the body of this RFP and is detailed in VI.B.10-12

1. Interfaces and Platform Support

Virginia Tech has a diverse client environment including Windows, Macintosh and Unix/Linux operating systems.

a) Does the proposed solution support multiple client platforms (e.g., Windows XP and Vista, Mac OS X and Linux), native e-mail clients (e.g. Eudora, Outlook/Outlook Express, Apple e-mail (Mac Mail), Entourage, Gnome Evolution) and web-based clients (e.g., Thunderbird)? Specifically, does it support the operating systems and platforms detailed in VI.B.1.a and 2.a?

SADA Systems:

Please see response to VI.B.1.a and 2.a.

b) Describe how the proposed solution will provide a secure, robust, common web interface for accessing all components of the solution (e-mail, calendar, address book, task list, etc) from a variety of browsers, as detailed in VI.B.3. Will the web e-mail client allow Users to choose between at least plain text and HTML e-mail formats (indicate any other formats supported)? Specify any other formats supported, and describe whether the User is able to choose a default format, and override the default on a per-message basis.

SADA Systems:

As a cloud-based product, Google Apps natively supports a common web interface for securely accessing all components of the solution from any standard browser. Users can access any of the Google Apps offerings from any of the others via simple menus, so, for instance, they have instant access to their own and shared documents directly from the mail interface.

Google designs products using industry best practices and non-proprietary standards, which result in a standards-compliant communication solution. Google Apps supports a variety of industry standards including; SMTP, MIME, IMAP, POP, TLS, MAPI, ActiveSync, Blackberry BES, iCal, XMPP, LDAP, SAML, SSL, OpenID, OAuth, HTML5, XML, XSLT, Atom, RSS, YAML, JDO, JPA, JDBC.

c) Describe how you will support access from and synchronization with common mobile devices for all components of the solution (e-mail, calendar, address book, task list, etc), including but not limited to the devices detailed in VI.B.4. Can you offer a simplified web interface available for use with mobile devices not supported directly?

SADA Systems:
Google Apps aims to provide users with seamless, more secure access to information regardless of location or device. Google Apps supports access to Gmail, Google Calendar, Docs, and Contacts from most common types of mobile devices. Information about accessing Google Apps from mobile devices and the specific Apps that can be accessed from each type of device can be found at http://www.google.com/apps/intl/en/business/mobile.html. Further information regarding specific syncing capabilities is outlined below:

**BES**

Google Apps Connector for Blackberry Enterprise Server allows for the synchronization of Mail, Calendar and Contacts. For enterprises, Gmail works with BlackBerry Mobile phones through the use of the Google Apps Connector for Blackberry Enterprise Server.

**Features**

- Push email delivery and send Messages sent from and received in your Gmail inbox are automatically pushed to your BlackBerry device within 60 seconds, keeping both inboxes up-to-date.
- Read/delete synchronization Emails read or deleted on your BlackBerry device are marked as read or deleted in your Gmail inbox, and vice-versa.
- Folder/label synchronization Select folders on your BlackBerry device to synchronize with labels in your Gmail interface.
- Global address lookup Search for and access email addresses and phone numbers for other users on your company domain.
- Calendar access: View your Google Calendar events and schedule from the native BlackBerry application, with two-way synchronization from your Google Calendar to BlackBerry device.
- Contacts synchronization: Contacts in your BlackBerry address book and in your Gmail account are automatically synchronized. Information added to Gmail is pushed to your BlackBerry device within 5 minutes, and vice-versa.
- Hosting Support: Support multiple Google Apps domains on a single BlackBerry Enterprise Server. This enables our partners to offer hosted services for supporting BlackBerry devices by sharing a single BlackBerry Enterprise Server across multiple Google Apps customers.
- Availability: Google Apps Connector for Blackberry Enterprise Server is available at no charge to Google Apps Premier and Google Apps Education Edition customers.

**Google Sync for iPhone, iPad, iPod Touch and Windows Mobile:**

Google Sync lets your users synchronize their mail, contacts and calendars to their mobile devices. This means that your users will have access (viewing and editing) to their inbox, address books and calendar events at any time. They can also get alerts (sound or vibration) for upcoming meetings and incoming messages. Google Sync works for both iPhone and Windows Mobile devices. These services are still in beta. Google Sync offers two-way synchronization between your calendar, contacts and email on a myriad of mobile devices. Updates are done automatically. Whether you update appointments and contacts from your mobile device or from your computer, you always have access to up-to-date information. Google Sync also offers controls for administrators to help ensure corporate policy enforcement across a range of mobile devices.

**Android:**

On some Android-powered devices, Google applications, such as Gmail, Google Calendar, Google Talk and Contacts come pre-installed. Access these apps by tapping their icons. When setting up the phone,
make sure to log in using the username and password for your domain, and your content will be automatically synced on the go. Gmail, Google Calendar and Google Docs in the mobile browser are also available in a single, streamlined interface, where you can seamlessly switch between applications. Bookmark http://www.google.com/m/a/example.com from your browser and add a shortcut icon to your homescreen by long-pressing and selecting the 'shortcut' then 'bookmark' options. But don't forget, you'll have to replace "example.com" with your actual domain name.

Palm webOS:

Instructions on configuring a Palm webOS device to access Gmail can be found at https://mail.google.com/support/bin/answer.py?hl=en&answer=150695.

**d)** How will you handle interface issues, particularly in relation to compliance responsibilities (ADA section 508 and WC3 standards), presentation, and access to your system?

**SADA Systems:**

Accessibility is very important to Google. We have published VPATs for our services and have a page devoted to our accessibility efforts. More information and Section 508 VPAT documents to support compliance can be found at: http://www.google.com/accessibility.

**e)** Will your system afford options for individualized institutional branding?

**SADA Systems:**

Google Apps for Education supports custom logo and colors branding for the web interface to Gmail, Google Calendar, and other Google Apps products.

**f)** What aspects of the display will be User-customizable, including display as format (coloring, font styles, etc.) of calendar events, e-mail messages, contacts and tasks based on categorization, sender, recipient, etc.?

**SADA Systems:**

The Google Apps user interface is highly customizable. This extends to, but is not limited to, labs, filters, labels, priority Inbox, conversational threading on/off in Gmail to date and time format, custom views, custom notification and sharing controls in Calendar.

**g)** Can you offer campus and inter-institutional operability between native clients (e.g. Eudora, Outlook, Apple E-mail), such that features like calendar free/busy time and shared e-mail folders can be accessible among institutions? What is your end-User support model?

**SADA Systems:**

Interoperability and cross-platform support are that core of Google Apps. Interoperability across institutions will go far beyond exchanging emails, attachments, and calendar entries. Without any special software, institutions will be able to seamless share calendars, free/busy information, real-time chat (text, voice and video), real-time collaborative documents (Google Docs), standard documents (MS Office, OpenOffice, RTF, CSV, PDF, etc), files of any type, online folders and even web sites/portals across institutions. Further, Google Groups can span multiple institutions to create private or public forums and permissions structures for the shared resources mentioned.
In terms of interoperability with native clients, Google provides SMTP, POP and IMAP email access for compatibility with desktop products such as Eudora, Thunderbird and Apple Mail. For Windows Microsoft Outlook 2003-2010, Google provides the Google Apps Sync for Microsoft Outlook tool to synchronize mail, calendar and contacts (http://tools.google.com/dlpage/gappssync).

Since Google Apps is delivered through the web browser and offers standards-based support for desktop software, it is truly a cross-platform solutions. End-users can choose Windows, Mac, Unix, mobile devices or any combination as their access vehicles.

Additionally, with Google Apps, institutions will benefit from all end-users being on the same “version” of the software. This will create interoperability, knowledge transfer and support advantages since end-users could work seamlessly in any institution’s environment.

2. Specific Component Functionality

Provide details on how the proposed solution meets the following criteria:

a) E-mail. Describe how your product offers the following basic e-mail functionality:

(1) Ability to send, receive, format and forward messages and attachments

**SADA Systems:**

Gmail gives users the ability to send, receive and forward messages to whomever the like. Gmail offers users the ability to switch between plain text and rich text formatting. The user preference is maintained for subsequently composed emails, and may be switched at any time.

(2) Ability for Users to define and manage e-mail filter rules that run on the server to automatically delete, redirect or file messages into folders.

**SADA Systems:**

In Gmail, there are labels to allow users to better organize their email. Labels are similar to folders, but there is one key difference: with folders, a user can put one email in only one folder; however, with labels the user is able to tag an email with multiple labels. Users can customize Gmail to automatically filter messages to the Trash for deletion, and can set up filters to send emails to various labels as they see fit.

(3) Ability to manage folders and copy, move, and store information to desktop or local storage.

**SADA Systems:**

Users can export email, attachments, and Google Docs to their desktop or local storage in industry standard formats.

- Attachments can be saved directly in their native format
- Emails and documents can be downloaded in RDF, PDF, Text, Open Office, Word, and HTML formats
- Spreadsheets can be downloaded in CSV, PDF, Text, Open Office, Excel, and HTML formats
- Presentations can be downloaded in PDF, Text, and PowerPoint formats

Users can configure the default download location in the browser settings.
Ability for Users to have two or more e-mail aliases in addition to their primary university provided ID, and to send e-mail from group accounts.

**SADA Systems:**

Google Apps enables you to create alternate personal addresses (nicknames) for a user based on the username or the domain. For example, the user bill@university.edu might also want to receive email addressed to william@university.edu. If you create william@university.edu as an email alias for bill@university.edu, Google Apps will deliver email for both of these addresses to the same Gmail inbox.

A user’s primary email address has special status: it is the address the user enters to log into Google Apps, to sync with his or her mobile device, and to share Google Docs and Sites.

If your Google Apps account has multiple domain names associated with it, a user’s email aliases can include email addresses in other domains that are part of your account. For example, bill@university.edu could have the email alias bill@college.edu as long as someone else does not already have that email address.

Users can apply the filters described earlier to automatically label, archive, delete, star, or forward their mail, even keep it out of Spam, based on these alternate personal addresses.

**Ability for Users to restore deleted e-mail messages and folders directly and without intervention from the system administrator.**

**SADA Systems:**

Each user gets 7.4 GB of email and IM storage, so they no longer have to delete emails. Instead, they can simply archive them out of their inbox; archived emails can be searched and retrieved without system administrator intervention. Also, deleted messages will remain in the Trash for 30 days, where it can be moved back to the Inbox.

Items deleted by an end user are recoverable by the end user without admin intervention for 30 days. End users would recover these messages by simply dragging and dropping or clicking a button to move them out of the trash.

For situations in which the end user "empties" items from the trash, those items would not be recoverable by the end user. However, in conjunction with Google Message Discovery, those messages could be recovered by a client-side administrator for up to 10 years. Google Message Discovery is priced separately.

**Other features you wish to highlight.**

**SADA Systems:**

Google has unrivaled search capabilities built into its applications. This search capability allows for complex queries including Boolean operators.

**Personal Calendars and Task Lists.** Provide details on how the proposed solution meets the following criteria:

**Basic calendaring functionality, including but not limited to inviting Users, groups and resources to events. Users should be able to see the free/busy times for all invitees, including all...**
the members of pre-existing and ad hoc groups (unless restricted by access controls). The system should be able to automatically schedule meetings, support a variety of types of recurring events, and permit the viewing or hiding of appointment details.

**SADA Systems:**

Inviting users, groups, and resources to events: Google Calendar lets users create invitations for special events, send those invitations to friends, and keep track of responses and comments all in one place. Users can also allow guests to modify the event.

In addition to basic calendaring features listed, Google Calendar lets users do the following:

1. **Share your schedule and easily schedule appointments** - Let your co-workers, family, and friends see your calendar, and view schedules that others have shared with you. When you know when everyone is free or busy, scheduling is a snap. Overlay multiple calendars to see when people are available. Google Calendar sends invitations and manages RSVPs. Calendars can be shared company-wide or with select co-workers. A range of sharing permission controls help maintain security and privacy. Publicize external company events by publishing a calendar to make it searchable in the Google Calendar gallery. Easily embed calendars into web pages.
2. **Get your calendar on the go** - With two-way syncing to your mobile phone's built-in calendar or a mobile version of Google Calendar that's made for the small screen, you can access your calendar while you're away from your desk. View and edit event details, add new events, and invite guests on mobile devices like the BlackBerry and iPhone. Even receive calendar notifications via SMS.
3. **Never forget another event again** - Customizable reminders help you stay on schedule. You can choose to be notified by email or get a text message sent right to your mobile phone.
4. **Send invitations and track RSVPs** - Invite other people to events on your calendar. Guests can RSVP to your events by email or via Google Calendar.
5. **Sync with your desktop applications** - Access your calendar however and whenever you want by syncing events with Microsoft Outlook, Apple iCal and Mozilla Sunbird.
6. **Work offline** - Know where you're supposed to be even when you don't have internet access. With offline access, you can view a read-only version of your calendar no matter where you are.
7. **Integrate with your email system** - Google Calendar is integrated into Gmail and interoperable with popular calendar applications.

(2) The calendar client(s) should provide daily, weekly and monthly views, and allow scrolling through and printing of calendars by day, week and month and the ability to view multiple calendars at the same time (both personal and global).

**SADA Systems:**

Google Calendar has day, week, month, 2 or 4 day, and agenda views that allow scrolling through and printing. Also, users have the ability to view multiple calendars (personal and global) at the same time.

(3) Ability to print calendar events such that all relevant information, including meeting location, conference call numbers, document links, etc. are included.

**SADA Systems:**
Printing calendars locally in standard formats including agenda is supported; the "Custom View" feature along with the ability to print to PDF allow for additional formats and user-defined formats including the Franklin format.

Google Calendar has the ability to print all information attached to an event including name of the event, time and date, location, source calendar, description (which can include any information user inputs), any attachments, list of guests, and list of reminders.

4 Ability to schedule resources, including but not limited to facilities, conference rooms, equipment and virtual venues (IM chat rooms, conference call bridges, etc); ability to support access controls for each type by Users or groups.

SADA Systems:

Google calendar supports scheduling any resource, such as facilities, conference rooms, equipment, and virtual venues. The resource calendar’s administrator can set visibility to the calendar at an organization or individual user level, including whether users are only able to see free/busy or all event details. The ability to view or utilize a resources may be restricted.

In addition, extra data about resources is supported through links to resource descriptions defined in HTML. Typically, administrators should also include information such as location, occupancy limits, and availability of audio-visual equipment in the resource name to facilitate finding suitable resources: the calendar automatically displays resources hierarchically based on this taxonomy.

Users can search for and see free/busy times for all invitees; they can also overlay multiple calendars to see when people and resources are available, subject to ACL's; this includes group calendars.

The "Find a Time" feature will automatically search for an optimal time based on people, group, and resource calendars; Google Calendar automatically sends invitations and manages RSVPs. Recurring events such as weekly, monthly, every Monday, Wednesday, Friday are supported.

5 Ability to support task lists at multiple priority levels.

SADA Systems:

Infinite priority levels are supported by moving tasks up and down the priority list.

c) Address Book/Contact Management. Provide details on how the proposed solution meets the following criteria:

1 Basic contact management functionality, including but not limited to last name, first name, middle initial, department, title, phone number, fax number, e-mailing address, e-mail address, business address, contact log, notes, etc.

SADA Systems:

Contacts can have all indicated fields and more with the “custom” field that allows users to create their own category in a contact.

2 Ability to synchronize contact information with desktop applications;

SADA Systems:
Supported. Contacts can be synchronized with desktop applications such as Outlook (via MAPI) or any POP, IMAP or ActiveSync client. Additionally, Google Apps Contacts integrate with native mobile client applications on the following platforms: Blackberry, Android, iPhone, Nokia E Series, Windows Mobile or PalmOS (for a complete list, see the link below). Further, Contacts are available on mobile-specific form factor web interfaces for any mobile web browser.

For more information please see:

http://www.google.com/mobile/


(3) Ability to share contact lists with other Users or groups.

**SADA Systems:**

Users can export contact lists to other users and import their contact lists. Administrators can also enable contact sharing for the domain, in which case all users created in the domain are shared contacts, similar to what is commonly referred to as a global address list.

3. Overall Solution Functionality and Interoperability

Provide details on how proposed solution meets the following criteria:

a) Delegation, Shared Use and Workflow. The system should provide a facility to delegate administration of User and group e-mailboxes, calendars, quotas, etc. to departmental administrators.

**SADA Systems:**

Google Apps let admins delegate administration of users and groups to whomever they choose.

(1) Describe how the system supports the creation and management of shared e-mailboxes, calendars, address books, and task lists with multiple owners and access control lists that can include User’s ad hoc groups.

**SADA Systems:**

Google's solution allows for shared calendars with a variety of access levels on an individual level. Gmail also allows mailbox delegation for up to 10 users per mailbox. Google Groups can be used to create shared mailboxes per this article:

http://www.google.com/support/a/bin/answer.py?hl=en&answer=167430

Users have the ability to generate task lists which can then be emailed (shared) to other users for consumption into their task lists. Additionally, tasks may be overlaid in users' calendars with reminders and due dates.

(2) Describe how the system supports the ability to delegate e-mail, calendar, tasks, and other functionality to another staff member (i.e., proxy assignments, including e-mail/phone, appointments, resources, reminder notes, tasks, etc.)

**SADA Systems:**

Proxy (or delegate) access is available for both Email and Calendar with Google Apps. Users may delegate access to their Google Apps mail and calendar accounts to another staff member in the
organization so they can manage sharing, read, send, and delete messages or calendar
appointments on the user's behalf. For example, users can delegate e-mail rights to an admin, or
they can set up a small group mailbox.

If someone has granted access to their account to another user, the user can access it by clicking
the down-arrow next to their email address in the upper-left corner. The delegator’s email address
can be selected from the drop-down menu.

A user may retract proxy (or delegate) privileges at any point.

A similar approach can also be used for shared mailboxes with Single Sign-On (SSO). SADA Systems
has developed an add-on module to its SSO solution for San Jose State University in which
Administrators can grant permissions to delegated mailboxes to users. During the authentication
process, a user with privileges will be able to select which account he/she would like to access.

Users have the ability to generate task lists which can then be emailed to other users for
consumption (Delegation) into their task lists. Additionally, tasks may be overlaid in users' calendars with reminders and due dates.

Users can create lists of items, set due dates and notes, and even add Gmail messages directly to
Tasks. Users can also use the tasks list to keep track of listing actions such as making a list of state
agencies or outlining a paper. Users can create as many lists as they need to organize their
information.

Users can turn any Gmail message into a task with one click. They can also turn any bulleted list
from another user - whether from Gmail or another system - directly into a task list.

Another option would be for users to leverage Google Docs to create collaborative documents
acting as shared task lists. Users can create documents as task lists, share them with one or more
collaborators and eventually subscribe to changes in order to be reminded every time any
collaborator adds an item to a task list or an item is marked as completed. Google Apps provides
numerous ways ‘out of the box’ to achieve the desired functionality but also supports the following
method as well.

(3) Describe how the system supports the ability for User-controlled setting of proxy access
limitations (e.g., Read/Write; Subscribe to Alarms and Appointments, Modify Options, Rules, and
Folders).

SADA Systems:

Users can delegate access to your Gmail account to someone else in their organization so they can
read, send, and delete messages on their behalf. For example, users can delegate e-mail rights to
an admin, or you can set up a small group mailbox. Delivered emails include proxy information for
the recipient.

(4) Describe how the system either supports multiple calendars, address books and task lists per
User, or allows Users to categorize calendar events, contacts and tasks. In either case, the
proposed solution should support sharing of these objects, with User configurable access controls.

SADA Systems:

Users can view multiple (personal, shared, and global) calendars at the same time. Google
calendars are color-coded by default so it’s easy to view and overlay calendars at the same time.
Google calendar supports multiple different viewing modes as well; day, week, month, year, and custom range.

- Personal calendars are the default users' calendars
- Users may also create additional calendars to share with a group or a list of individuals, as well as global calendars shared with the entire organization

Users can categorize contacts and tasks easily in Google Apps. Calendars, contacts, and tasks are can be shared with user configurable controls.

**b) Personal, Group and Global Address Books.** Personal and group address books should all be available within the e-mail and calendaring functions to any authorized Users. A common global address book, bound to the university’s existing directory services, should also be available to all Users and accessible within the e-mail and calendar functions. Additionally, please describe whether your solution would enable Virginia Tech to share global address books inter-institutionally. Any clients delivered with the solution should provide auto-completion for common address book lookup fields, such as names and addresses.

**SADA Systems:**

Google Apps domains have one Global Address List (GAL) per domain. However, the Google Apps Directory Sync (GADS) tool and the **ability to integrate multiple LDAP systems to provide consolidated GAL to end users.**

With Google Apps Directory Sync, you can automatically provision users, groups and non-Virginia Tech contacts based on the user data in any LDAP server. GADS supports LDAP servers such as Microsoft Active Directory and Novell eDirectory. Google Apps Directory Sync connects to your Google Apps directory and adds/deletes user accounts to match your existing organizational schema.

The Google Apps Directory Sync configuration wizard guides you through customizing your synchronization and mapping of your LDAP user list to your Google Apps users, nicknames, shared contacts and groups. You can also synchronize rich user profile data like home/work/mobile phone numbers, addresses and job titles. To manage your synchronization, you can perform test synchronizations, and configure change limits, notifications, and scheduled synchronizations.

For more information please see: [http://www.google.com/support/a/bin/answer.py?answer=106368](http://www.google.com/support/a/bin/answer.py?answer=106368)

Administrators can enable contact sharing to allow each user in a Google Apps domain to have easy access to all other users in the domain. The shared contact list is similar to what is commonly referred to as a global address list.

Through Google Contacts, there is a searchable directory that can be enabled. When typing an email or sending a calendar invite, there is an auto-complete function which will query these contacts. Through the Provisioning API or the Google Apps Directory Sync tool, you can ensure that these contacts are updated via Virginia Tech’s directory.

**c) Categorization/Tagging.** A User should be able to apply multiple customizable categories or tags to e-mail messages, address book entries, and calendar events and tasks.

**SADA Systems:**

Google Apps support the use of labels in Gmail, groups in Google Contacts, multiple calendars in Google Calendar, and folders in Google Docs.
d) Searching and Sorting. Provide details on how the proposed solution meets the following criteria:

(1) The ability for Users to search messages, calendars and address books, either all at once or by selecting specific e-mail folders, calendars or address books.

SADA Systems:

Google has unrivaled search capabilities built into its applications. This search capability allows for complex queries including Boolean operators. Users can easily search messages, calendars, address books, and docs. Gmail now has a lab that can be activated that lets users search in Gmail, Google Docs, and Google Sites simultaneously, all from one place.

(2) The ability for Users to specify multiple search criteria, including searching for resources using the metadata.

SADA Systems:

Google has unrivaled search capabilities built into its applications. This search capability allows for complex queries including Boolean operators. User simply type in whatever criteria they wish and Google will search for items that contain those keywords.

(3) The ability within the web e-mail interface for Users to sort folders by various criteria (sender, subject, date, etc.), and should support displaying messages in threads.

SADA Systems:

Google Apps support the use of labels in Gmail that can be set up with any or all of the following criteria “From”, “To”, “Subject”, “Has the words”, “Doesn’t have”, and “Has attachment”. Google also supports displaying messages in threads.

(4) The use of indexing or related technologies to accelerate e-mailbox and calendar searches.

SADA Systems:

Google has unrivaled search capabilities built into its applications. This search capability allows for complex queries including Boolean operators.

Additionally, there are labels to allow users to better organize their email. Labels are similar to folders, but there is one key difference: with folders, a user can put one email in only one folder; however, with labels the user is able to tag an email with multiple labels.

4. Anti-spam, Virus Protection and Open Relays

Provide details on how the proposed solution meets the following criteria:

a) How will you enable filtering of incoming and outgoing e-mail through an anti-virus scanner capable of completely quarantining infected messages? Describe in detail the quarantine response employed by your solution (e.g., “messages flagged as suspicious are placed in a quarantine area for up to 14 days; daily or weekly e-mail notifications are sent to the User; and the User connects to a Web-based administration site to delete or release a message.”) Are the scanner’s virus signatures updated at least daily? Does the solution allow the university to additionally route incoming messages through its own server, if desired, for additional filtering? Are the scanner’s virus signatures updated at least daily?

SADA Systems:
There are two levels of spam, phishing, and virus filtering available with Google Apps.

Google Apps includes Gmail-based spam, phishing, and virus protection for all messages routed to Google Apps, suppressing malicious messages and automatically routing spam to Gmail’s Spam Folder. This is automatic, effective, and requires no configuration or maintenance on the part of the customer to maintain. Users have the option to mark messages as spam, which is then used as an input into the filtering process; the system does not rely on this step.

Customers requiring greater control over the filtering behavior for their users may make use of Google Message Security, an additional service available to Google Apps customers.

The Google Message Security (additional fees apply) service detects malicious messages such as spam, phishing attacks, or viruses by applying hundreds of rules to each message that passes through the data center. The service blocks obvious spam immediately, then diverts borderline spam to a Spam folder or a Quarantine Summary for later evaluation. From there, users can review individual messages in their Message Center or view the Quarantine Summary for any legitimate messages that were falsely quarantined and need to be restored to the user’s Inbox. Otherwise, spam is deleted automatically after a period of time.

b) Provide details about what products you will use for spam filtering and give a detailed spam filtering options (e.g., “messages flagged as suspicious are, at the Users option, either deleted or placed into a separate folder for up to 14 days; and the User can set the sensitivity for spam rankings via settings in the LDAP directory.) Will the proposed solution work with the university’s existing anti-spam e-mail gateways (Mirapoint Junkmail Manager) and filter messages marked as spam by the university gateway into separate folders? How do you ensure that spam definitions are kept up to date?

**SADA Systems:**

There are two levels of spam, phishing, and virus filtering available with Google Apps.

Google Apps includes Gmail-based spam, phishing, and virus protection for all messages routed to Google Apps, suppressing malicious messages and automatically routing spam to Gmail’s Spam Folder. This is automatic, effective, and requires no configuration or maintenance on the part of the customer to maintain. Users have the option to mark messages as spam, which is then used as an input into the filtering process; the system does not rely on this step.

Customers requiring greater control over the filtering behavior for their users may make use of Google Message Security, an additional service available to Google Apps customers.

The Google Message Security (additional fees apply) service detects malicious messages such as spam, phishing attacks, or viruses by applying hundreds of rules to each message that passes through the data center. The service blocks obvious spam immediately, then diverts borderline spam to a Spam folder or a Quarantine Summary for later evaluation. From there, users can review individual messages in their Message Center or view the Quarantine Summary for any legitimate messages that were falsely quarantined and need to be restored to the user’s Inbox. Otherwise, spam is deleted automatically after a period of time.

c) Does the proposed solution allow administrators to define global filters that can be applied to all incoming or outgoing messages for all Users?

**SADA Systems:**
GMail provides its own spam, virus, and phishing scam filtering technologies. Messages from blacklisted hosts are not delivered to users. Our technology places probable spam in a folder, where it is kept for 30 days and then deleted. Users can help train our spam filter by reporting spam that arrives at their Inbox as well as identifying non-spam messages placed in the spam folder. Our service also disallows users from downloading messages and files which are virus infected.

In order to allow admins to define global filters, Google Message Security or Discovery would need to be purchased. Your Message Security and Message Discovery services include Content Manager, in which you can use to create custom content filters for email. These filters can block or quarantine messages with specific words or phrases or even unique patterns of letters or numbers. You can set up content filters for both inbound and outbound email. Filters always apply to all users in a user organization.

d) Does the proposed solution support white-lists, blacklists, and auto-deletion, controlled at the individual Users level and at the local system administrator level?

**SADA Systems:**

Google Apps allows white-lists. When an admin adds an IP address to an email whitelisted, mails sent from this IP address will generally not be marked spam. At this time, it is not possible to whitelist specific users based on their email address or domain name. Please note that email whitelists are not exclusive. If you create a whitelist for your Google Apps account, it will affect your entire domain. There's currently no functionality in place for you or your users to only receive mail from a self-defined list of senders.

Messages from blacklisted hosts are not delivered to users. Our technology places probable spam in a folder, where it is kept for 30 days and then deleted. Users can help train our spam filter by reporting spam that arrives at their Inbox as well as identifying non-spam messages placed in the spam folder. Our service also disallows users from downloading messages and files which are virus infected.

e) Does the proposed solution restrict open relaying, including multilevel relaying (i.e., it must not accept or deliver e-mail for non-local addresses, and must not accept non-local e-mail from another system which accepts e-mail from non-local clients)?

**SADA Systems:**

Google Apps is not able to operate as an open relay. Only a Google Apps user who has successfully authenticated may send an email outside of the domain via the Google Apps SMTP system.

5. Protocols and Standards

Please list all e-mail protocols supported, including but not limited to IETF E-mail standards (RFC2821 - SMTP, RFC2822 – Internet Message Format, RFC4511 - LDAP). We seek standards-based solutions; therefore, please provide technical details identifying which protocols you can support and how, including those identified in VI.B.5 and any others relevant standards or protocols.

**SADA Systems:**

Google designs products using industry best practices and non-proprietary standards, which result in a standards-compliant communication solution. In addition to the protocols specified in VI.B.5, Google Apps supports a variety of industry standards including; SMTP, MIME, IMAP, POP, TLS, MAPI, ActiveSync,
Blackberry BES, iCal, XMPP, LDAP, SAML, SSL, OpenID, OAuth, HTML5, XML, XSLT, Atom, RSS, YAML, JDO, JPA, JDBC.

**F. Service Levels**

Institutional e-mail and calendar systems are expected to have high availability. In certain cases, faculty are also clinicians and service levels have direct bearing on clinical care capabilities. During campus emergencies rapid dissemination of e-mail is critical to campus safety plans. (See VI.B.7). Other core business functions are significantly impacted during E-mail and calendar outages.

1. **Performance and Availability**

What is your basic service model? If you believe you can offer better than industry-standard services, describe why and how.

**a) The proposed solution should deliver individual e-mail within 7 days of contract signing.**

**SADA Systems:**

When starting a Google Apps deployment and migration project, it usually takes 2 weeks to ‘ramp up’ and begin work. This includes full discovery of the current email environment, refining scope, development of a project plan, prepping the environment and completing the required deliverables to execute the deployment and migration. However, SADA can work within the time restraints that are required.

**b) What has been your system availability and how do you measure it (e.g., 99.9%, 99.95%, 99.99%, 99.995) for all Users over the past three years (or the duration of its existence, if less than 3 years)? What would be the functional and financial effect of increasing or decreasing the system guarantee/reliability by “one 9” or “half a 9” of reliability, relative to the actual measured three year availability? (E.g., increasing from an actual measured performance of 99.9% to 99.95% or 99.99%; decreasing from an actual measured performance of 99.99% to 99.9% or 99.95%). Please provide uptimes for your system on a month-by-month basis over the past 12 months. What fault tolerance, failover or other measures do you offer that provide continuity and redundancy to ensure availability of services?**

**SADA Systems:**

Google guarantees a 99.9% uptime SLA as part of its Education Edition (with downtime defined as >5% server side error rate). Information on the SLA can be found at http://www.google.com/apps/intl/en/terms/sla.html. The actual uptime Google achieved in 2010 was 99.984%, equaling 7 minutes of downtime a month.

**c) The proposed solution must support the peak User load 20,000 simultaneous sessions with no noticeable delay of any operation.**

**SADA Systems:**

Google's dedicated global data network has multiple nodes in the US, and its cold-potato model ensures that once a packet hits the network it remains on the network as long as possible. Organizations will typically see the highest level of service for their Google services even when other areas of the internet are experiencing issues.
d) Describe your proposed incident response procedures, addressing specifically how you will manage unscheduled outages, interrupted services, or a customer's report of degradation in service. Include specifics as to how you will investigate and resolve service level interruptions.

**SADA Systems:**

Google provides the web-based Google Apps Help Center contains answers to most commonly asked end-user questions and ample self-service material in form of articles and tutorial videos. For the large majority of questions, chances are that someone else has asked it and that Google already has an answer appropriate for your end users in our help centers, minimizing the need for them to contact the help desk. Google continuously updates these FAQs as new features are released. End users can also search or post questions on the Help Forum, which is very active and moderated by Google employees. Information is searchable and categorized by topic so end users can easily find others who have similar questions.

Google Apps offers the following incident levels:

P1 - VERY HIGH IMPACT - Product/Service Unusable in Production.

P2 - HIGH IMPACT - Use of Product/Service Severely Impaired.

P3 - MEDIUM IMPACT - Use of Product/Service Partially Impaired.

Google offers a support SLA with respect to the first response time for an incident. P1 Priority support Requests are responded to with a target initial response time of one hour and are responded to 24 x 7. If contact is made for a P1 Priority support Request on a weekend or applicable holiday, a phone call is needed to trigger a return support response. P2 & P3 Priority support Requests are responded to during business hours of the location to which the Requests are assigned. P2 Priority support Requests will be responded to with an initial target response time of 1 business day or less.


Google's Enterprise Support Portal is available 24x7 year-round for incidents to be submitted. Google's End User and Admin Help centers are also available 24x7 year-round.


1.1. Customer Efforts to Fix Errors. Prior to making a request to Google, Customer will use reasonable efforts to fix any error, bug, malfunction or network connectivity defect without escalation to Google. Thereafter, a Customer Contact may submit a written request for technical support through the online help center or support portal as provided by Google, or by phone.

1.2. Characterization of Requests. Customers designate priority upon submission of Requests. Upon receiving a request from Customer Contact, Google will determine whether the request is a "Service Unusable," "Standard Request" or a "Feature Request" (as defined in Section 7). Any such determination made by Google is final and binding on Customer. Google reserves the right to change Customer’s Priority designation if Google believes that Customer’s designation is incorrect and will inform Customer of any such change in its response to the support Request. Customer may appeal any such reclassification to Google’s Support management for review through any available support channel.
1.3. Procedures for Acknowledgement and Resolution of Requests. When making a Request, Customer will provide requested diagnostic information including but not limited to: (i) describing the problem, the configuration, and Customer’s network; providing relevant data; and (iii) communicating further via email or telephone to answer questions and assist Google Support Personnel as appropriate.

1.4. Request Acknowledgement. Google may respond to a Request by acknowledging receipt of the Request. Customer acknowledges and understands that Google may be unable to provide answers to, or resolve all, Requests.

1.5. Feature Requests. If Google deems a Request as a Feature Request, Google will log such Request for consideration to add to a future update or release of the Services and will consider the matter closed. Google is under no obligation to respond to or resolve any Feature Request or to include any such Feature Request in any future update or release.

e) Please describe the way in which feature enhancements are released to your product (e.g., separate beta testing vs. en-masse beta testing with the entire population). How will the Customer and End Users be notified of upcoming or released product features?

**SADA Systems:**

After deploying Google Apps, the University will be assigned a Partnership Manager who will conduct confidential road map presentations with the University to keep them informed of the strategic direction of the product. In addition, the University can elect to participate in our Trusted Tester program. This will give them the option to test new products and features that are not yet broadly released.

Notifications of upcoming or released product features are available in multiple ways. Users can subscribe to be notified via email, or they visit [http://whatsnew.googleapps.com/](http://whatsnew.googleapps.com/) to view the newest and upcoming releases.

f) In the event of an unscheduled outage, please describe your process of informing Customer and End Users of root cause and preventative steps to avoid reoccurrence of similar outages.

**SADA Systems:**

The Google Apps Status Dashboard provides information on service disruptions and outages as well as additional information, where applicable, by service type (e.g. mail, calendar).

Organizations can subscribe to notifications via an RSS feed.

For Google Apps customers, our recovery point objective (RPO) design target is zero, and our recovery time objective (RTO) design target is instant failover. Gmail, Google Calendar, Google Talk, Google Groups, Google Docs and Google Sites have a 99.9% uptime guarantee, and our actual reliability has been significantly higher than this commitment.

g) Please list the primary metrics available for the e-mail and calendar applications.

**SADA Systems:**

Google Apps includes reporting that provides visibility into service usage across your organization. The Administration Console makes available usage information on a per-user basis, as well programmatically via the Google Apps Reporting API. Some of the key reporting available includes: activity status for each account (whether or not email has been accessed), email storage usage versus...
quota (per domain and per user), the number of users using the default Gmail interface versus another email client, and Quota Limit Account reporting with lists of accounts approaching or have exceeding their disk space quota.

Google Analytics can be used to track usage of Google Apps component services at a more granular level. Traffic (visitor behavior) on your sites, documents, presentations, and spreadsheets can be tracked and analyzed.

Finally, Google Message Security provides reporting with extensive analysis into email message traffic, spam, virus, and usage over a day or week. The following reports are produced by the message security service: daily reports for the previous calendar day, custom date range reports from the past 6 weeks, current day traffic logs for Content Manager and Outbound Messages.

h) Describe your maintenance plan for both hardware and software in non-emergency situations. How will you ensure minimal interference with our services? Will you coordinate all regular maintenance with customer scheduling and needs, including consideration of individual institution’s academic calendar? If a delay is requested by a customer, are you prepared to advise us regarding the effect of any such delay will have on the services, services levels, and/or fees?

SADA Systems:

There will be no more than twelve hours of planned / scheduled downtime per calendar year. Customers would be notified of planned / scheduled downtime at least five days prior to the commencement of such downtime. Since August 2008, Google Apps uptime has been 99.98% with no (zero minutes) of scheduled downtime. All service interruptions and current service availability are published publicly at http://www.google.com/appsstatus.

i) Please describe your change control procedures and how the Customer and End Users receive prior notification of scheduled downtime for maintenance or upgrades.

SADA Systems:

There will be no more than twelve hours of planned / scheduled downtime per calendar year. Customers would be notified of planned / scheduled downtime at least five days prior to the commencement of such downtime. Since August 2008, Google Apps uptime has been 99.98% with no (e.g. zero minutes) of scheduled downtime. All service interruptions and current service availability are published publicly at http://www.google.com/appsstatus.


j) The proposed solution must support Virginia Tech’s emergency broadcast system as detailed in VI.B.7. Please provide specific information regarding your latencies, basic confirmations, and the SLA standards you can commit to in this area.

SADA Systems:

Please see response detailed in VI.B.7.

k) Please share your annual testing plan for Disaster Recovery and/or business continuity.

SADA Systems:
Google has many mitigation strategies in place for disaster recovery. Google has real-time replication of data across geographically disparate data centers. Google maintains a number of geographically distributed data centers. Google will physically secure datacenters, maintain data on Google-owned servers, and replicate Apps data across multiple systems within a single data center as well as back up data in a Google-owned secondary data center. The secondary data center will be in a different geographic disaster area from the first. The client's data will reside in at least two Google data centers. These data center will be in different geographic disaster zones. Our Data Centers are redundant and can shift to a user's secondary data center. To minimize service interruption due to hardware failure, natural disaster, or other catastrophe, Google implemented comprehensive disaster recovery program at all of its data centers.

This program includes multiple components to eliminate single point-of-failure, including the following: Distributed data center architecture Google operates a geographically distributed set of data centers ensure swift failover. Management of the data centers is also distributed to provide location-independent, around-the-clock coverage, and system administration. Data replication and backup To help ensure availability in the event of a disaster, all of the client's data is replicated to separate systems in different data centers. If a disaster occurred that affected one data center, the client's data will be served from the secondary data center. The data between a user's primary data center and their secondary data center is constantly replicated in real time. There is nothing that the client or a client employee needs to do to act upon to invoke this. We have built monitoring tools that help look for a malfunction or even slowness in a datacenter and automatically, push users to their secondary data center. The only requirement is that client still have internet access. In addition to the redundancy of data and no single point of failure model for our data centers. We have also have a business continuity plan for our corporate office in Mountain View, CA. We have a plan that accounts for having suffered a major calamity, and people and services in are unavailable for 30+ days. This plan insures continued operations or our services to our customers.

2. Storage, individual e-mail quotas, and scalability

What range of capacity can you deliver and at what cost? Specify costs if capacity were set at 2GB, 10GB, or at 25GB. Describe how your proposed solution will support archiving old inactive messages to a lower cost message store. Archiving should be configurable per User and group.

**SADA Systems:**

Google Apps for Education is provided completely free of cost for use by students, faculty, staff and alumni for accredited nonprofit K-12 schools, Colleges and Universities. The Gmail service currently provides 7.4 GB of storage per mailbox. Archiving beyond this 7.4 GB of storage is available via Google Message Discovery to the University at 66% discount. GMD is available on a per user basis.

3. User Support Services

**SADA Systems:**


Describe in detail your end-User support services, including but not limited to,

- telephone support;

**SADA Systems:**
Google Apps for Education customers have access to 24x7 support free of charge. This includes online support and telephone support for systems critical issues.

b) online support;

**SADA Systems:**

Google provides the web-based Google Apps Help Center contains answers to most commonly asked end-user questions and ample self-service material in form of articles and tutorial videos. For the large majority of questions, chances are that someone else has asked it and that Google already has an answer appropriate for your end users in our help centers, minimizing the need for them to contact the help desk. Google continuously updates these FAQs as new features are released. End users can also search or post questions on the Help Forum, which is very active and moderated by Google employees. Information is searchable and categorized by topic so end users can easily find others who have similar questions.

c) campus training;

**SADA Systems:**

Campus HelpDesk training is available. Details can be found in section VI.F.5.

d) availability (e.g., 24-hour technical phone contact); and

**SADA Systems:**

Google Apps for Education customers have access to 24x7 support free of charge.

e) when and how the campus Help Desk can escalate to you.

**SADA Systems:**

Campus Help Desk may escalate to Google at any time. Google will provide access to help center and phone support for customers on a 24 x 7 basis. 1 Priority support Requests are responded to with a target initial response time of one hour and are responded to 24 x 7. If contact is made for a P1 Priority support Request on a weekend or applicable holiday, a phone call is needed to trigger a return support response. P2, P3 & P4 Priority support Requests are responded to during business hours of the location to which the Requests are assigned. P2 Priority support Requests will be responded to with an initial target response time of 1 business day or less.

"Priority" means the level of impact a Request is having on Customer’s operations and is used to establish target response times.

- P1: Critical Impact – Service Unusable in Production
- P2: High Impact – Service Use Severely Impaired
- P3: Medium Impact – Service Use Partially Impaired
- P4: Low Impact – Service Fully Usable

Furthermore SADA Systems can also provide support on most Google related issues and help escalate them to Google’s tier two support.

4. Documentation
Within one week of contract award, the Vendor shall supply Virginia Tech with complete documentation, service manuals, and appropriate system engineering bulletins for all components proposed in the response to this RFP, both hardware and software. Documentation must be received in machine readable form (e.g., on Compact Discs) and appropriate for loading on university-owned servers.

**SADA Systems:**

Acknowledged.

5. Training

Vendor should include online training materials, training for three (3) e-mail and calendar administrators, and “train the trainer” training for three (3) training professional from Virginia Tech. If this training is offered as separate, off-site courses, Vendor should include course descriptions and schedule of offered courses thru 12/2011.

**SADA Systems:**

Making the switch to a new communications platform is an important change for Virginia Tech, and you want your deployment to be as smooth as possible, with minimal disruption to productivity and daily operations. You know that some of your users are apprehensive about the change, and many will need help getting started, no matter how much documentation and training you provide beforehand. To ensure the best possible deployment experience for both your users and support staff, you need a solid support plan in place on “Day One.”

SADA will develop a “Google Guides” program in which Virginia Tech internal training staff will be trained on Google Apps and how to train others to use the product. Curriculum developed during the pilot may be re-used at any time by Virginia Tech’s training team. SADA will deliver the training via online webinar, but can also deliver the training on-site, at the request of the University.

- Training for Trainers/Google Guides – Messaging. For anyone who will be asked to train others. Each session includes: Intro to Apps, Gmail, Contacts, Chat, Tasks.
- Training for Trainers/Google Guides – Collaboration Part I. For anyone who will be asked to train others. Each session includes: Calendar, Docs.
- Training for Trainers/Google Guides – Collaboration Part II. For anyone who will be asked to train others. Each session includes: Groups, Sites.

SADA will develop a wiki-type web based knowledge repository for Google Apps deployment data which will provide a ready reference for administrators and help-desk/call center staff. The knowledge repository will be built on Google sites technology, a part of Google Apps - and is fully hosted and supported by Google.

Content will be customized and will contain deployment-specific information. The knowledge base will be used by Administrators as reference and by help-desk/call center staff as a resource by which to support end-users.

- Training for Google Apps Administrators. For anyone with Domain Administrator Access. Each session includes: Google Apps Control Panel and Basic Troubleshooting.
- Training for Google Apps HelpDesk Staff. For anyone who will asked to troubleshoot Google Apps for End Users. Each session includes: Google Apps Basic Troubleshooting.
SADA understands that the Virginia Tech Internal IT group has previous experience migrating to users to a Google solution. Therefore, the necessary training time required by the University may be less than what SADA recommends. Please note that SADA will work with the University to design a training package that will fit the needs of Virginia Tech staff.

SADA recommends the following package for Virginia Tech:

- Curriculum Customization
  - For Trainers / End-Users
  - For Admins/HelpDesk
  - Google Site Creation
    - Presentation Integration
    - End-User and Admin Quizzes
  - Training experience satisfaction surveys
- 2 days on-site: Sample Schedule: Can be customized
  - 1 day - Admin / HelpDesk Training
  - 1 days - End Users / Trainers Training
  - 3 Remote Webinar Sessions - 2 hours each

If client chooses on-site option the following travel expenses/terms apply:

- SADA will bill client for the following:
  - Travel time @ $1,500.00 per staff member per day of traveling
  - Minimal Air Travel Requirements:
    - Coach Class Ticket from Los Angeles
    - No more than one stop/connection
  - Business Class Hotel Room near client site for each staff member
- Client to provide or arrange for ground transportation to/from hotel - work site(s) while staff on-site
- Client may arrange for air travel / lodging / ground transportation directly or SADA will bill client at cost.

Virginia Tech can choose the above package or decide on a different package or individual on-site or webinar classes.

G. Additional SADA Offerings

**SADA Systems**

SADA Systems offers a range of Google Apps related services. Each tool or service is listed below in detail. Pricing for these items and services, as well as prices for other items in the RFP can be found section IV.H below.

1. SADA’s QuickStart

   The initial phase of discovery, preparation and engineering is critical to a successful deployment of Google Apps in an organization. Leverage SADA’s knowledge and experience to help plan and configure Google Apps for your organization’s email, and email continuity needs. SADA will provide assistance with the set-up of the Google Apps for Education Edition account, including the following:
   - Basic discovery of the existing infrastructure provided by SADA’s Google Apps engineering team.
   - Assist with sign up for Business Edition and set up of initial Google Apps accounts.
   - Import and set-up of the initial group of account users. This can be done in-batch by SADA via CSV file.
This proposal valid for 180 days post April 4th, 2011 submission.

2. Google Message Configuration

- SADA will provision new accounts in Google Apps then develop a strategy for implementing the Postini Message Security suite of services as per client need and then activate/configure such for client.
- SADA will help configure settings for Google Message Security, Encryption, as well as Archiving to your desired requirements

3. Microsoft Outlook Sync or GASMO

- Google has developed a sync service that allows Microsoft Outlook to be configured to work with Google Apps in a simulated matter as such that Outlook views Google Apps as it would an Exchange server. SADA will help in the event of needed troubleshooting for the tool as well as providing best practices for using the Outlook Sync.

4. SADA’s User Provisioning and Sync Tool

SADA offers a choice of two methods to periodically synchronize an Identity Management data source with Google Apps Accounts, ensuring user information is always current.

- Option 1: Hosted Sync for Google Apps:
  - LDAP, Database, or CSV account provisioning and sync tool.
  - SADA will deploy its hosted batch provisioning interface which comes with full logging capabilities. The advantage to this solution is that it requires no additional infrastructure to support it.
  - CSV provisioning - Client will provide a destination for a .CSV file which will be created by the Client’s own IT resource(s) on a regular basis.
  - LDAP provisioning - Client will provide outside access to LDAP (via port 389 or a custom port)
  - Database provisioning - Client will provide outside access to database.

- Option 2: On-Premise Sync for Google Apps:
  - LDAP, Database, or CSV account provisioning and sync tool. In this scenario, SADA’s same custom tool as described in option one will reside in the Client’s environment, and can sync the accounts with an Identity Management data source on a regular interval.

5. SADA’s LDAP Group Provisioning Tool

SADA offers a choice of two methods to periodically synchronize an Identity Management data source with Google Apps, ensuring distribution group information is always current. Since a group address will "auto complete" after you start typing it only after you have sent a message to that group, our sync tool automatically adds newly created groups to Domain Shared Contacts. This approach makes groups available via "auto complete" interface to your users within 24 hours regardless of whether a user sent an email to a group or not.

- Option 1: Hosted Sync for Google Apps:
  - LDAP
  - SADA will deploy its hosted batch provisioning interface which comes with full logging capabilities. The advantage to this solution is that it requires no additional infrastructure to support it.
  - LDAP provisioning - Client will provide outside access to LDAP (via port 389 or a custom port)

- Option 2: On-Premise Sync for Google Apps:
This proposal valid for 180 days post April 4th, 2011 submission.

6. SADA's Google Apps Single Sign On Service

SADA will deploy a Single Sign-On page which allows users to log into Google Apps with the same credentials already in the LDAP server.

- Option 1: Hosted Single Sign-On Services:
  o The use of a custom log-in page for Google Apps allows the Client’s organization to:
    ▪ Manage all users from the existing LDAP based data system.
    ▪ All communication between our system and the Client’s servers is fully secure and encrypted.
    ▪ SADA sets up a custom log-in page for the Client's users based on the branding standards provided by the Client.

- Option 2: On-Premise Single Sign-On Services:
  o This option of our Single Sign-On Services Solution functions exactly as the hosted version however our application and custom page would reside on infrastructure provided by the Client.

7. SADA’s Single Sign-On Password Sync for Google Apps

- We have identified an ideal authentication mechanism that allows a seamless experience for users AND administrators to leverage LDAP & SSO without compromising user data store administration, behavior and policies.

- SADA modifies the existing SSO code by adding a synchronization module. The module works in the following way:
  o A user attempts to access a Google web application (Gmail, Calendar, Start Page, etc).
  o Google redirects user to the SSO page.
  o User signs in to the page using his/her LDAP account

- If LDAP authentication succeeds, the synchronization module captures the password that the user typed in and sends this password to Google Apps using an API Update call.

8. GAL Sync

SADA Systems has developed a tool that will make the Global Address List (GAL) that is stored in the existing LDAP server available to Google Apps users.

- SADA System’s GAL Migration Tool consists of two parts: Shared Contacts sync and User Profiles sync. The Shared Contacts and User Profiles information appears in Contacts under the client’s Directory. Information is synchronized one-way only, from LDAP to Google Apps.
- The tool can be configured to synchronize only Shared Contacts, only User Profiles, or both.
- The tool is executed in the command line and can be scheduled to run on predetermined intervals (every 24 hours).

9. Block of support

A block of time for support and advice in the deployment of Google Apps for your organization. The time doesn’t expire until it’s used up, and you get the benefit of support from SADA.

- Enterprise-level support for Google Apps
- Knowledge and experience, the SADA edge
- What you get: - Support from SADA Systems via phone, email, screenshare, and webinar - Can be used for support on any Google Apps related - Block of time never expires. - Additional blocks of time can be purchased when all time is utilized. - Requires pre-payment of full amount.
- 10 or 20 or 40 hour block of time that never expires
  - $1,450 for 10 hours of remote support
  - $2,750 for 20 hours of remote support
  - $5,250 for 40 hours of remote support

10. Mobility Strategy

- Google provides a free, robust application for a variety of mobile devices that allows users to access their Google Apps email accounts. The application includes features such as being able to switch between Gmail accounts, create mobile drafts of messages, and view message attachments, including photos, Microsoft Word documents and PDF files. The application supports devices such as BlackBerry, iPhone, Android OS, Windows Mobile and several other platforms.
- Additionally the Google Sync for Blackberry application allows users to synchronize their BlackBerry’s native calendar and contacts applications with their Google account.
- SADA will assist Client in the deployment of mobile device solutions for Google Apps by providing set-up instructions for devices as selected by Client as well as providing support to Client’s IT staff during this process. Please note that the scope of this deliverable does not include SADA setting up individual devices for Client.

H. Cost

**SADA SYSTEMS:**

SADA’s proposals are offered to Virginia Tech in a menu style format from which the University may select the appropriate services and products that will ultimately meet their objectives.

SADA’S “standard” Google Apps implementation services are all “flat fee” and by design do not constitute a “time and materials” billing structure. For custom work outside of our standard deliverables however, our hourly bill rate is $195/hour.
This proposal valid for 180 days post April 4th, 2011 submission.

### Google Apps Accounts and Other Licenses

<table>
<thead>
<tr>
<th>QTY</th>
<th>Item</th>
<th>Price</th>
<th>Total Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>78,000</td>
<td>Google Apps for Education Accounts</td>
<td>$0.00</td>
<td>FREE</td>
</tr>
<tr>
<td>TBD</td>
<td>Google Message Security</td>
<td>$4.00</td>
<td>TBD</td>
</tr>
<tr>
<td>TBD</td>
<td>Google Message Discovery – 1 Year Retention</td>
<td>$8.33</td>
<td>TBD</td>
</tr>
<tr>
<td>TBD</td>
<td>Google Message Encryption – Discount to $30.63 for purchase of 5000 licenses or more</td>
<td>$35.00</td>
<td>TBD</td>
</tr>
</tbody>
</table>

### Google Apps Deployment and Migration Services

<table>
<thead>
<tr>
<th>QTY</th>
<th>Item</th>
<th>On-Premise Rate</th>
<th>Hosted Rate</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Email Migration</td>
<td>$39,995.00</td>
<td>$39,995.00</td>
<td>$39,995.00</td>
</tr>
<tr>
<td>1</td>
<td>QuickStart</td>
<td>$2,995.00</td>
<td>N/A</td>
<td>$2,995.00</td>
</tr>
<tr>
<td>1</td>
<td>Google Message Configuration Services</td>
<td>$4,995.00</td>
<td>N/A</td>
<td>$4,995.00</td>
</tr>
<tr>
<td>1</td>
<td>Microsoft Outlook Sync</td>
<td>$1,995.00</td>
<td>N/A</td>
<td>$1,995.00</td>
</tr>
<tr>
<td>1</td>
<td>User Provisioning and Sync Tool</td>
<td>$14,795.00</td>
<td>$11,995.00</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>User Provisioning and Sync Tool – Maintenance and Support</td>
<td>$2,795.00</td>
<td>$4,495.00</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>LDAP Group Provisioning Sync Tool</td>
<td>$14,795.00</td>
<td>$11,995.00</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>LDAP Group Provisioning Sync Tool – Maintenance and Support</td>
<td>$1,995.00</td>
<td>$3,795.00</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>Google Apps Single Sign-On Service</td>
<td>$11,695.00</td>
<td>$10,495.00</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>Google Apps Single Sign-On Service – Maintenance and Support</td>
<td>$2,295.00</td>
<td>$3,295.00</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>SADA’s Single Sign-On Password Sync for Google Apps</td>
<td>$6,495.00</td>
<td>$6,495.00</td>
<td>$6,495.00</td>
</tr>
<tr>
<td>1</td>
<td>Mobility Strategy</td>
<td>$1,995.00</td>
<td>N/A</td>
<td>$1,995.00</td>
</tr>
<tr>
<td>1</td>
<td>Admin User Training</td>
<td>$9,200.00 + Expenses</td>
<td>N/A</td>
<td>$9,200.00 + Expenses</td>
</tr>
<tr>
<td>1</td>
<td>Project Management and Consulting</td>
<td>$19,995.00</td>
<td>N/A</td>
<td>$19,995.00</td>
</tr>
</tbody>
</table>

Subtotal: $87,665.00 + TBD
Sales Tax: Included
Total: $87,665.00 + TBD

### Annual Reoccurring Fees

<table>
<thead>
<tr>
<th>QTY</th>
<th>Item</th>
<th>On-Premise Rate</th>
<th>Hosted Rate</th>
<th>Total Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User Provisioning and Sync Tool – Maintenance and Support</td>
<td>$2,795.00</td>
<td>$4,495.00</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>LDAP Group Provisioning Sync Tool – Maintenance and Support</td>
<td>$1,995.00</td>
<td>$3,795.00</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>Google Apps Single Sign-On – Maintenance and Support</td>
<td>$2,295.00</td>
<td>$3,295.00</td>
<td>TBD</td>
</tr>
</tbody>
</table>

Total: TBD
I. Additional Relevant Information

**SADA Systems:**

SADA ranked Google’s #1 Enterprise Partner in the second half of 2010.

SADA was one of the world’s first 10 Google Apps partners having been part of the initial partner launch campaign in 2007. We also have six of the world first 100 Google Apps Certified Deployment Specialists, one of which will be serving as the lead solutions engineer on this deployment. The Google Apps Deployment Specialist Certification covers key Google Apps fundamentals such as overall understanding of the product, networking/email fundamentals, directory service fundamentals, technical architecture of Google Apps, security, configurations and troubleshooting basics.

The Google Apps Deployment Specialist Certification ensures that SADA’s team of Google Apps deployment engineers has the required knowledge and skills necessary to execute the hands-on configuration, deployment, and migration of larger (> 500) seat Google Apps deployment.

Successfully having migrated over 2,000,000 mailboxes from a variety of environments for over unique 200 clients SADA’s Cloud Team is unrivaled.

SADA has a demonstrated track record and competency in the implementation and customization of Google Apps and providing related consulting services.

SADA has assumed a major leadership role in the Google Apps space, and has built a significant part of its business around the implementation and customization of Google’s products. No one has more experience with Google Apps than SADA.

**VII. PROPOSAL PREPARATION AND SUBMISSION:**

A. General Requirements

1. **RFP Response:** In order to be considered for selection, Offerors must submit a complete response to this RFP. One (1) original, eight (8) copies and one (1) electronic media copy in generally used formats on CD, DVD, or USB Flash Drive media of each proposal must be submitted to:

   Virginia Tech
   Information Technology Acquisitions (0214)
   1700 Pratt Drive
   Blacksburg, VA 24061

   Reference the Opening Date and Hour, and RFP Number in the lower left hand corner of the return envelope or package.

   No other distribution of the proposals shall be made by the Offeror.

2. **Proposal Preparation:**

   a) Proposals shall be signed by an authorized representative of the Offeror. All information requested should be submitted. Failure to submit all information requested may result in Virginia Tech requiring prompt submission of missing information and/or giving a lowered evaluation of the proposal. Proposals which are substantially incomplete or lack key information may be rejected by Virginia Tech at its discretion. Mandatory requirements are those required by law or regulation or are such that they cannot be waived and are not subject to negotiation.
b) Proposals should be prepared simply and economically providing a straightforward, concise description of capabilities to satisfy the requirements of the RFP. Emphasis should be on completeness and clarity of content.

c) Proposals should be organized in the order in which the requirements are presented in the RFP. All pages of the proposal should be numbered. Each paragraph in the proposal should reference the paragraph number of the corresponding section of the RFP. It is also helpful to cite the paragraph number, subletter, and repeat the text of the requirement as it appears in the RFP. If a response covers more than one page, the paragraph number and subletter should be repeated at the top of the next page. The proposal should contain a table of contents which cross references the RFP requirements. Information which the offeror desires to present that does not fall within any of the requirements of the RFP should be inserted at an appropriate place or be attached at the end of the proposal and designated as additional material. Proposals that are not organized in this manner risk elimination from consideration if the evaluators are unable to find where the RFP requirements are specifically addressed.

d) Each copy of the proposal should be bound in a single volume where practical. All documentation submitted with the proposal should be bound in that single volume.

e) Ownership of all data, material and documentation originated and prepared for Virginia Tech pursuant to the RFP shall belong exclusively to Virginia Tech and be subject to public inspection in accordance with the Virginia Freedom of Information Act. Trade secrets or proprietary information submitted by an Offeror shall not be subject to public disclosure under the Virginia Freedom of Information Act. However, to prevent disclosure the Offeror must invoke the protections of Section 2.2-4342F of the Code of Virginia, in writing, either before or at the time the data or other materials is submitted. The written request must specifically identify the data or other materials to be protected and state the reasons why protection is necessary. The proprietary or trade secret material submitted must be identified by some distinct method such as highlighting or underlining and must indicate only the specific words, figures, or paragraphs that constitute trade secret or proprietary information. The classification of an entire proposal document, line item prices and/or total proposal prices as proprietary or trade secrets is not acceptable and may result in rejection of the proposal.

3. Oral Presentation: Offerors who submit a proposal in response to this RFP may be required to give an oral presentation of their proposal to Virginia Tech. This will provide an opportunity for the Offeror to clarify or elaborate on the proposal but will in no way change the original proposal. Virginia Tech will schedule the time and location of these presentations. Oral presentations are an option of Virginia Tech and may not be conducted. Therefore, proposals should be complete.

B. Specific Requirements

Proposals should be as thorough and detailed as possible so that Virginia Tech may properly evaluate your capabilities to provide the required goods and services. Offerors are required to submit the following information/items as a complete proposal:

1. A copy of your latest annual report.

**SADA Systems:**

SADA Systems is financially stable and can provide more insight to financial standing upon request and establishment of NDA. Meanwhile we will disclose the following revenue numbers and accolades to help attest to its financial stability.
- $6,500,000 - 2010
- $3,456,000 - 2009
- $2,985,000 - 2008
- $2,234,000 - 2007
- $2,109,000 - 2006
- $1,444,000 - 2005
- Inc. 5000 - fastest growing private companies in the U.S. – 2010
- Inc. 5000 - fastest growing private companies in the U.S. – 2009
- Inc. 5000 - fastest growing private companies in the U.S. – 2008
- Inc. 5000 - fastest growing private companies in the U.S. – 2007

2. Four (4) recent references, either educational or governmental, for whom you have provided the type of goods and services described herein. Include the date(s) the goods and services were furnished, the client name, address and the name and phone number of the individual Virginia Tech has your permission to contact.

**SADA Systems:**

SADA has a demonstrated track record and competency in the implementation and customization of Google Apps and providing related consulting services as the references below can attest to.

**Northwestern University**
1880 Campus Drive, Kresge 1-346, Evanston, Illinois, USA 60208
Contact: Wendy Woodward
Phone: +1.847.467.7851
Email: wwk@northwestern.edu
Relationship: 2007 – Present

**Kent State University**
Stewart Hall, 1550 Johnston Drive, Kent, OH, USA, 44240
Contact: Jared Boehm
Phone: +1.330.672.8629
Email: jtboehm@kent.edu
Relationship: 2009 – Present

**Doane College**
1014 Bosewell Ave, Crete, NE, USA, 68333
Contact: Dan Schneider
Phone: +1.402.826.8298
Email: dan.schneider@doane.edu
Relationship: 2009 – Present

**City of Los Angeles**
200 N. Main Street, Los Angeles, CA, USA, 90012
Contact: Charlene Dennis
Phone: +1.213.978.2873
Email: charlene.dennis@lacity.org
Relationship: 2009 – Present

3. Responses to the requirements as noted in Section VI formatted as noted above in Paragraph VII.A.2
Please see Section VI.

4. Any proposed exceptions to the RFP terms and conditions.

**SADA Systems:**

SADA has no exceptions to the RFP terms and conditions.

5. Small, Women-owned and Minority-owned Business (SWAM) Utilization:

If your business can not be classified as SWAM, describe your plan for utilizing SWAM subcontractors if awarded a contract. Describe your ability to provide reporting on SWAM subcontracting spend when requested. If your firm or any business that you plan to subcontract with can be classified as SWAM, but has not been certified by the Virginia Department of Minority Business Enterprise (DMBE), it is expected that the certification process will be initiated no later than the time of the award. If your firm is currently certified, you agree to maintain your certification for the life of the contract. For assistance with SWAM certification, visit the DMBE website at www.dmbe.virginia.gov. Any questions relating to SWAM businesses or SWAM subcontracting opportunities can be directed to Mark Cartwright, the University’s Assistant Director for Supplier Diversity, at 540-231-3333 or mcartwright@vt.edu.

**SADA Systems:**

SADA is classified as a small, women-owned business. Please see attached Certificate.

6. The return of the General Information Form and addenda, if any, signed and filled out as required.

**SADA Systems:**

The General Information Form can be found on page 2 of this response. SADA acknowledges receipt of two addenda for this RFP, which are signed at the end of this document.

Please note that for future correspondence/questions on this response to this RFP, please contact:

Mike Kulinski
SADA Systems, Inc.
Regional Sales Manager
mike.kulinski@sadasystems.com
+1.202.656.0650
Questions and Answers from the Pre-Proposal Conference through March 21, 2011

Q1. What platforms will be migrated? Does this include Exchange?
A1. Migration is mainly from a Sun-based hardware/software solution – JAVA. Some Exchange users may choose to migrate, but is not the primary thrust and will not be required. No plans for the proposed email solution to interface with Oracle.

Q2. Number of users being migrated?
A2. We’ve been trimming and expect the number to be 70-80,000. At this moment the count is about 78,000.

Q3. Size of mail storage repository?
A3. The mail store is 2 TB (terabytes). We have no quota, and we retain records for 62-days.

Q4. What archive solution is used?
A4. We have no archive solution. Methodology for individual end-users to store online may be provided in proposals (similar to .pst but different format).

Q5. What is the breakdown of supported clients?
A5. We encourage web-based interface. Proposals could provide the oldest and latest version of all clients the proposed system supports.

Q6. Do you need a Blackberry enterprise solution?
A6. We don’t have or need a Blackberry enterprise solution and don’t support them. The majority of Blackberry users are on Exchange and use ActiveSync or Goodlink.

Q7. Must, should, may – what is the intended difference?
A7. Shall and must items are essential to meet our system requirements. Should and may are identified features, and if the proposed solution has those features they ideally would be detailed in proposals.

Q8. How should pricing be presented?
A8. Ideally for scalability, cost could be provided per user, per year. Base solutions could include all ‘shall’ items, with other items priced as options.
Q9. How long should proposal pricing be valid?
A9. Six months is appropriate.

Q10. What is the timing to award?
A10. We are aiming for an award decision this summer, ideally to implement by mid-August.

Q11. What integration with vendor’s ID management solution is needed?
A11. We want to leverage our existing ID management, Open LDAP, as listed in the RFP.

Q12. What is needed for authentication?
A12. Describe all authentication solutions with which your proposed system can interact.

Q13. Will the migrating email need to support calendar and contacts?
A13. These will not be used or supported.

Q14. What is expected for system security data?
A14. Since this is a hosted solution, proposals should fully describe physical security, access control, patch and penetration test schedules, and other issues. See some relevant security URLs below. VT will enforce its own internal security policies.

Q15. Will the migration include multiple domains and names? Are these all on the same platform?
A15. The initial migration will be only the main domain vt.edu. We’d like the option after initial migration to offer our sub-domain groups the ability to migrate as well (ex: xxx.vt.edu). VT is decentralized, so multiple platforms are used.

Q16. What groups of users will be migrating?
A16. Students, faculty, staff, retirees, and VT affiliates will be migrating. A handful of sponsored users are subject to ITAR and FISMA regulations and require hosting in US, and these may be migrating as a separate group depending on the proposed solution.

Q17. Will the solution need to display Free/Busy?
A17. No, this is outside the scope.

Q18. What is the last day for questions?
A18. March 28, 3pm is the last date for our office to receive questions. Addendums with questions and answers will be posted to the ITA and eVA websites listed in the RFP. We will not be extending the deadline.

Q19. Will the security requirements detailed in the RFP, such as HIPPA, apply to all users, or is this a segregated group?
A19. These requirements apply to all users.

Q20. Will you provide information on Graham-Leach-Bliley?
A20. That act relates to information privacy. Information is available at http://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act and other sources.

Q21. What level of support will be provided by VT’s internal IT?
A21. For implementation we have a project team in place representing critical aspects of the project; these people work with the current mail system. For system usage, VT will provide first-level help desk and VT will make any necessary contact with the service provider.

Q22. Are there other criteria or review groups or processes beyond the RFP?
A22. Selection will be based on the criteria in the RFP, including proposal responses, potential follow-up clarification questions and/or demonstrations. Student and Faculty/Staff representatives are included on the VT review team.

Below are security standard URLs related to this RFP.


FEDERAL INFORMATION PROCESSING STANDARD (FIPS) 199, STANDARDS FOR SECURITY CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS

Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems

Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems

<table>
<thead>
<tr>
<th>FULL LEGAL NAME (PRINT)</th>
<th>FEDERAL TAXPAYER NUMBER (ID#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SADA Systems, Inc.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BUSINESS NAME/DBA NAME/TA NAME</th>
<th>FEDERAL TAXPAYER NUMBER (ID#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(If different than the Full Legal Name)</td>
<td>(If different than ID# above)</td>
</tr>
<tr>
<td>SADA Systems, Inc.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BILLING NAME</th>
<th>FEDERAL TAXPAYER NUMBER (ID#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Company name as it appears on your invoice)</td>
<td>(If different than ID# above)</td>
</tr>
<tr>
<td>SADA Systems, Inc.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PURCHASE ORDER ADDRESS</th>
<th>PAYMENT ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>5250 Vineland Avenue</td>
<td>5250 Vineland Avenue</td>
</tr>
<tr>
<td>North Hollywood, CA 91601</td>
<td>North Hollywood, CA 91601</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONTACT NAME/TITLE (PRINT)</th>
<th>SIGNATURE (IN INK)</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tony Safoian, CEO</td>
<td></td>
<td>4/4/2011</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E-MAIL ADDRESS</th>
<th>TELEPHONE NUMBER</th>
<th>TOLL FREE TELEPHONE NUMBER</th>
<th>FAX NUMBER TO RECEIVE E-PROCUREMENT ORDERS</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:tony.safoian@sadasystems.com">tony.safoian@sadasystems.com</a></td>
<td>818.766.2400</td>
<td>866.997.0000</td>
<td>818.766.0090</td>
</tr>
</tbody>
</table>

Please note that for future correspondence/questions on this response to this RFP, please contact:
Mike Kulinski
SADA Systems, Inc.
Regional Sales Manager
mike.kulinski@sadasystems.com
+1.202.656.0650
ADDENDUM # 2 TO RFP # 0016512

For

E-mail/Collaboration Services

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
INFORMATION TECHNOLOGY ACQUISITIONS (0214)
1700 PRATT DRIVE
BLACKSBURG, VA 24061

DATE
March 31, 2011

ORIGINAL DUE DATE AND HOUR
April 4, 2011 at 3:00 PM (not changed)

ADDRESS ALL INQUIRIES AND CORRESPONDENCE TO: Nancy Sterling
E-MAIL ADDRESS: john.krallman@vt.edu TELEPHONE NUMBER (540) 231-9517
FAX NUMBER (540) 231-4110

Questions and Answers through March 30, 2011

Q1) How many users require archiving and e-discovery (e.g. everybody, faculty only, etc)? Question #1 is designed to
determine if ALL users require archiving and e-discovery. If only some require this service, we will consider providing
appropriate scenarios (with corresponding pricing options) in the proposal.

A1) Only a subset of users require archiving and e-discovery; those are principally senior administrators, who are also
generally users of our Exchange system, and may be getting archiving services there. It’s perfectly acceptable to bid
archiving/e-discovery as an optional per-user component.

Q2) How many internal IT resources does VirginiaTech plan to assign to this project? Does VirginiaTech require that the
successful vendor handle all aspects of a start-to-finish implementation, or is self-service an option where a designated
sub-group of users would be implemented by vendor, training on the process provided to VirginiaTech personnel, who
would then handle the remaining mailboxes (with vendor support available when required)? Question #2 is designed to
determine if VirginiaTech might be interested in a ‘self-service’ option as outlined in the question.

A2) The Internal IT group is familiar with email migrations, and recently migrated alumni users off of our central
systems to a Google solution. A project team has already been formed with key representatives from all the
appropriate internal groups prepared to handle implementation. We require the successful bidder to provide at a
minimum appropriate engineering/technical contacts inside the organization able to perform effective corrective
measures as needed, and provide necessary documentation and accesses required for Virginia Tech to successfully
implement the transition, and are prepared to do the work in preparing our provisioning system, creating users,
migrating e-mail if needed, etc. Bidders can provide proposals for higher levels of implementation if such configuration
services are an available offering.

Q3) What is the exact version of the Oracle OCUCS mail server, and is that simply a rename of the previous Sun One
Messaging server. ...i.e. did you upgrade the Sun One server to Oracle (and what Oracle version), or is it still just Sun
One renamed to Oracle and what Sun One version?

A3) Sun Java(tm) System Messaging Server 6.3-5.02 (built Oct 12 2007; 32bit). Oracle OCUCS is simply the name it’s
currently marketed under.
This proposal valid for 180 days post April 4th, 2011 submission.

<table>
<thead>
<tr>
<th>FULL LEGAL NAME (PRINT)</th>
<th>FEDERAL TAXPAYER NUMBER (ID#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SADA Systems, Inc.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BUSINESS NAME/DBA NAME/TA NAME</th>
<th>FEDERAL TAXPAYER NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>(If different than the Full Legal Name)</td>
<td>(If different than ID# above)</td>
</tr>
<tr>
<td>SADA Systems, Inc.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BILLING NAME</th>
<th>FEDERAL TAXPAYER NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Company name as it appears on your invoice)</td>
<td>(If different than ID# above)</td>
</tr>
<tr>
<td>SADA Systems, Inc.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PURCHASE ORDER ADDRESS</th>
<th>PAYMENT ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>5250 Vineland Avenue</td>
<td>5250 Vineland Avenue</td>
</tr>
<tr>
<td>North Hollywood, CA 91601</td>
<td>North Hollywood, CA 91601</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONTACT NAME/TITLE (PRINT)</th>
<th>SIGNATURE (IN INK)</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tony Safoian, CEO</td>
<td></td>
<td>4/4/2011</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E-MAIL ADDRESS</th>
<th>TELEPHONE NUMBER</th>
<th>TOLL FREE TELEPHONE NUMBER</th>
<th>FAX NUMBER TO RECEIVE E-PROCUREMENT ORDERS</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:tony.safoian@sadasystems.com">tony.safoian@sadasystems.com</a></td>
<td>818.766.2400</td>
<td>866.997.0000</td>
<td>818.766.0090</td>
</tr>
</tbody>
</table>

Please note that for future correspondence/questions on this response to this RFP, please contact:
Mike Kulinski
SADA Systems, Inc.
Regional Sales Manager
mike.kulinski@sadasystems.com
+1.202.656.0650
SUPPLIER CLEARINGHOUSE
CERTIFICATE OF ELIGIBILITY

CERTIFICATE EXPIRATION DATE: 01-05-2014

The Supplier Clearinghouse for the Utility Supplier Diversity Program of the California Public Utilities Commission hereby certifies that it has audited and verified the eligibility of:

Sada Systems, Inc.
of North Hollywood, California as a WBE

pursuant to Commission General Order 156, and the terms and conditions stipulated in the Verification Application Package. This Certificate shall be valid only with the Clearinghouse seal affixed hereto.

Eligibility must be maintained at all times, and renewed within 30 days of any changes in ownership or control. Failure to comply may result in a denial of eligibility. The Clearinghouse may reconsider certification if it is determined that such status was obtained by false, misleading or incorrect information. Decertification may occur if any verification criterion under which eligibility was awarded later becomes invalid due to Commission ruling. The Clearinghouse may request additional information or conduct on-site visits during the term of verification to verify eligibility.

This certification is valid only for the period that the above named firm remains eligible as determined by the Clearinghouse. Utility companies may direct inquiries concerning this Certificate to the Clearinghouse at 800-359-7998 in Los Angeles.

VON: 4HS00004

Determination Date: 01-05-2011
Attachment C

Contract UCP-TS-C02-12

Proposal Clarifications and Negotiations
SADA clarification questions and responses:

1) Will the Google Apps Directory Sync tool make it possible to provision new accounts based on affiliation status in our enterprise directories without administrative intervention? Will it be possible to deprovision accounts automatically?

- The Google Apps Directory Sync (GADS) provisions accounts based on security groups/organizational units defined in your directories. Once these groups are defined, you will add, suspend, and remove users as you do today in your directory. Those updates then get synced to Google Apps using an automated schedule in GADS. Furthermore, the University can organize users in Google Apps to reflect the structure in your directories. This allows you to then enable/disable settings for users in a specific organization in Google Apps. To deprovision a user account, the Google Apps Directory Sync tool will perform this task during it scheduled sync. When a user is removed or suspended from your directory, that change will get synced to Google Apps without administrative interference.

2) Assuming we chose to do most or all of the migration work ourselves with in-house resources, would we contract for Google Apps for Edu services with you, or with Google directly? Can we select services off your list in an a-la-carte fashion, e.g. only contract you to provide training, or to provide your toolset for our use?

- If the University decides to only purchase Google Apps for Education (and not Google Message Discovery, Security, or Encryption) it will activate the licenses directly with Google, whether or not a partner is involved in the migration. Since the licenses are free, there is no reseller necessary to activate the accounts. The accounts will be subject to the Terms found at: [http://www.google.com/apps/intl/en/terms/education_terms.html](http://www.google.com/apps/intl/en/terms/education_terms.html). If the University selects to purchase GMD, GMS, or GME, it will enter into a separate reseller agreement with SADA. Also, if any of SADA's tools or services are purchased by the University, SADA and the University will enter into a Professional Services Agreement.

- SADA services are available in an a la carte fashion, so that the University may pick and choose whichever tools or services it wishes to meet its objectives. SADA encourages the University to select those tools and services it feels it needs. If selected, SADA will work with the University to determine how to best utilize both the University IT Staff and the SADA team for the successful and timely completion of the project.
TERMS AND CONDITIONS

RFP General Terms and Conditions

http://www.purch.vt.edu/html.docs/terms/GTC_RFP_100110.pdf

Special Terms and Conditions

1. **AUDIT**: The Contractor hereby agrees to retain all books, records, and other documents relative to this contract for five (5) years after final payment, or until audited by the Commonwealth of Virginia, whichever is sooner. Virginia Tech, its authorized agents, and/or the State auditors shall have full access and the right to examine any of said materials during said period.

2. **AVAILABILITY OF FUNDS**: It is understood and agreed between the parties herein that Virginia Tech shall be bound hereunder only to the extent of the funds available or which may hereafter become available for the purpose of this agreement.

3. **CANCELLATION OF CONTRACT**: Virginia Tech reserves the right to cancel and terminate any resulting contract, in part or in whole, without penalty, upon 60 days written notice to the Contractor. In the event the initial contract period is for more than 12 months, the resulting contract may be terminated by either party, without penalty, after the initial 12 months of the contract period upon 60 days written notice to the other party. Any contract cancellation notice shall not relieve the Contractor of the obligation to deliver and/or perform on all outstanding orders issued prior to the effective date of cancellation.

4. **CONTRACT DOCUMENTS**: The contract entered into by the parties shall consist of the Request for Proposal including all modifications thereof, the proposal submitted by the Contractor, the written results of negotiations, the Commonwealth Standard Contract Form, all of which shall be referred to collectively as the Contract Documents.

5. **INSURANCE**: By signing and submitting a proposal under this solicitation, the Offeror certifies that if awarded the contract, it will have the following insurance coverage at the time the work commences. Additionally, it will maintain these during the entire term of the contract and that all insurance coverage will be provided by insurance companies authorized to sell insurance in Virginia by the Virginia State Corporation Commission.

   **INSURANCE COVERAGES AND LIMITS REQUIRED:**
   
   A. Worker's Compensation – Statutory requirements and benefits.
   B. Employers Liability – $100,000.00
   C. General Liability – $500,000.00 combined single limit. Virginia Tech and the Commonwealth of Virginia shall be named as an additional insured with respect to goods/services being procured. This coverage is to include Premises/Operations Liability, Products and Completed Operations Coverage, Independent Contractor's Liability, Owner's and Contractor's Protective Liability and Personal Injury Liability.
   D. Automobile Liability – $500,000.00
   E. Builders Risk – For all renovation and new construction projects under $100,000 Virginia Tech will provide All Risk – Builders Risk Insurance. For all renovation contracts, and new construction from $100,000 up to $500,000 the contractor will be required to provide All Risk – Builders Risk Insurance in the amount of the contract and name Virginia Tech as additional insured. All insurance verifications of insurance will be through a valid insurance certificate.

   The contractor agrees to be responsible for, indemnify, defend and hold harmless Virginia Tech, its officers, agents and employees from the payment of all sums of money by reason of any claim against them arising out of any and all occurrences resulting in bodily or mental injury or property damage that may happen to occur in connection with and during the performance of the contract, including but not limited to claims under the Worker's Compensation Act. The contractor agrees that it will, at all times, after the completion of the work, be responsible for, indemnify, defend and hold harmless Virginia Tech, its officers, agents and employees from all liabilities resulting from bodily or mental injury or property damage directly or indirectly arising out of the performance or nonperformance of the contract.

6. **NOTICES**: Any notices to be given by either party to the other pursuant to any contract resulting from this solicitation shall be in writing, hand delivered or mailed to the address of the respective party at the following address:
7. **PROPOSAL ACCEPTANCE PERIOD**: Any proposal received in response to this solicitation shall be valid for (120) days. At the end of the (120) days the proposal may be withdrawn at the written request of the Offeror. If the proposal is not withdrawn at that time it remains in effect until an award is made or the solicitation is cancelled.

8. **CONTRACTOR RESPONSIBILITIES**: The Contractor shall be responsible for completely supervising and directing the work under this contract and all subcontractors that he may utilize, using his best skill and attention. Subcontractors who perform work under this contract shall be responsible to the Contractor. The Contractor agrees that he is as fully responsible for the acts and omissions of his subcontractors and of persons employed by them as he is for the acts and omissions of his own employees.

9. **PROPOSAL PRICES**: Proposal shall be in the form of a firm unit price for each item during the contract period.

10. **QUANTITIES**: Quantities set forth in this solicitation are estimates only, and the Contractor shall supply at proposal prices actual quantities as ordered, regardless of whether such total quantities are more or less than those shown.

11. **RENEWAL OF CONTRACT**: This contract may be renewed by Virginia Tech upon written agreement of both parties for five successive one year periods, or as negotiated under the terms of the current contract, and at a reasonable time (approximately 90 days) prior to the expiration.

12. **COMMUNICATIONS**: Communications regarding this Request for Proposals (RFP) shall be formal from the date of issue for this RFP, until either a Contractor has been selected or the Information Technology Acquisitions Office rejects all proposals. Formal communications will be directed to the Information Technology Acquisitions Office. Informal communications, including but not limited to request for information, comments or speculations regarding this RFP to any University employee other than an Information Technology Acquisitions Office representative may result in the offending Offeror’s proposal being rejected.

13. **RIGHT TO SELECT PROJECT PERSONNEL**: The University has the right to interview and select all of the Contractor’s personnel that will provide services under the Agreement.

14. **RIGHT TO REMOVE PROJECT PERSONNEL**: The University has the right to remove any of the selected Contractor’s personnel that will provide services under the Agreement.

15. **SUBCONTRACTS**: No portion of the work shall be subcontracted without prior written consent of Virginia Tech. In the event that the Contractor desires to subcontract some part of the work specified herein, the Contractor shall furnish Virginia Tech the names, qualifications and experience of their proposed subcontractors. The Contractor shall, however, remain fully liable and responsible for the work to be done by his subcontractor(s) and shall assure compliance with all requirements of the contract.

16. **ADVERTISING**: In the event a contract is awarded for supplies, equipment, or services resulting from this solicitation, no indication of such sales or services to Virginia Tech will be used in product literature or advertising without the prior written consent of Virginia Tech. The Contractor shall not state in any of the advertising or product literature that the Commonwealth of Virginia or any agency or institution of the Commonwealth has purchased or uses its products or services.

17. **CERTIFICATION TESTING AND ACCEPTANCE**: The system specified in the contract shall be considered ready for production testing upon receipt of documentation from the Contractor that a successful system audit or diagnostic test was performed at the site demonstrating that the system meets the minimum design/performance capabilities stipulated by
the contract. The system shall be deemed ready for production certification testing on the day following receipt of this
documentation. Virginia Tech shall provide written confirmation of its acceptance following successful completion of the
production certification test. System (software and/or hardware) payment will be authorized after the successful
completion and certification test(s).

18. **SEVERAL LIABILITY:** Virginia Tech will be severally liable to the extent of its purchases made against any contract
resulting from this solicitation. Applicable entities described herein will be severally liable to the extent of their
purchases made against any contract resulting from this solicitation.

19. **DEFINITIONS:**
   A. “Brand Features” means the trade names, trademarks, service marks, logos, domain names, and other distinctive
      brand features of each party, respectively, as secured by such party from time to time.
   B. “Customer” means Virginia Tech and any public body, public or private health or educational institutions, or Virginia
      Tech’s affiliated corporations and/or partnerships, including any entities identified by Customer as affiliates or
      collaborators.
   C. “Customer Data” includes credentials issued to Customer by Vendor and all records relating to Customer’s use of
      Vendor services and administration of End User accounts, including any Personal Data of Customer personnel that
      does not otherwise constitute Personal Data of an End User.
   D. “Data” means information whether in oral or written (including electronic) form, created, obtained, transmitted, used,
      maintained, processed, and disposed of by Customer, End Users, and Vendor in the course of using and
      configuring/providing, respectively, the Services under an agreement between the parties, and includes Customer
      Data, End User Data, and Personal Data.
   E. “Data Compromise” means a security-relevant event in which the security policy of a system used to create, transmit,
      maintain, use, process, or store data is disobeyed or otherwise breached, and in which Data is exposed to
      unauthorized disclosure, access, alteration, or use.
   F. “End User” means the individuals authorized by Customer to access and use the Services provided by Vendor under
      an agreement between the parties.
   G. “End User Data” includes End User account credentials and information, and all records sent, received, or created by
      or for End Users, including email content, headers, and attachments, and any Personal Data of any End User or third
      party contained therein or in any logs or other records of Vendor reflecting End User’s use of Vendor services.
   H. “Personal Data” includes but is not limited to: personal identifiers such as name, address, phone number, date of
      birth, Social Security Number, and student or personnel identification number; Protected Health Information (PHI) as
      that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; personal
      identifiable information contained in student education records as that term is defined in the Family Educational
      Rights and Privacy Act, 20 USC 1232g; nonpublic personal information as that term is defined in the
      Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; credit and debit card numbers and/or
      access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment
      Card Industry Data Security Standards; other financial account numbers and/or access codes; driver’s license
      number; and other state- or federal-identification numbers such as passport, visa or state identity card numbers
   I. “Services” means any services offered as part of the RFP, or otherwise contracted.

20. **SERVICE ENTRY PLAN:**
   Vendor will develop, provide to Customer, and implement a detailed entry plan that provides for:
   A. the successful and uninterrupted transfer to Vendor of each service provided by Customer to End Users;
   B. the timely and successful integration of Vendor software, applications and Services with Customer’s existing identity
      management and access management systems;
   C. the timely and successful integration with specified Customer applications;
   D. the availability of and support for the Services via specified Customer and End User devices including mobile
      devices; and
   E. Customer’s ability to, directly or through instructions to Vendor, create, modify, suspend, eliminate, assign aliases
      for, and internally delegate the administration of individual and group accounts created as part of Vendor’s provision
      of Services.

21. **RIGHTS AND LICENSE IN AND TO CUSTOMER AND END USER DATA:**
   The parties agree that as between them, all rights including all intellectual property rights in and to Customer and End
   User data shall remain the exclusive property of Customer, and Vendor has a limited, nonexclusive license to use these
data as provided solely for the purpose of performing its obligations hereunder. Neither party has any rights, implied or
otherwise, to the other’s data, content, or intellectual property, except as the parties expressly agreed otherwise in writing.

22. **DATA PRIVACY:**
A. Vendor will use Customer Data and End User Data only for the purpose of fulfilling its duties hereunder and for Customer’s and its End User’s sole benefit, and will not share such data with or disclose it to any third party without the prior written consent of Customer or as otherwise required by law. By way of illustration and not of limitation, Vendor will not use such data for Vendor’s own benefit and, in particular, will not engage in “data mining” of Customer or End User Data or communications, whether through automated or human means, except as specified and expressly required by law or authorized in writing by Customer.
B. Vendor will provide access to Customer and End User Data only to those Vendor employees and subcontractors who need to access the data to fulfill Vendor’s obligations under this Agreement. Vendor will ensure that employees who perform work on the Vendor’s behalf have read, understood, and received appropriate instruction as to how to comply with the data protection provisions contained herein, and have undergone all background screening and possess all qualifications required by Customer prior to being granted access to the Data.

23. **DATA SECURITY AND INTEGRITY:**
A. All facilities used to store and process Customer and End User data will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Vendor’s own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, Vendor warrants that all Customer Data and End User Data will be encrypted in transmission (including via web interface) and storage at no less than 128-bit level, and that Vendor will comply with all other technical specifications of Customer. Vendor will comply with the requirements of FERPA, HIPAA, ITAR, and FISMA. Vendor will use industry-standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services to Customer.
B. Vendor will configure the Services to filter spam while permitting communications from third-party Internet Protocol addresses identified by Customer as legitimate.
C. Note - Section 23C applies to Google Inc, the Vendor storing and processing Customer data, and does not apply to SADA Systems Inc, which shall not store or process Customer data.
Vendor will at its expense conduct or have conducted at least annually:
   i. A SAS 70 audit of Vendor’s security policies, procedures and controls resulting in the issuance of a Service Auditor’s Report Type II;
   ii. a vulnerability scan, performed by a scanner approved by Customer, of Vendor’s systems and facilities that are used in any way to deliver Services; and a formal penetration test, performed by a process and qualified personnel approved by Customer, of Vendor’s systems and facilities that are used in any way to deliver services hereunder
   iii. Vendor will provide Customer upon request the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations to Customer and report on such. Customer may require, at its expense, Vendor to perform additional audits and tests, the results of which will be provided promptly to Customer.

24. **DATA INTEGRITY:**
Vendor will take commercially reasonable measures, including regular data integrity audits, to protect Customer and End User Data against deterioration or degradation of data quality and authenticity.

25. **RESPONSE TO LEGAL ORDERS, DEMANDS OR REQUESTS FOR DATA:**
A. Except as otherwise expressly prohibited by law, Vendor will:
   i. immediately notify Customer of any subpoenas, warrants, or other legal orders, demands or requests received by Vendor seeking Customer and/or End User Data;
   ii. consult with Customer regarding its response;
   iii. cooperate with Customer’s reasonable requests in connection with efforts by Customer to intervene and quash or modify the legal order, demand or request; and
   iv. upon Customer’s request, provide Customer with a copy of its response.
B. If Customer receives a subpoena, warrant, or other legal order, demand or request seeking Customer or End User Data maintained by Vendor, Customer will promptly provide a copy to Vendor. Vendor will promptly supply Customer with copies of data required for Customer to respond, and will cooperate with Customer’s reasonable requests in connection with its response.
26. **DATA COMPROMISE RESPONSE:**
   A. Immediately upon becoming aware of a Data Compromise, or of circumstances that could have resulted in unauthorized access to or disclosure of Customer or End User Data, Vendor will notify Customer, fully investigate the incident, and cooperate fully with Customer’s investigation of and response to the incident. Except as otherwise required by law, Vendor will not provide notice of the incident directly to the persons whose data were involved, regulatory agencies, or other entities, without prior written permission from Customer.
   B. Notwithstanding any other provision hereunder, and in addition to any other remedies available to Customer under law or equity, Vendor will reimburse Customer in full for all costs incurred by Customer in investigation and remediation of such Data Compromise, including but not limited to providing notification to third parties whose data were compromised and to regulatory agencies or other entities as required by law or contract; the offering of 6 months’ credit monitoring to each person whose data were compromised; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Data Compromise.

27. **DATA RETENTION AND DISPOSAL:**
   A. Vendor will use commercially reasonable efforts to retain data in an End User’s account, including attachments, until the End User deletes them or for an alternative time period mutually agreed by the parties.
   B. Using appropriate and reliable storage media, Vendor will regularly back up Customer and End User Data and retain such backup copies for a minimum of 30 days. At the end of that time period and at Customer’s election, Vendor will either securely destroy or transmit to Customer repository the backup copies. Upon Customer’s request, Vendor will supply Customer a certificate indicating the records destroyed, the date destroyed, and the method of destruction used.
   C. Vendor will retain logs associated with End User activity for a minimum of 90 days, unless the parties mutually agree to a different period.
   D. Vendor will immediately place a “hold” on the destruction under its usual records retention policies of records that include Customer and End User Data, in response to an oral or written request from Customer indicating that those records may be relevant to litigation that Customer reasonably anticipates. Oral requests by Customer for a hold on record destruction will be reduced to writing and supplied to Vendor for its records as soon as reasonably practicable under the circumstances. Customer will promptly coordinate with Vendor regarding the preservation and disposition of these records. Vendor shall continue to preserve the records until further notice by Customer.

28. **DATA TRANSFER UPON TERMINATION OR EXPIRATION:**
   A. Upon termination or expiration of an agreement between the parties, Vendor will ensure that all Customer and End User Data are transferred to Customer or a third party designated by Customer securely, within a reasonable period of time, and without significant interruption in service, all as further specified in the Technical Specifications provided at that time. Vendor will ensure that such migration uses facilities and methods are compatible with the relevant systems of the transferee, and to the extent technologically feasible, that Customer will have reasonable access to Customer and End User Data during the transition.
   B. Vendor will notify Customer of impending cessation of its business or that of a tiered provider and any contingency plans in the event of notice of such a failure. This includes immediate transfer of any previously escrowed assets and data and providing Customer access to Vendor’s facilities to remove and destroy Customer-owned assets and data. Vendor shall implement its exit plan and take all necessary actions to ensure a smooth transition of Service with minimal disruption to Customer. Vendor will provide a fully documented description of Services and perform and document a gap analysis by examining any differences between its services and those to be provided by its successor. Vendor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in delivery of its Services along with supporting documentation, indicating which if any of these are owned by or dedicated to Customer. Vendor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on Customer, all such work to be coordinated and performed in advance of the formal, final transition date.

29. **SERVICE LEVELS, INTERRUPTIONS IN SERVICE, SUSPENSION AND TERMINATION OF SERVICE, CHANGES TO SERVICE:**
   A. Vendor warrants that the Services will be performed in a professional and workmanlike manner consistent with industry standards reasonably applicable to such Services. Vendor further warrants that the Services will be Operational at least 99.99% of the time in any given month during the term of this Agreement, meaning that the outage or downtime percentage will be not more than .01%. In the event of a Service outage, Vendor will
   i. promptly and at Vendor’s expense use commercial best efforts to restore the Services as soon as possible, and
   ii. unless the outage was caused by a force majeure event, refund or credit Customer, at Customer’s election, the pro-rated amount of fees corresponding to the time Services were unavailable. Neither party will be liable to the other for any failure or delay in performance to the extent said failures or delays are proximately caused.
by forces beyond that party’s reasonable control, provided that the party resumes performance as soon as it is reasonably able to do so.

B. From time to time it may be necessary or desirable for either the Customer or Vendor to propose changes in the Services provided. Automatic upgrades to any software used by Vendor to provide the Services that simply improve the speed, efficiency, reliability, or availability of existing Services and do not alter or add functionality, are not considered “changes to the Services” and such upgrades will be implemented by Vendor on a schedule no less favorable than provided by Vendor to any other customer receiving comparable levels of Services.

C. Vendor will provide Customer with a minimum of one (1) days’ prior notice of scheduled downtime in the provision of Services for maintenance or upgrades. To the extent possible, Vendor will schedule downtime during times of ordinarily low use by Customer. In the event of unscheduled and unforeseen downtime for any reason, except as otherwise prohibited by law Vendor will promptly notify Customer and cooperate with Customers’ reasonable requests for information regarding the downtime (including causes, effect on Services, and estimated duration).

D. Customer may suspend or terminate (or direct Vendor to suspend or terminate) an End User’s access to Services in accordance with Customer’s policies. Vendor may suspend access to Services by Customer or an End User immediately in response to an act or omission that reasonably appears to jeopardize the security or integrity of Vendor’s Services or the network(s) or facilities used to provide the Services. Suspension will be to the minimum extent, and of the minimum duration, required to prevent or end the security issue. Vendor may suspend Customer’s access to Services if, after at least thirty (30) days’ written notice to Customer and subsequent good-faith, commercially reasonable efforts to resolve the matter with Customer to the parties’ mutual satisfaction, Customer remains in material breach of the terms of an agreement between the parties. The suspension will be lifted immediately once the breach is cured. Vendor may suspend access to Services by an End User in response to (i) a material breach by End User of any terms of use s/he has agreed to in connection with receiving the Services. Vendor will notify Customer of any suspension of End User access to Services before suspension or, if notice before is not feasible, as soon as reasonably possible thereafter.

30. **INSTITUTIONAL BRANDING:** Vendor will provide reasonable and appropriate opportunities for Customer branding of Vendor services. Each party shall have the right to use the other party’s trademarks only in connection with performing the functions provided in this Agreement. Any use of a party’s trademarks will inure to the benefit of the party holding intellectual property rights in and to that trademark.

31. **EMERGENCY COMMUNICATIONS:** Vendor warrants that its Services are compatible with and will not interfere with Customer’s provision of emergency communications in compliance with applicable law and Customer policies. This includes enabling and supporting at least one (1) Customer simulations annually of emergency communications.

32. **WARRANTIES AND LIABILITY:**
   A. Vendor warrants that all services provided to Customer shall conform to and be performed in accordance with Vendor’s proposal and that Vendor’s services shall not infringe any third-party intellectual property rights.
   B. The Contractor agrees that the goods and services furnished under any award resulting from this solicitation shall be covered by the most favorable commercial warranties the contractor gives any customer for such goods and services and that the rights and remedies provided therein are in addition to and do not limit those available to Virginia Tech by any other clause of this solicitation. A copy of this warranty must be furnished with the proposal.
Attachment D

Contract UCP-TS-C02-12

Agreements for Virginia Tech Use:
Master Professional Services Agreement, Maintenance and Support Agreement,
Google Apps Customer Agreement
This MASTER PROFESSIONAL SERVICES AGREEMENT ("Agreement"), is made and entered into as of January 1, 2012 (the “Effective Date”), by and between SADA Systems Inc., a corporation organized under the laws of the state of California, with offices 5250 Lankershim Blvd., Suite 620, North Hollywood, CA 91601 (“SADA”), and Virginia Polytechnic Institute and State University, a state government agency and educational institute of the Commonwealth of Virginia with offices at 1700 Pratt Drive, Blacksburg, Virginia 24061 (“Client”). SADA and Client may be referred to in this Agreement individually as a “Party” and collectively as the “Parties.”

1. BACKGROUND, OBJECTIVES, CONSTRUCTION AND INTERPRETATION

1.1 Background and Objectives. This Agreement will serve as a framework under which SADA will provide certain information technology services (the “Services”), as described in Exhibit A (Statement of Work), attached hereto and incorporated herein, and as further requested by Client from time to time during the term of this Agreement and agreed upon in an executed Statement of Work (as defined in Section 2.2).

1.2 Definitions.
(A) Capitalized terms used in this Agreement have the meaning assigned to them in the applicable Section. Terms, acronyms and phrases that are used in the information technology industry or other pertinent business context should be interpreted in accordance with their generally understood meaning in such industries or business context.

(B) The word “include” and its derivatives (such as “including” and “includes”) mean “include without limitation.”

1.3 References and Interpretation.
(A) Headings, captions and titles used in this Agreement are included for convenience only and in no way define the scope or content of this Agreement or are to be used in the construction or interpretation of this Agreement. Any reference to a particular article or section number or exhibit is a reference to that specified article, section or exhibit of this Agreement, except to the extent that the cross-reference expressly refers to another document.

(B) If there is a conflict or inconsistency between the terms of this Agreement and any executed Statement of Work, the terms of this Agreement will prevail except to the extent that the executed Statement of Work specifically and expressly states an intent to supersede specific terms of this Agreement with applicability only to that executed Statement of Work. Notwithstanding the preceding sentence, no executed Statement of Work will be effective to: (1) expand, eliminate or restrict the scope of any indemnity obligation set forth in Article 10; (2) change any limitation of liability set forth in Article 11; or (3) settle or resolve any dispute between the Parties.

2. SCOPE OF SERVICES

2.1 Provision of Services. SADA will perform the Services identified in Exhibit A and those Services identified in additional Statements of Work entered into and executed by each of the Parties. Absent an executed Statement of Work, this Agreement does not, in and of itself, represent a commitment by either Party to provide any minimum amount of charges or services.

2.2 Statements of Work. From time to time during the term of this Agreement, Client may ask SADA to perform services that are not described in an executed Statement of Work or this Agreement.
Following any such request, SADA will prepare and deliver a Statement of Work substantially in the form of Exhibit A ("Statement of Work"). Each Statement of Work will contain:

(A) a description of the work SADA expects to perform in connection with such project, including a description of any deliverables;

(B) a prospective schedule for commencing and completing such work; and

(C) SADA’s prospective charges for such work.

If a proposed Statement of Work is mutually acceptable to the Parties, the Parties will execute such Statement of Work. Each executed Statement of Work will incorporate and be subject to all the terms and conditions of this Agreement, except for any provisions of this Agreement that are specifically excluded or modified in such executed Statement of Work (subject to Section 1.3(B)).

2.3 Modification of an Executed Statement of Work. Either Party may request modifications to an executed Statement of Work by submitting a written change order request to the other Party (each, a "Change Order"). If acceptable to both Parties, the Change Order will be executed by the Parties and will become part of the applicable executed Statement of Work. SADA will not be bound by the terms of any Change Order until it is executed by SADA.

2.4 Cooperation. Client understands that SADA’s performance is dependent on Client’s timely and effective cooperation, and that the quality of the Services are dependent on Client providing timely and accurate information to SADA and access to the required Client resources in accordance with the objectives of the applicable executed Statement of Work. Accordingly, any delay or nonperformance by SADA will be excused if and to the extent that such nonperformance results from Client’s failure to perform its responsibilities.

3. TERM, TERMINATION AND SUSPENSION OF SERVICES

3.1 Term. The term of this Agreement will begin on the Effective Date and will continue in effect until the later of the active time period of Contract UCP-TS-C02-12, and (B) the expiration or earlier termination of the last remaining executed Statement of Work, unless extended or terminated earlier in accordance with the terms of this Agreement. The Parties may agree to extend the term by written agreement to that effect.

3.2 Termination for Cause. If a Party commits: (A) a material breach of this Agreement that is capable of being cured within 30 days after notice of breach from the non-breaching Party, but is not cured within such period, or (B) a material breach of this Agreement that is not subject to cure with due diligence within 30 days of written notice thereof, then the non-breaching Party may, by giving written notice to the breaching Party, terminate this Agreement or the applicable Statement of Work, as of a date specified in the notice of termination.

3.3 Termination for Non-Payment. If undisputed invoices under this Agreement totaling at least two months’ charges are at any time outstanding and unpaid for 45 days, and Client fails to make such payment within 30 days of receiving written notice from SADA of its failure to make such payment, SADA may, by giving written notice to Client, terminate this Agreement and any executed Statement of Work as of the date specified in the notice of termination.

3.4 Termination for Convenience. Client reserves the right to terminate or cancel this Agreement or any executed Statement of Work as set forth in Section 3 of the terms and conditions contained within Client's RFP #0016512 included in the Standard Contract, the terms of which are incorporated in this Agreement.

3.5 Consequences of Termination. If this Agreement or any executed Statement of Work is terminated in accordance with the terms of this Article, SADA will be entitled to receive payment for all Services performed prior to termination in accordance with the terms of this Agreement or the applicable
executed Statement of Work. In addition, if SADA terminates any executed Statement of Work pursuant to Section 3.2 or Section 3.3, SADA will be entitled to reimbursement for any reasonable obligations SADA has entered into for the purpose of performing Services that cannot be cancelled. Termination of an executed Statement of Work will not affect any other executed Statements of Work then in effect. Termination of this Agreement will result in immediate termination of all executed Statements of Work then in effect.

4. Intentionally deleted.

5. PROPRIETARY RIGHTS

5.1 Client IP. As between Client and SADA, all right, title and interest in and to Client IP (as defined below) will remain the exclusive property of Client. To the extent necessary to provide the Services, Client hereby grants SADA, solely to provide the Services, a non-exclusive, non-transferable, fully paid-up and royalty-free, limited right to access and use the Client IP; provided that the rights granted to SADA hereunder will automatically expire effective upon the date that SADA ceases, for any reason, to provide the applicable Services. For purposes of this Agreement, “Client IP” will mean (A) software and tools, (B) processes, procedures and methodologies, (C) formulas, templates and formats, and (D) documents and other written materials, whether proprietary to Client or licensed to Client from third parties (other than SADA), that are provided to SADA by Client in order for SADA to provide the Services and fulfill its obligations under this Agreement.

5.2 SADA IP.

(A) As between SADA and Client, all right, title and interest in and to SADA IP (as defined below) will remain the exclusive property of SADA. Except to the extent that the Parties enter into separate license agreements with respect to any software products to be provided by SADA (in which case such software products will be governed by the terms of those license agreements), to the extent necessary to receive or use the Services or use any deliverable, SADA hereby grants to Client a perpetual, non-exclusive, worldwide, fully paid-up and royalty-free license to access and use (and to allow third parties to access and use solely for the benefit of Client) the SADA IP, for no additional consideration. Notwithstanding the foregoing, in the event that a Statement of Work provides for services and deliverables to be provided to Client on a trial or pilot basis, Client’s license to access and use any SADA IP necessary to receive or use the services or deliverables provided as part of such trial or pilot will not be perpetual, but will be limited to the period of such trial or pilot phase, as set forth in the applicable Statement of Work.

(B) Nothing in this Section will be construed to grant Client any right to separate SADA IP from the deliverable into which it is incorporated and Client will not (and will not knowingly allow any third party to) adapt, modify, translate, reverse engineer, decompile, disassemble or attempt to decode or disassemble any source code or underlying ideas or algorithms of any SADA IP or part thereof. Client will not sell, rent, lease, sublease, license, lend, market or commercially exploit such SADA IP or use SADA IP for the benefit of any affiliate, organization or other third party not contemplated by the applicable executed Statement of Work, or assign or transfer any rights with respect to SADA IP granted under this Agreement.

(C) For purposes of this Agreement, “SADA IP” will mean (A) software and tools, (B) processes, procedures and methodologies, (C) formulas, templates and formats, and (D) documents and other written materials, whether proprietary to SADA or licensed to SADA from third parties (other than Client or its affiliates) that are used to provide the Services, together, in each case, with any modifications or enhancements thereto and derivative works based thereon. Client acknowledges and agrees that with respect to any SADA IP licensed to SADA from third parties, any rights granted to SADA hereunder or under any executed Statement of Work, will be subject to all restrictions set forth in the applicable third party agreements.

5.3 Developed Property and Works Made for Hire. Subject to Section 5.2, SADA acknowledges and agrees that Client will have all right, title and interest in and to all Developed Property (as defined
below) developed in the course of providing the Services. All Developed Property developed under this Agreement in accordance with the terms of an executed Statement of Work will be deemed to be “works made for hire.” To the extent any Developed Property is not deemed “works made for hire” by operation of law, SADA hereby irrevocably assigns, transfers and conveys to Client, without further consideration, all of its right, title and interest in and to such Developed Property (including all patent, copyright, trademark, trade secret and other intellectual property and proprietary rights). SADA will execute any documents or take any other actions as may be reasonably necessary, or as Client may reasonably request, to perfect the ownership rights defined in this Section. For purposes of this Agreement, “Developed Property” will mean intellectual property generated or developed specifically for Client by SADA under an executed Statement of Work and paid for by Client. To qualify as Developed Property under this Agreement, such intellectual property must be explicitly and specifically called out in an executed Statement of Work and such executed Statement of Work must include a written acknowledgement by SADA that the Parties intend to transfer the rights to such intellectual property to Client upon payment by Client.

5.4 Residual Knowledge. Nothing in this Agreement will restrict a Party from using Services-related ideas, concepts, know-how, methodologies, processes, technologies, algorithms or techniques that are general in nature and retained in the unaided mental impressions of the Party’s personnel, which either Party, individually or jointly, develops or discloses under this Agreement; provided that, in doing so, each Party does not breach its obligations under Article 7 or infringe the intellectual property rights of the other Party or third parties who have licensed or provided materials to the other Party. Except for the license rights set forth in this Article, neither this Agreement nor any executed Statement of Work grants any license to either Party under any patents or copyrights of the other Party. The Parties acknowledge that SADA has the right to: (A) provide consulting or other services of any kind or nature to any person or entity as SADA, in its sole discretion, deems appropriate, and (B) use any works of authorship or other intellectual property included in the deliverables (other than Developed Property, if any) to develop for itself, or for others, materials or processes similar to those contemplated or produced under this Agreement.

6. CHARGES AND INVOICES

6.1 General. Subject to the provisions of this Agreement, Client will pay SADA the amounts set forth in each executed Statement of Work (including any Change Orders thereto).

6.2 Reimbursement of Expenses. Client agrees to reimburse SADA for costs and expenses incurred in connection with SADA’s performance of the Services, including reasonable travel expenses, provided Client has approved such expenses in advance. SADA will provide Client with receipts or other documentation substantiating all reimbursable costs and expenses.

6.3 Invoices and Payment. SADA will invoice Client for all amounts due under an executed Statement of Work in accordance with the schedule set forth in such executed Statement of Work. Each invoice submitted to Client pursuant to this Agreement will be due and payable by Client within 30 days of receipt.

6.4 Disputed Fees and Late Payments. Client agrees to notify SADA within 15 days of its receipt of an invoice from SADA, if Client disputes any amount or item in such invoice in good faith. Notwithstanding any dispute, Client will pay the undisputed portion of an invoice when due and payable. If Client withhold any amount associated with disputed amounts pursuant to this Section, Client will provide SADA with a description of the basis for such withholding. Upon resolution of a dispute involving any withheld amounts, Client will pay SADA such portion, if any, of the disputed amount agreed or determined to be owing to SADA within 30 days after resolution of the dispute.

7. CONFIDENTIALITY

7.1 Disclosure of Confidential Information. The Parties agree that in the course of SADA’s performance of the Services, each Party may access, receive or exchange information that is confidential in nature. For purposes of this agreement “Confidential Information” will include all information, in any
form, furnished or made available, directly or indirectly, by one Party ("Disclosing Party") to the other Party ("Recipient") that is marked confidential, restricted, or is otherwise designated as confidential. Confidential Information will also include information that, by virtue of the nature of the information or the circumstances surrounding disclosure, a reasonable party would understand to be proprietary to Disclosing Party or confidential, including without limitation: (A) any personally identifiable information or financial information of any individual; (B) information concerning the operations, affairs and business of a Party, a Party’s financial affairs, or a Party’s relations with its customers and employees; (C) in the case of Client, Client IP; and (D) in the case of SADA, SADA IP.

7.2 Exclusions. Confidential Information does not include, and this Article does not apply to, information that (A) is or subsequently becomes published or available to the public through no fault of Recipient, (B) is received by Recipient from a third party without a duty of confidentiality; (C) is independently developed by Recipient without reference to Disclosing Party’s Confidential Information, or (D) was in Recipient’s possession or was known to Recipient before it was disclosed to Recipient by Disclosing Party.

7.3 Restrictions on Disclosure and Use. The Parties agree:

(A) Neither Party will make any use of the other Party’s Confidential Information or any copies thereof, for any purpose other than those contemplated by this Agreement.

(B) Neither Party will reveal, disclose or provide access to the other Party’s Confidential Information to any third party without the prior consent of such Party, provided that both Parties may share Confidential Information with their responsible employees who have a need to know such Confidential Information to perform their duties. Client understands that all materials provided to Client by SADA are provided solely for Client’s internal use. Notwithstanding anything to the contrary in this paragraph, SADA may disclose Confidential Information to properly authorized entities as and to the extent necessary for performance of the Services, so long as in each such case, the receiving entity first agrees to the obligations described in this Article.

(C) Recipient will take security precautions at least as great as the precautions Recipient takes to protect its own confidential information, and at any rate will take commercially reasonable security precautions to ensure that no one, other than a person authorized pursuant to this Section, gains access to Disclosing Party’s Confidential Information without Disclosing Party’s prior written consent. In the event that Recipient becomes aware of any unauthorized use or disclosure of Disclosing Party’s Confidential Information, Recipient will immediately give notice to Disclosing Party and will assist Disclosing Party in remedying such unauthorized use or disclosure.

(D) Recipient is permitted to disclose Confidential Information as required by law, regulation or subpoena, provided that Recipient will (i) give Disclosing Party prompt notice of any such requirement, which notice must be sufficient to permit Disclosing Party to seek relief to prevent such disclosure, (ii) cooperate with Disclosing Party to secure confidential treatment of the Confidential Information, and (iii) disclose only that portion of Disclosing Party’s Confidential Information that is legally required.

(E) Confidential Information is and will remain the exclusive property of Disclosing Party. Each Party agrees that it will have no proprietary interest in the other Party’s Confidential Information and that nothing contained in this Agreement will be construed to grant either Party any rights, by license or otherwise, to any of the other Party’s Confidential Information disclosed pursuant to this Agreement.

(F) The obligations set forth in this Section will apply to Confidential Information provided, furnished or otherwise disclosed by Disclosing Party to Recipient, whether prior to or following the Effective Date.

7.4 Controlling Provisions. For purposes of this Agreement, each executed Statement of Work, and the Services contemplated by this Agreement and such executed Statements of Work, the provisions
of this Article will have precedence over and supersede any confidentiality or non-disclosure agreement executed by the Parties prior to the Effective Date.

8. REPRESENTATIONS, WARRANTIES AND COVENANTS

8.1 Authorization. Each Party represents and warrants to the other that: (A) it has the requisite corporate power and authority to enter into this Agreement and to carry out the transactions contemplated by this Agreement; and (B) the execution, delivery and performance of this Agreement and the consummation of the transactions contemplated by this Agreement have been duly authorized by the requisite corporate action on the part of such Party.

8.2 Performance of Services. SADA represents, warrants and covenants to Client that the Services will be performed by qualified personnel with promptness and diligence in a workmanlike manner, consistent with applicable industry standards.

8.3 Viruses and Disabling Code. SADA will use commercially reasonable efforts to prevent the coding or introduction of viruses, disabling code or similar items into the Client systems by SADA or its agents; and SADA will, in the event a virus, disabling code or similar item is found to have been introduced into the software Deliverables or Client systems by SADA or its agents, at no additional charge, assist Client in reducing the effects of the virus, disabling code or similar item.

8.4 Disclaimer. OTHER THAN AS PROVIDED IN THIS AGREEMENT, NEITHER PARTY PROVIDES ANY EXPRESS WARRANTIES OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN ADDITION, SADA MAKES NO EXPRESS OR IMPLIED WARRANTIES RELATING TO THIRD PARTY PRODUCTS OR SERVICES.

8.5 Limited Warranty. In the event that any implied warranties, guarantees or conditions implied by local law cannot be waived, then any such implied warranties are limited in duration to 90 days from delivery of the applicable Service or deliverable.

9. Intentionally deleted.

10. INDEMNIFICATION

10.1 By SADA. SADA agrees to indemnify, defend, and hold Client harmless from and against all losses, liabilities, damages, and related costs (including settlement costs and reasonable attorneys' fees) (collectively, “Losses”) arising out of a third party claim that the Services, SADA IP or any deliverables infringe or misappropriate any patent, copyright, trade secret or trademark of a third party. Notwithstanding the foregoing, in no event will SADA have any obligations or liability under this Section arising from: (A) use of any Service or deliverable in a modified form or in combination with materials not furnished or approved by SADA, (B) use by Client or its agents of such item in a manner not reasonably consistent with the applicable specifications, requirements or instructions for such item, and (C) any content, information or data provided by Client or other third parties.

10.2 Infringement. If the Services or any deliverable or item used by SADA to provide the Services or any deliverable becomes, or in SADA's reasonable opinion is likely to become, the subject of an infringement or misappropriation claim or proceeding, SADA will, at its expense: (A) secure the right to continue using the Services, deliverable or item; (B) replace or modify the Services, deliverable or item to make it non-infringing, provided that any such replacement or modification will not degrade the performance or quality of the affected component of the Services or deliverable; or (C) if SADA cannot accomplish either of the foregoing using commercially reasonable efforts, and only in such event, SADA will discontinue providing the Services or remove the deliverable or item and the charges will be equitably adjusted to reflect such removal.

10.3 General. Client will promptly notify SADA of any claim for which it is seeking indemnification and will cooperate with SADA in defending the claim. SADA will have full control and authority over the
defense, provided that: (A) any settlement requiring Client to admit liability or pay any money will require Client’s prior written consent, such consent not to be unreasonable withheld or delayed; and (B) Client may join in the defense of a claim with its own counsel at its own expense.

11. LIABILITY

11.1 Limitation of Liability.

(A) In no event will either party be held liable under this Agreement for special, indirect, consequential, exemplary or punitive damages (including, without limitation, damages for loss of data, business interruption or lost profits), whether in an action of contract, negligence, or otherwise, even if such party is aware of or has been advised of the possibility of such damages in advance and even if direct damages do not satisfy a remedy.

(B) Except as provided in Section 11.2, neither party may be held liable under this Agreement for more than the aggregate amount actually paid to SADA by Client under the applicable Statement(s) of Work giving rise to such loss.

11.2 Exceptions to Limitation of Liability. The limitations set forth in Section 11.1(B) will not apply to: (A) damages occasioned by a Party’s breach of its obligations with respect to the other Party’s intellectual property rights, (B) Losses that are the subject of indemnification obligations under this Agreement, or (C) Losses determined to be the direct result of a Party’s gross negligence or intentional or willful misconduct.

12. FORCE MAJEURE

No Party will be liable for any default or delay in the performance of its obligations under this Agreement if and to the extent such default or delay is caused, directly or indirectly, by fire, flood, earthquake, elements of nature or acts of God, riots, civil disorders, acts of terrorism, or any other similar cause beyond the reasonable control of such Party (each such event, a “Force Majeure Event”). Any Party so delayed in its performance will promptly notify the Party to whom performance is due by telephone (to be confirmed in writing within two days of the inception of such delay) and describe at a reasonable level of detail the circumstances causing such delay.

13. Intentionally deleted.

14. GENERAL PROVISIONS

14.1 Relationship of the Parties. SADA, in furnishing the Services, is acting as an independent contractor. SADA is not an agent of Client and has no authority to represent Client as to any matters, except as expressly authorized in this Agreement.

14.2 Waiver of Default. No delay or omission by either Party to exercise any right or power under this Agreement will be construed to be a waiver thereof. A waiver by either Party of any breach or covenant will not be construed to be a waiver of any succeeding breach thereof or of any other covenant.

14.3 Third Party Beneficiaries and Use of Work. Neither Party intends this Agreement to benefit, or create any right or cause of action in or on behalf of, any person or entity other than the Parties. Client understands and agrees that Services performed by SADA under this Agreement are intended only for the parties specified in the applicable executed Statement of Work and may be misleading if used in another context or for another party and agrees not to use any deliverables or documents produced under this Agreement for any purpose other than the intended purpose without SADA’s prior written consent.
14.4 **Survival.** The provisions of Section 4, Article 5, Section 6.4, Article 7, Section 8.4, Article 10, Article 11, Article 13 and this Article, as well as any other provision of this Agreement that contemplates performance or observance subsequent to termination or expiration of this Agreement will survive expiration or termination of this Agreement and continue in full force and effect for the period set forth therein, or if no period is set forth therein, indefinitely.

14.5 **Severability.** If any provision of this Agreement is found to be illegal or otherwise unenforceable in any respect, that provision will be deemed to be restated to reflect as nearly as possible the original intent of the Parties in accordance with applicable law. The remainder of this Agreement will remain in full force and effect.

14.6 **Entire Agreement; Amendment and Waiver.** This Agreement and each of the executed Statements of Work hereto, including any exhibits referred to herein or therein, each of which is incorporated herein for all purposes, is a part of Contract UCP-TS-C02-12 executed by Client and SADA (the "Standard Contract") and is not a standalone agreement. To the extent that anything contained in this Agreement conflicts or is inconsistent with the terms and conditions contained within Client’s RFP #0016512 included in the Standard Contract, the RFP terms shall take precedence. No change, waiver or discharge hereof will be valid unless made in writing and signed by an authorized representative of the Party against which such change, waiver of discharge is sought to be enforced. Notwithstanding the foregoing, the parties agree that the requirements set forth in Section 23.C of the Special Terms and Conditions to the Standard Contract will not apply to SADA.

14.7 **Counterparts.** This Agreement may be executed in any number of counterparts, all of which taken together will constitute one single agreement between the Parties.

**IN WITNESS WHEREOF,** this Agreement has been executed by the Parties through their duly authorized officers as of the date set forth above.

SADA Systems, Inc. Virginia Polytechnic Institute and State University

_____________________________  _____________________________
Tony Safoian, President and CEO  Print name:   John D. Krallman
Print title:  Director of IT Business & Financial Affairs
EXHIBIT A

STATEMENT OF WORK

This Statement of Work is entered into in connection with the Master Professional Services Agreement ("Agreement") by and between SADA Systems Inc. ("SADA") and Virginia Polytechnic Institute and State University ("Client") dated [DATE OF AGREEMENT]. The terms and conditions of the Agreement are incorporated herein by reference. Capitalized terms not defined in this Statement of Work will have the same meaning given to them in the Agreement. This Statement of Work describes certain Services and deliverables that will be provided by SADA to Client pursuant to the terms and conditions of the Agreement.

GENERAL INFORMATION

<table>
<thead>
<tr>
<th>Project Title:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
</tr>
<tr>
<td>Term of SOW:</td>
</tr>
<tr>
<td>Service Recipients:</td>
</tr>
</tbody>
</table>

SADA INFORMATION

<table>
<thead>
<tr>
<th>Project Manager:</th>
</tr>
</thead>
<tbody>
<tr>
<td>SADA Personnel:</td>
</tr>
<tr>
<td>SADA sites:</td>
</tr>
</tbody>
</table>

PROJECT TRACKING AND OVERSIGHT

<table>
<thead>
<tr>
<th>Reports:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meetings:</td>
</tr>
</tbody>
</table>

SERVICES

Scope of Project; Services.

Description of Services

CLIENT RESPONSIBILITIES

[This Section should describe Client’s obligations under this Statement of Work.]

Client Facilities.

Client will provide the following facilities or access to the following facilities to SADA in accordance with the terms of the Agreement:
[Enter details concerning the work space, computer equipment, and access provided by Client to SADA personnel performing Services under this Statement of Work.]

PRICING

The following charges apply to the Services to be performed under this Statement of Work.
This MAINTENANCE AND SUPPORT AGREEMENT ("Agreement"), is made and entered into as of [EFFECTIVE DATE] (the “Effective Date”), and sets forth the terms and conditions governing the maintenance and support services to be provided by SADA Systems Inc., a corporation organized under the laws of California ("SADA") to Virginia Polytechnic Institute and State University, a state government agency and educational institute of the Commonwealth of Virginia ("Client") with respect to the SADA software products identified in the table below (together, “Software”), which Software is being provided to Client under the Statement of Work to the Master Professional Services Agreement between the parties, each dated [EFFECTIVE DATE OF SOW].

<table>
<thead>
<tr>
<th>SADA Software Product(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-Premise Sync for Google Apps</td>
</tr>
<tr>
<td>Hosted Sync for Google Apps</td>
</tr>
<tr>
<td>AuthMagic for Google Apps (Password Sync)</td>
</tr>
<tr>
<td>On-premise Single Sign On for Google Apps</td>
</tr>
<tr>
<td>Hosted Single Sign On for Google Apps</td>
</tr>
</tbody>
</table>

1. TERM AND RENEWAL

1.1 Term. The term of this Agreement will begin on the date set forth in the preamble, subject to provision of payment, and will continue in effect for the period of time Contract UCP-TS-C02-12 is active (the “Initial Term”). The Agreement expires at the end of the term unless renewed.

1.2 Renewal. Within 60 days of expiration of the Initial Term or any renewal term, SADA will provide notification to Client with instructions for renewal. SADA may modify the fees for any renewal term upon written notice to Client at least 30 days prior to expiration of the then-current term.

1.3 Termination for Non-Payment. If undisputed invoices under this Agreement are at any time outstanding and unpaid for 45 days, and Client fails to make such payment within 30 days of receiving a written reminder notice from SADA of its failure to make such payment in a timely manner, SADA may, by giving written notice to Client, terminate this Agreement as of the date specified in the notice of termination.

2. MAINTENANCE AND SUPPORT SERVICES

2.1 Support Services. For so long as this Agreement is in effect, SADA will provide basic maintenance and support services (the “Support Services”) consisting of:

(A) Error Correction and Resolution. SADA will be responsible for using all reasonable diligence to correct verifiable and reproducible failures of the Software to conform in any material respect to its published specifications ("Errors") when reported in accordance with SADA’s standard reporting procedures, as set forth in Exhibit A. An “Error Correction” means either a modification or addition that, when made or added to the Software, brings the Software into material conformity with its published specifications, or a mutually agreed upon procedure or routine that, when observed in the regular operation of the Software, avoids the practical adverse effect of such nonconformity. An Error Correction, when completed, may be provided in the form of a “temporary fix,” consisting of sufficient programming and operating instructions to implement the Error Correction. Such temporary fixes shall be permanently resolved no later than the next release.
(B) **Staff.** SADA will maintain a trained staff capable of rendering the services set forth in this Agreement.

2.2 **Cooperation of the Customer.** Client agrees to notify SADA promptly following the discovery of any Error. Further, upon discovery of an Error, Client agrees, if requested by SADA, to submit to SADA a listing of output and any other reasonable and necessary data that SADA may require in order to reproduce the Error and the operating conditions under which the Error occurred or was discovered. In addition, Client is responsible for procuring, installing, and maintaining all equipment, telephone lines, communication interfaces, and other hardware necessary to operate the Software. SADA will not be responsible for delays caused by events or circumstances beyond its reasonable control.

Client acknowledges and agrees that SADA’s provision of Support Services is subject to the following:

(A) Client will provide SADA with necessary access to personnel and equipment;

(B) Client will provide supervision, control and management of the use of the Software. In addition, Client will implement procedures for the protection of information and the implementation of backup facilities in the event of errors or malfunction of the Software or equipment;

(C) Client will document and promptly report detected errors or malfunctions of the Software to SADA and take commercially reasonable steps necessary to carry out procedures for the rectification of errors or malfunctions within a reasonable time after such procedures have been received from SADA;

(D) Client is responsible for backup of all programs and data;

(E) Client will properly train its personnel in the use and application of the Software; and

(F) Client will retain responsibility for all change management, risk management and governance controls that Client deems appropriate or are required by Client’s internal policies and practices.

2.3 **Exceptions.** This Agreement does not include services requested as a result of, or with respect to, causes which are not attributable to SADA. Causes which are not attributable to SADA include, but are not limited to, the matters, which are not covered by the Support Services:

(A) Any problem resulting from the misuse, improper use, alteration or damage of the Software;

(B) Any problem caused by modifications in any version of the Software not made or authorized by SADA;

(C) Any problem resulting from programming other than the Software or equipment; or

(D) Any problem resulting from the combination of the Software with such other programming or equipment to the extent such combination has not been approved by SADA.

If Client requires support for any of the foregoing exceptions, Client will be responsible to pay SADA’s normal charges and expenses for time or other resources provided by SADA to diagnose or attempt to correct any such problem.

3. **MAINTENANCE AND SUPPORT FEES**

In consideration of the Support Services detailed in an executed SOW, if any, and subject to the terms and conditions of this Agreement, Client agrees to pay SADA a fee based on Contract UCP-TS-C02-12.
4. INCIDENT REPORTING, CATEGORIZATION, RESPONSE TIMES AND ESCALATION
SADA will manage Error Correction and Resolution in terms of incident reporting, categorization, response time and escalation as set forth in the service level agreement attached as Exhibit A. SADA may change its policies with respect to the matters set forth in Exhibit A from time to time, provided that SADA will provide Client with at least 30 days advance written notice of any material changes to such policies. If the proposed change has a material adverse effect on Client and Client does not agree to the change, Client will notify SADA prior to the implementation of a planned change. If Client notifies SADA as required, then Client will remain governed by the terms in effect immediately prior to the change (or any other arrangement agreed by the parties) until the end of the then-current term. If this Agreement is renewed, it will be renewed under SADA’s then current policies. SADA will undertake to implement any proposed changes to the matters set forth in Exhibit A in such a manner as to minimize an adverse impact to the level of service provided under the terms of this Agreement.

5. LIMITED WARRANTY AND DISCLAIMER

5.1 SADA will perform its services under this Agreement in a professional and workmanlike manner.

5.2 OTHER THAN AS EXPRESSLY PROVIDED IN THIS AGREEMENT, SADA DOES NOT PROVIDE ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR OTHERWISE. EXCEPT AS SET FORTH IN SECTION 5.1, WITH RESPECT TO ANY SOFTWARE TO BE PROVIDED UNDER THIS AGREEMENT, THE SOFTWARE IS BEING DELIVERED TO CLIENT AS-IS AND SADA MAKES NO WARRANTY AS TO ITS USE OR PERFORMANCE. SADA DOES NOT WARRANT THAT THE SOFTWARE WILL MEET CLIENT’S REQUIREMENTS; THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. SADA CANNOT WARRANT THE PERFORMANCE OR RESULTS CLIENT MAY OBTAIN BY USING THE SOFTWARE. IN ADDITION, SADA MAKES NO EXPRESS OR IMPLIED WARRANTIES RELATING TO ANY THIRD PARTY PRODUCTS OR SERVICES.

6. LIMITATION OF LIABILITY

6.1 IN NO EVENT, WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING BREACH OF WARRANTY, NEGLIGENCE, AND STRICT LIABILITY IN TORT), WILL SADA BE HELD LIABLE UNDER THIS AGREEMENT FOR LOSS OF DATA OR DATA STORAGE, SYSTEMS OR BUSINESS INTERRUPTION, COMPUTER FAILURE OR MALFUNCTION, OR FOR INDIRECT OR CONSEQUENTIAL (INCLUDING LOST PROFITS), EXEMPLARY, PUNITIVE OR SPECIAL DAMAGES ARISING IN ANY WAY OUT OF THIS AGREEMENT, EVEN IF SUCH PARTY IS AWARE OF OR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE, OR FOR ANY CLAIM BY ANY THIRD PARTY; PROVIDED, HOWEVER, THAT THIS LIMITATION DOES NOT APPLY WITH RESPECT TO DAMAGES DETERMINED TO BE THE DIRECT RESULT OF SADA’S GROSS NEGLIGENCE OR INTENTIONAL OR WILLFUL MISCONDUCT.

6.2 ANY DAMAGES THAT SADA IS REQUIRED TO PAY FOR ANY PURPOSE WHATSOEVER UNDER THIS AGREEMENT WILL BE LIMITED TO THE AGGREGATE FEE PAID UNDER THIS AGREEMENT.

7. MISCELLANEOUS

7.1 Waiver. No delay or omission by either party to exercise any right or power under this Agreement will be construed to be a waiver thereof. A waiver by either party of any breach or covenant will not be construed to be a waiver of any succeeding breach thereof or of any other covenant.

7.2 Severability. If any provision of this Agreement is found to be illegal or otherwise unenforceable in any respect, that provision will be deemed to be restated to reflect as nearly as possible the original intent of the parties in accordance with applicable law. The remainder of this Agreement will remain in full force and effect.
7.3 **Survival.** Sections 5 (Limited Warranty and Disclaimer), 6 (Limitation of Liability), and 7 (Miscellaneous) will survive any expiration or termination of this Agreement and continue in full force and effect.

7.4 **Force Majeure.** No Party will be liable for any default or delay in the performance of its obligations under this Agreement if and to the extent such default or delay is caused, directly or indirectly, by fire, flood, earthquake, elements of nature or acts of God, riots, civil disorders, acts of terrorism, or any other similar cause beyond the reasonable control of such Party (each such event, a “**Force Majeure Event**”). Any Party so delayed in its performance will promptly notify the Party to whom performance is due by telephone (to be confirmed in writing within two days of the inception of such delay) and describe at a reasonable level of detail the circumstances causing such delay.

7.5 **Entire Agreement; Amendment and Waiver.** This Agreement and its Exhibit A is a part of Contract #UCP-TS-C02-12 executed by Client and SADA (the “**Standard Contract**”) and is not a standalone agreement. To the extent that anything contained in this Agreement conflicts or is inconsistent with the terms and conditions contained within Client’s RFP #0016512 included in the Standard Contract, the RFP terms shall take precedence. No change, waiver or discharge hereof will be valid unless made in writing and signed by an authorized representative of the party against which such change, waiver or discharge is sought to be enforced.

**IN WITNESS WHEREOF,** this Agreement has been executed by the parties through their duly authorized officers as of the date set forth above.

SADA Systems, Inc. 

_____________________________  By:  ________________________________
Tony Safoian, President and CEO  John D. Krallman

CLIENT

_____________________________  ________________________________

Director of IT Business & Financial Affairs
Exhibit A: Service Level Agreement

Introduction

This exhibit sets forth the method by which SADA Systems, Inc. (SADA) determines incident prioritization, manages response times and escalates support requests in connection with the services it provides.

Priority Definition & Establishment

When a client notifies SADA of an incident, SADA will prioritize the incident in accordance with the following definitions, which are based on business impact. Incident prioritization is at the sole discretion of SADA. Any incidents which have been set above their allotted Priority will be dropped to the appropriate Priority by an authorized member at SADA, which will also reset the response time for the incident.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Definition</th>
<th>Example</th>
</tr>
</thead>
</table>
| Level 1  | • Defect causing the software product to be unusable or inoperable  
• Major function is unavailable with no acceptable bypass/workaround  
• Response time not being met | • Server crash/failure  
• Network failure |
| Level 2  | • Major function is unavailable but acceptable bypass/workaround is available | • Important file unavailable  
• Application fault |
| Level 3  | • Defect causing a minor function to be disabled.  
• Some function is not working correctly  
• Minimal impact on the user community | • Important meeting  
• File unavailable  
• Printer problem |
| Level 4  | • Defect is not time-critical  
• Single user impact  
• Defect causing no function to be disabled  
• Does not impact user community | • How do I…?  
• How much would …cost?  
• Non critical info requests |

Response & Resolution Timeframes

SADA’s incident management process includes triage, documentation and prioritization, and is designed to deliver the following elements:

- A clear agreement between SADA and the client as to what the incident is about
- An owner for the problem both at SADA and your company.
- A clear summary from SADA as to what the next steps are.
- An expected time frame to temporary and/or permanent resolution of the problem.

In furnishing you with this information SADA satisfies the ‘Response’ as constituted by this service level agreement. The response times set out by this service level agreement begin only after an incident has been reported, captured, triaged and prioritized. Target response times are as follows:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Max. Response Time</th>
<th>Workaround Resolution Time</th>
<th>Status Updates</th>
<th>Permanent Resolution Times</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>60 minutes</td>
<td>4 clock hours</td>
<td>2 Hours</td>
<td>2 days</td>
</tr>
<tr>
<td>Level 2</td>
<td>90 minutes</td>
<td>8 clock hours</td>
<td>6 hours</td>
<td>4 days</td>
</tr>
<tr>
<td>Level 3</td>
<td>4 Hours</td>
<td>2 business days</td>
<td>1 business day</td>
<td>15 days</td>
</tr>
<tr>
<td>Level 4</td>
<td>8 Hours</td>
<td>7 business days</td>
<td>1 business day</td>
<td>30 days</td>
</tr>
</tbody>
</table>
Response times applied to support incidents that are reported outside SADA’s normal business hours (Monday through Friday, 9:00am – 6:00pm pacific time, excluding national holidays) must be initiated by way of SADA’s emergency telephone system. Incidents reported by email and/or the Client Portal outside SADA’s regular business hours will be responded to on the start of the next business day (at which time the response time for the incident will begin), under the guidelines provided above.

Escalation & Remediation

An incident can be anything that degrades or interrupts the client’s information technology supported business processes, activities and workflows. The following process describes the means in which SADA will handle all incidents.

1. Support request is received
2. Service request is created
3. Issue is identified, documented, triaged, prioritized and assigned within the incident management system.
4. Issue is qualified to determine if it can be resolved through Tier 1 Support

**If issue can be resolved through Tier 1 Support:**
5. Level 1 Resolution - issue is worked to successful resolution.
6. Quality Control - Issue resolution is verified with client
7. Service request is closed, after complete resolution details have been updated in the incident management system.

**If issue cannot be resolved through Tier 1 Support:**
6. Issue is escalated to Tier 2 Support
7. Issue is qualified to determine if it can be resolved by Tier 2 Support

**If issue can be resolved through Tier 2 Support:**
8. Level 2 Resolution - issue is worked to successful resolution
9. Quality Control – Issue resolution is verified with client
10. Service request is closed, after complete resolution details have been updated in the incident management system.

**If issue cannot be resolved through Tier 2 Support:**
9. Issue is escalated to Tier 3 Support
10. Issue is qualified to determine if it can be resolved through Tier 3 Support

**If issue can be resolved through Tier 3 Support:**
11. Level 3 Resolution - issue is worked to successful resolution
12. Quality Control – Issue resolution is verified with client.
13. Service request is closed, after complete resolution details have been updated in the incident management system.

**If issue cannot be resolved through Tier 3 Support:**
12. Issue is escalated to onsite support (dispatch)
13. Issue is qualified to determine if it can be resolved through onsite support

**If issue can be resolved through Onsite Support:**
14. Onsite resolution - issue is worked to successful Resolution.
15. Quality Control – Issue resolution is verified with client
16. Service request is closed, after complete resolution details have been updated in the incident management system.

**If issue cannot be resolved through Onsite Support:**
17. Management Decision Point – request is updated with complete details of all activity performed. Next actionable step based on facts at hand and available resources.
18. Possible outcomes may include:
   i. Re-entry into the Incident Management process
   ii. Escalation/entry into the Problem Management process
   iii. Service Credits (as defined below)
vi. Client negotiation or compromise

Support Tiers

SADA has established the following Tiered support model for IT Service Desk (Helpdesk) operations. The SADA Helpdesk (including the emergency telephone system for incidents reported outside SADA’s normal business hours) is the single point of contact (SPOC) for all issues reported, which are then identified, documented, prioritized and assigned to internal resources for troubleshooting and resolution prior to the performance of any quality assurance activities and final closure. This service level agreement is only in effect when incident requests are reported through the Helpdesk support system, via phone, email or the Client Portal.

SADA has developed this support Tier structure as the foundation of an incident management process/escalation path. The Tiered structure supports a scalable approach to incident management and problem management. It is important to understand that incidents can be escalated between and among these Tiers during maintenance, incident and problem management resolution. Furthermore, specific individuals can, at times, conduct all incident and problem management activities through several levels of escalation.

<table>
<thead>
<tr>
<th>Support Tier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1 Support</td>
<td>All support incidents begin in Tier 1, where the initial ticket is created,</td>
</tr>
<tr>
<td></td>
<td>the issue is identified and clearly documented, and a basic hardware/software</td>
</tr>
<tr>
<td></td>
<td>troubleshooting is initiated</td>
</tr>
<tr>
<td>Tier 2 Support</td>
<td>All support incidents that cannot be resolved with Tier 1 Support are</td>
</tr>
<tr>
<td></td>
<td>escalated to Tier 2, where more complex support on hardware/software issues</td>
</tr>
<tr>
<td></td>
<td>can be provided by more experienced engineers.</td>
</tr>
<tr>
<td>Tier 3 Support</td>
<td>Support incidents that cannot be resolved by Tier 2 Support are escalated</td>
</tr>
<tr>
<td></td>
<td>to Tier 3, where support is provided by the most qualified and experienced</td>
</tr>
<tr>
<td></td>
<td>engineers who have the ability to resolve the most complex issues, and/or</td>
</tr>
<tr>
<td></td>
<td>can collaborate with 3rd party (vendor) support engineers.</td>
</tr>
</tbody>
</table>

Service Downtime and Service Credits

For purposes of this service level agreement, “Service Downtime” is any unplanned interruption in service availability during which the Client is unable to access the services or software, provided the interruption is determined (and confirmed by SADA) to have been caused by a problem within the service or software provided by SADA. Service Downtime will be measured as the total length of time of the unplanned interruption in service availability during a calendar month. Scheduled downtime will not count toward Service Downtime and SADA will have no responsibility for any unplanned outages arising from third-party hardware or software failures. Response and Resolution Time Credit Schedule:

For any breach of SADA’s obligations under “Response and Resolution Time Frames” above, the following credits will apply:

<table>
<thead>
<tr>
<th>Type of Breach</th>
<th>Number of times</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Time Breach</td>
<td>1-2 times in any calendar month</td>
<td>10 day extension to current term of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintenance and Support Agreement</td>
</tr>
<tr>
<td>Response Time Breach</td>
<td>3-4 times in any calendar month</td>
<td>20 day extension to current term of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintenance and Support Agreement</td>
</tr>
<tr>
<td>Response Time Breach</td>
<td>5 or more times in any calendar month</td>
<td>30 day extension to current term of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintenance and Support Agreement</td>
</tr>
<tr>
<td>Consecutive Response Time Breaches</td>
<td>1 or more Response Time breaches in each month of any</td>
<td>30 day ADDITIONAL extension to current</td>
</tr>
<tr>
<td></td>
<td>consecutive 3-month period</td>
<td>term of Maintenance and Support Agreement</td>
</tr>
<tr>
<td>Any Resolution Time Breach</td>
<td>N/A</td>
<td>30 day extension to current term of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintenance and Support Agreement</td>
</tr>
</tbody>
</table>
Claiming Service Credits; Maximum Service Credits:

In order to receive any Service Credit described above, a client must notify SADA in writing that it is electing to claim such Service Credit within 30 days of the time client becomes eligible to receive a Service Credit. In the case of Service Credits tied to a Response Time breach, such notice will be timely if given within 30 days following the close of the calendar month in which such breach occurred. Any such notice should be sent to servicecredits@sadasystems.com along with incident details including the date and time of the first report to SADA, the ticket # assigned by SADA, and the reason for the credit request. Failure to comply with this requirement in a timely manner will forfeit Customer’s right to receive a Service Credit for a period as to which the notice requirement has expired. In no event will the aggregate number of Service Credits extended by SADA to a client for breaches occurring in a single calendar month exceed two months or 60 days (whichever is less) extension to the current term of the Maintenance and Support Agreement. Service Credits may not be exchanged for, or converted to, monetary amounts.

Credit Calculation Examples:

**Response Time Breach:**
- Response Time breach on Jan 1st and Jan 15th,
  Breach Count = 2, Extension Credit = 10 days (2x in one calendar month)

- Response Time breach on Jan 31st and Feb 1st,
  Breach Count = 2, Extension Credit = 20 days (1x in each of two calendar months)

- Response Time breach on June 30th, July 30th and August 30th
  Breach Count = 3, Extension Credit = 60 days (1x in June; 1x in July and 1x August + 30 days for repeated breaches over consecutive 3-month period)

**Resolution Time Breach:**
- Resolution Time breach on Jan 1st,
  Breach Count = 1, Extension Credit = 30 days

- Resolution Time breach on April 1st and April 5th,
  Breach Count = 2, Extension Credit = 60 days

**Response & Resolution Time Breaches:**
- Response Time breach on August 1st, August 15th, August 20th,
  Resolution Time breach on August 25th,
  Extension Credit: 50 days (3 x Response in one calendar month, 1x Resolution)
This GOOGLE APPS CUSTOMER AGREEMENT (this “Agreement”), is made and entered into as of [EFFECTIVE DATE] (the “Effective Date”), between SADA Systems Inc., a corporation organized under the laws of the state of California, with offices at 5250 Lankershim Blvd., Suite 620, North Hollywood, CA 91601 (“SADA”), and Virginia Polytechnic Institute and State University, a state government agency and educational institute of the Commonwealth of Virginia, with offices at 1700 Pratt Drive, Blacksburg, Virginia 24061 (“Customer”).

1. SERVICES AND TERMS OF SERVICE

1.1 Service. This Agreement establishes the terms under which SADA, as an authorized reseller of Google, Inc. (“Google”), will provide Customer with access to the Google hosted services set forth in Exhibit A (the “Services”).

1.2 Support. Customer will respond to questions and complaints from the individuals Customer permits to use the Services (such individuals, “End Users”) or third parties relating to Customer’s or End Users’ use of the Services. SADA will provide front-line technical support directly to Customer’s technology administrators with respect to questions, complaints and other support issues that Customer cannot resolve, and SADA is hereby authorized by Customer to submit Customer support issues to Google on behalf of Customer. Customer may also contact Google with respect to technical support issues in accordance with Google’s technical support guidelines (the “TSSG”) available at http://www.google.com/apps/intl/en/terms/tssg.html or such other URL as may be provided by Google.

1.3 Google Apps Terms of Service. Customer understands and agrees that the End Users will be required to agree to Google’s Terms of Service before using the Services, which will be presented by Google upon End User’s first log in. The Terms of Service govern End User’s access to and use of the Services.

1.4 Service Levels. The Google Apps Covered Services (as defined in the Google SLA) will meet the requirements set forth in the Google Apps Service Level Agreement found at http://www.google.com/apps/intl/en/terms/sla.html (the “Google SLA”). In the event of a breach of such service levels, as Customer’s sole and exclusive remedy, Customer will be provided the remedies set forth in the Google SLA.

2. CUSTOMER OBLIGATIONS, During the term of this Agreement, Customer will have the following obligations, in addition to those set forth elsewhere in this Agreement.

2.1 Compliance with Law; Compliance with Agreement. Customer will comply with all laws, rules and regulations applicable to its use of the Services, including those regarding the management and administration of its electronic messaging system. Customer acknowledges and agrees that SADA and Google are serving as a data processor and their responsibilities and liability do not extend to the internal management or administration of Customer’s electronic messaging system or messages. Customer is responsible for ensuring that it and its End Users use the Services in accordance with the Terms of Service and Acceptable Use Policy, as set forth in Section 1.3 and Section 2.5.

2.2 Customer Administration of the Services. Customer is responsible for: (A) maintaining the confidentiality of the password and administrative account provided to Customer by Google for the purpose of administering End User accounts; (B) designating those of Customer’s employees and SADA’s employees who are authorized to access the administrative account; and (C) ensuring that all activities that occur in connection with Customer’s administrative account comply with the Terms of Service.
2.3 Privacy. Customer agrees to protect the privacy rights of its End Users in accordance with all applicable laws and regulations.

2.4 Unauthorized Use. Customer will use commercially reasonable efforts to prevent unauthorized use of the Services, and to terminate any unauthorized use. Customer will promptly notify SADA or Google of any unauthorized use of, or access to, the Services of which it becomes aware.

2.5 Acceptable Use Policy. Customer agrees that its use of the Services is subject to its compliance with Google’s Acceptable Use Policy, which is available at http://www.google.com/apps/intl/en/terms/use_policy.html (or such URL as Google may provide) and which may be updated from time to time.

2.6 Intended Use; Email Accounts. The Services are for use with normal business messaging traffic only, and may not be used for any other purpose, including use of the message encryption services (if applicable) with machine generated message encryption and delivery. For each End User for which Customer will be routing email and/or archiving email, if any, through the Services, Customer shall establish an email account in Google’s identity management systems. Failure to abide by the terms of this Section may be considered a material breach of this Agreement and, if not cured by Customer following notice by SADA, may result in a suspension of Services until such failure is remedied.

3. CHARGES AND PAYMENT

3.1 Fees. Customer will pay SADA the fee(s) set forth on Exhibit A to this Agreement in accordance with Section 3.3. Following the Initial Term, SADA has the right to change the fee, effective as of the next renewal date, provided that SADA will notify Customer of any fee increase prior to the expiration of the then-current term.

3.2 Support Charges. Any support to be provided by SADA under Section 1.3 of this Agreement will be performed on business days between the hours of 9:00 a.m. to 6:00 p.m. Pacific Time, at no additional cost. Any support services requested by Customer outside these hours will be billed to Customer at an hourly rate of $292.50.

3.3 Payment Options. Customer will pay for the Services on a full prepaid basis for the Initial Term of this Agreement and each succeeding 12-month renewal term, to the extent applicable.

(A) Fees for prepaid orders where SADA issues an invoice are due within thirty (30) days after Customer’s receipt of the invoice, and are considered delinquent 30 days after the due date of the applicable invoice.

3.4 Currency. Customer will make all payments in U.S. dollars.

4. TERM, TERMINATION AND ADDITIONAL END USER ACCOUNTS

4.1 Term. The term of this Agreement will begin on the Effective Date and will continue for an initial period as set forth in Exhibit A (such period, the “Initial Term”). At the end of the Initial Term, the parties may agree to renew this Agreement. All terms and conditions of this Agreement shall apply during each renewal term, except for the fees. The fee for each renewal term will be the rates then in effect, as described in Section 3.1.

4.2 Termination. This Agreement will terminate: (A) immediately upon termination or expiration of Customer’s right to use the Services as a result of a termination of the Terms of Service by Google or Customer; (B) upon expiration of the then-current term if Customer has not chosen to renew this Agreement prior to the expiration of the then-current term; or (C) upon expiration of the then-current term if SADA has provided at least 60 days’ advance written notice of termination to Customer.

4.3 Effects of Termination. If this Agreement terminates, then the rights granted hereunder by any party to the other will cease immediately and Customer’s access to the Services will cease.
4.4 Additional End User Accounts. Customer may alter the number of End User Accounts per Customer domain at any time. For End User Accounts added during the Initial Term or any Renewal Term, the initial term for such End User Accounts will be pro-rated, beginning on the date of the applicable order and ending on the expiration of the applicable term. Customer may request End User Accounts by notifying its designated SADA account manager. For each purchase of End User Accounts, SADA will issue a quote to Customer. End User Accounts automatically renew in accordance with the terms of this Agreement, unless terminated by either party in accordance with the terms of this Agreement. SADA cannot transfer End User Accounts from one Customer domain name to another.

4.5 Archived Messages. If the Services include archiving functionality, Customer messages will be retained for up to the period set forth in Exhibit A, provided that Customer renews the applicable Services with SADA for each year of such retention period. The retention period will apply to all data archived under the Services. Failure to renew the applicable Services during the retention period will terminate SADA's and Google's obligation to retain any of Customer's data or indexes.

5. CUSTOMER DATA AND CONFIDENTIAL INFORMATION

5.1 Customer Data. SADA will treat all Customer Data in accordance with laws and regulations applicable to the data and will implement policies and procedures with respect to the Customer Data no less protective of the rights of Customer or its End Users as those found in Google’s Privacy Policy (located at http://www.google.com/intl/en/privacy/privacy-policy.html) or Google’s Privacy Notice (located at http://www.google.com/apps/intl/en/terms/users_privacy.html). Changes to the Privacy Policy and Privacy Notice will be made as stated in the applicable policy. For purposes of this Agreement, “Customer Data” means all data and information provided by Customer's End Users via the sign up process for the Services, as well as data, including electronic messages and any attachments provided, generated, transmitted or displayed via the Services by Customer or its End Users.

5.2 Confidential Information. Each party will: (A) protect the other party’s Confidential Information with the same standard of care it uses to protect its own Confidential Information, but in no event less than reasonable care; and (B) not disclose the other party’s Confidential Information, except to affiliates, employees, agents and professional advisors who need to know it (and, in the case of non-employees, who have agreed in writing or are otherwise bound, to keep it confidential). Each party (and any affiliates, employees and agents to whom the Confidential Information was disclosed) may use such Confidential Information only to exercise rights and fulfill obligations under this Agreement, while using reasonable care to protect it. SADA is responsible for any actions of its affiliates, employees and agents in violation of this Section. Customer is responsible for any actions of its employees and agents in violation of this Section. For purposes of this Agreement, “Confidential Information” is information disclosed by one party to the other party under this Agreement that is marked as confidential or would normally be considered confidential under the circumstances. In particular, Customer Data and SADA’s pricing are Confidential Information.

5.3 Exceptions. Confidential Information does not include information that: (A) is or subsequently becomes published or available to the public through no fault of the recipient, (B) is received by the recipient from a third party without a duty of confidentiality; (C) is independently developed by recipient, or (D) was in the recipient’s possession or was known to the recipient before it was disclosed to the recipient by the disclosing party.

5.4 Required Disclosure. Each party may disclose the other party's Confidential Information when required by law but only after it, if legally permissible: (A) uses commercially reasonable efforts to notify the other party; and (B) gives the other party the chance to challenge the disclosure.

6. INTELLECTUAL PROPERTY RIGHTS. Except as expressly set forth herein, this Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other's intellectual property. As between the parties, Customer owns all Intellectual Property Rights in Customer
Data. The parties acknowledge and agree that Google owns all Intellectual Property Rights in the Services. For purposes of this Agreement, “Intellectual Property Rights” means current and future worldwide rights under patent law, copyright law, trade secret law, trademark law, moral rights law and other similar rights.

7. DISCLAIMER OF WARRANTIES. SADA AND GOOGLE MAKE NO WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY OR NONINFRINGEMENT. SADA AND GOOGLE MAKE NO REPRESENTATION ABOUT ANY CONTENT OR INFORMATION MADE ACCESSIBLE BY OR THROUGH THE SERVICE. CUSTOMER ACKNOWLEDGES THAT THE SERVICES ARE NOT A TELEPHONY SERVICE AND THAT THE SERVICES ARE NOT CAPABLE OF PLACING OR RECEIVING ANY CALLS, INCLUDING EMERGENCY CALLS, OVER PUBLICLY SWITCHED TELEPHONE NETWORKS.

8. Intentionally deleted.

9. LIMITATION OF LIABILITY. IN NO EVENT, WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING BREACH OF WARRANTY, NEGLIGENCE AND STRICT LIABILITY IN TORT), WILL EITHER PARTY BE HELD LIABLE UNDER THIS AGREEMENT FOR INDIRECT OR CONSEQUENTIAL, EXEMPLARY, PUNITIVE OR SPECIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, LOST PROFITS; LOSS OF USE OR LOSS OF DATA), EVEN IF SUCH PARTY IS AWARE OF OR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE AND EVEN IF DIRECT DAMAGES DO NOT SATISFY A REMEDY. IN NO EVENT WILL EITHER PARTY BE HELD LIABLE UNDER THIS AGREEMENT FOR MORE THAN THE AMOUNT PAID BY CUSTOMER TO SADA FOR THE SERVICES DURING THE 12 MONTHS PRIOR TO THE EVENT GIVING RISE TO LIABILITY. IN NO EVENT WILL GOOGLE BE HELD LIABLE FOR ANY DAMAGES, WHETHER DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL, ARISING FROM SADA’S DISTRIBUTION AND RESALE OF THE SERVICES. These limitations of liability do not apply to a party's indemnification obligations.

10. GENERAL PROVISIONS

10.1 Third Party Beneficiary. The parties agree that Google is a third party beneficiary of this Agreement. There are no other third party beneficiaries to this Agreement.

10.2 Waiver of Default. No delay or omission by either party to exercise any right or power under this Agreement will be construed to be a waiver thereof. A waiver by either party of any breach or covenant will not be construed to be a waiver of any succeeding breach thereof or of any other covenant.

10.3 Survival. The provisions of Section 3.6, Article 5, Article 6, Article 7, Article 8, Article 9 and this Article, as well as any other provision of this Agreement that contemplates performance or observance subsequent to termination or expiration of this Agreement will survive expiration or termination of this Agreement and continue in full force and effect for the period set forth therein, or if no period is set forth therein, indefinitely.

10.4 Force Majeure. Neither SADA nor Google shall be liable for inadequate performance to the extent caused by a circumstance beyond its reasonable control, including, without limitation, domain name server issues outside its direct control, labor strikes or shortages, riots, insurrection, fires, flood, storm, explosions, acts of God, war, terrorism, governmental action, labor conditions, earthquakes and material shortage.

10.5 Severability. If any provision of this Agreement is found to be illegal or otherwise unenforceable in any respect, that provision will be deemed to be restated to reflect as nearly as possible the original
intent of the parties in accordance with applicable law. The remainder of this Agreement will remain in full force and effect.

10.6 Entire Agreement; Amendment and Waiver. This Agreement and any exhibits referred to herein, each of which is incorporated herein for all purposes, is a part of Contract # UCP-TS-C02-12 executed by Client and SADA (the “Standard Contract”) and is not a standalone agreement. To the extent that anything contained in this Agreement conflicts or is inconsistent with the terms and conditions contained within Client’s RFP #0016512 included in the Standard Contract, the RFP terms shall take precedence. No change, waiver or discharge hereof will be valid unless made in writing and signed by an authorized representative of the party against which such change, waiver of discharge is sought to be enforced.

10.7 Counterparts. The parties may enter into this Agreement in counterparts which taken together will constitute one instrument.

IN WITNESS WHEREOF, this Agreement has been executed by the parties through their duly authorized officers as of the date set forth above.

SADA Systems, Inc.  CLIENT

_____________________________  _____________________________
Tony Safoian, President and CEO  John D. Krallman
Director of IT Business & Financial Affairs
EXHIBIT A

Under the terms of the Agreement of which this Exhibit is a party, SADA will provide the following Google products to Customer in the indicated quantity and at the indicated pricing:

<table>
<thead>
<tr>
<th>Item</th>
<th>Quantity</th>
<th>Price Per Item</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Apps Postini GMD 1-Year</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Apps Postini GMD 10-Year</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Message Encryption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Message Security only</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Apps End User Accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Initial Term of this Agreement will be ________ months.

Customer opts to pay for the Services:

- □ On a prepaid basis
- □ On a month-to-month or other periodic basis using SADA’s Cloud Subscription service

Customer understands that in order to qualify for periodic financing payments using SADA’s Cloud Subscription service, Customer must satisfy a credit check and enter into a loan and financing agreement with [FINANCING ENTITY]. If Customer does not qualify for such month-to-month payments, Customer must pay for the Services on a prepaid basis.

**Overage Charge**

Customer shall notify SADA in the event that Customer exceeds the number of mailboxes/units set forth above for any Postini, message encryption or message security product, such notice to be provided to SADA within 10 days of the occurrence of such overage. Upon becoming aware of any such overage (whether from Customer or otherwise), SADA will charge Customer an “Overage Charge” for each month during which an overage exists. Such Overage Charge will be equal to the product of (A) the number of excess mailboxes and (B) 1/12 of the annual charge per mailbox, which Overage Charge will be invoiced to Customer by SADA monthly in arrears.
Attachment E

Contract UCP-TS-C02-12

Agreements for Cooperative Use:

Master Professional Services Agreement, Maintenance and Support Agreement,
Google Apps Customer Agreement
This MASTER PROFESSIONAL SERVICES AGREEMENT ("Agreement"), is made and entered into as of [EFFECTIVE DATE] (the "Effective Date”), by and between SADA Systems Inc., a corporation organized under the laws of the state of California, with offices 5250 Lankershim Blvd., Suite 620, North Hollywood, CA 91601 ("SADA"), and ______________________, a state government agency and educational institute of the Commonwealth of Virginia with offices at ______________________ ("Client"). SADA and Client may be referred to in this Agreement individually as a “Party” and collectively as the “Parties.”

1. BACKGROUND, OBJECTIVES, CONSTRUCTION AND INTERPRETATION

1.1 Background and Objectives. This Agreement will serve as a framework under which SADA will provide certain information technology services (the “Services”), as described in Exhibit A (Statement of Work), attached hereto and incorporated herein, and as further requested by Client from time to time during the term of this Agreement and agreed upon in an executed Statement of Work (as defined in Section 2.2).

1.2 Definitions.  
(A) Capitalized terms used in this Agreement have the meaning assigned to them in the applicable Section. Terms, acronyms and phrases that are used in the information technology industry or other pertinent business context should be interpreted in accordance with their generally understood meaning in such industries or business context.

(B) The word “include” and its derivatives (such as “including” and “includes”) mean “include without limitation.”

1.3 References and Interpretation.  
(A) Headings, captions and titles used in this Agreement are included for convenience only and in no way define the scope or content of this Agreement or are to be used in the construction or interpretation of this Agreement. Any reference to a particular article or section number or exhibit is a reference to that specified article, section or exhibit of this Agreement, except to the extent that the cross-reference expressly refers to another document.

(B) If there is a conflict or inconsistency between the terms of this Agreement and any executed Statement of Work, the terms of this Agreement will prevail except to the extent that the executed Statement of Work specifically and expressly states an intent to supersede specific terms of this Agreement with applicability only to that executed Statement of Work. Notwithstanding the preceding sentence, no executed Statement of Work will be effective to: (1) expand, eliminate or restrict the scope of any indemnity obligation set forth in Article 10; (2) change any limitation of liability set forth in Article 11; or (3) settle or resolve any dispute between the Parties.

2. SCOPE OF SERVICES

2.1 Provision of Services. SADA will perform the Services identified in Exhibit A and those Services identified in additional Statements of Work entered into and executed by each of the Parties. Absent an executed Statement of Work, this Agreement does not, in and of itself, represent a commitment by either Party to provide any minimum amount of charges or services.

2.2 Statements of Work. From time to time during the term of this Agreement, Client may ask SADA to perform services that are not described in an executed Statement of Work or this Agreement.
Following any such request, SADA will prepare and deliver a Statement of Work substantially in the form of Exhibit A ("Statement of Work"). Each Statement of Work will contain:

(A) a description of the work SADA expects to perform in connection with such project, including a description of any deliverables;

(B) a prospective schedule for commencing and completing such work; and

(C) SADA’s prospective charges for such work.

If a proposed Statement of Work is mutually acceptable to the Parties, the Parties will execute such Statement of Work. Each executed Statement of Work will incorporate and be subject to all the terms and conditions of this Agreement, except for any provisions of this Agreement that are specifically excluded or modified in such executed Statement of Work (subject to Section 1.3(B)).

2.3 Modification of an Executed Statement of Work. Either Party may request modifications to an executed Statement of Work by submitting a written change order request to the other Party (each, a "Change Order"). If acceptable to both Parties, the Change Order will be executed by the Parties and will become part of the applicable executed Statement of Work. SADA will not be bound by the terms of any Change Order until it is executed by SADA.

2.4 Cooperation. Client understands that SADA’s performance is dependent on Client’s timely and effective cooperation, and that the quality of the Services are dependent on Client providing timely and accurate information to SADA and access to the required Client resources in accordance with the objectives of the applicable executed Statement of Work. Accordingly, any delay or nonperformance by SADA will be excused if and to the extent that such nonperformance results from Client’s failure to perform its responsibilities.

3. TERM, TERMINATION AND SUSPENSION OF SERVICES

3.1 Term. The term of this Agreement will begin on the Effective Date and will continue in effect until the later of the active time period of Contract UCP-TS-C02-12, and (B) the expiration or earlier termination of the last remaining executed Statement of Work, unless extended or terminated earlier in accordance with the terms of this Agreement. The Parties may agree to extend the term by written agreement to that effect.

3.2 Termination for Cause. If a Party commits: (A) a material breach of this Agreement that is capable of being cured within 30 days after notice of breach from the non-breaching Party, but is not cured within such period, or (B) a material breach of this Agreement that is not subject to cure with due diligence within 30 days of written notice thereof, then the non-breaching Party may, by giving written notice to the breaching Party, terminate this Agreement or the applicable Statement of Work, as of a date specified in the notice of termination.

3.3 Termination for Non-Payment. If undisputed invoices under this Agreement totaling at least two months’ charges are at any time outstanding and unpaid for 45 days, and Client fails to make such payment within 30 days of receiving written notice from SADA of its failure to make such payment, SADA may, by giving written notice to Client, terminate this Agreement and any executed Statement of Work as of the date specified in the notice of termination.

3.4 Termination for Convenience. Client reserves the right to terminate or cancel this Agreement or any executed Statement of Work as set forth in Section 3 of the terms and conditions contained within Client's RFP #0016512 included in the Standard Contract, the terms of which are incorporated in this Agreement.

3.5 Consequences of Termination. If this Agreement or any executed Statement of Work is terminated in accordance with the terms of this Article, SADA will be entitled to receive payment for all Services performed prior to termination in accordance with the terms of this Agreement or the applicable
executed Statement of Work. In addition, if SADA terminates any executed Statement of Work pursuant to Section 3.2 or Section 3.3, SADA will be entitled to reimbursement for any reasonable obligations SADA has entered into for the purpose of performing Services that cannot be cancelled. Termination of an executed Statement of Work will not affect any other executed Statements of Work then in effect. Termination of this Agreement will result in immediate termination of all executed Statements of Work then in effect.

4. Intentionally deleted.

5. PROPRIETARY RIGHTS

5.1 Client IP. As between Client and SADA, all right, title and interest in and to Client IP (as defined below) will remain the exclusive property of Client. To the extent necessary to provide the Services, Client hereby grants SADA, solely to provide the Services, a non-exclusive, non-transferable, fully paid-up and royalty-free, limited right to access and use the Client IP; provided that the rights granted to SADA hereunder will automatically expire effective upon the date that SADA ceases, for any reason, to provide the applicable Services. For purposes of this Agreement, “Client IP” will mean (A) software and tools, (B) processes, procedures and methodologies, (C) formulas, templates and formats, and (D) documents and other written materials, whether proprietary to Client or licensed to Client from third parties (other than SADA), that are provided to SADA by Client in order for SADA to provide the Services and fulfill its obligations under this Agreement.

5.2 SADA IP.

(A) As between SADA and Client, all right, title and interest in and to SADA IP (as defined below) will remain the exclusive property of SADA. Except to the extent that the Parties enter into separate license agreements with respect to any software products to be provided by SADA (in which case such software products will be governed by the terms of those license agreements), to the extent necessary to receive or use the Services or use any deliverable, SADA hereby grants to Client a perpetual, non-exclusive, worldwide, fully paid-up and royalty-free license to access and use (and to allow third parties to access and use solely for the benefit of Client) the SADA IP, for no additional consideration. Notwithstanding the foregoing, in the event that a Statement of Work provides for services and deliverables to be provided to Client on a trial or pilot basis, Client’s license to access and use any SADA IP necessary to receive or use the services or deliverables provided as part of such trial or pilot will not be perpetual, but will be limited to the period of such trial or pilot phase, as set forth in the applicable Statement of Work.

(B) Nothing in this Section will be construed to grant Client any right to separate SADA IP from the deliverable into which it is incorporated and Client will not (and will not knowingly allow any third party to) adapt, modify, translate, reverse engineer, decompile, disassemble or attempt to decode or disassemble any source code or underlying ideas or algorithms of any SADA IP or part thereof. Client will not sell, rent, lease, sublease, license, lend, market or commercially exploit such SADA IP or use SADA IP for the benefit of any affiliate, organization or other third party not contemplated by the applicable executed Statement of Work, or assign or transfer any rights with respect to SADA IP granted under this Agreement.

(C) For purposes of this Agreement, “SADA IP” will mean (A) software and tools, (B) processes, procedures and methodologies, (C) formulas, templates and formats, and (D) documents and other written materials, whether proprietary to SADA or licensed to SADA from third parties (other than Client or its affiliates) that are used to provide the Services, together, in each case, with any modifications or enhancements thereto and derivative works based thereon. Client acknowledges and agrees that with respect to any SADA IP licensed to SADA from third parties, any rights granted to Client hereunder or under any executed Statement of Work, will be subject to all restrictions set forth in the applicable third party agreements.

5.3 Developed Property and Works Made for Hire. Subject to Section 5.2, SADA acknowledges and agrees that Client will have all right, title and interest in and to all Developed Property (as defined
below) developed in the course of providing the Services. All Developed Property developed under this Agreement in accordance with the terms of an executed Statement of Work will be deemed to be “works made for hire.” To the extent any Developed Property is not deemed “works made for hire” by operation of law, SADA hereby irrevocably assigns, transfers and conveys to Client, without further consideration, all of its right, title and interest in and to such Developed Property (including all patent, copyright, trademark, trade secret and other intellectual property and proprietary rights). SADA will execute any documents or take any other actions as may be reasonably necessary, or as Client may reasonably request, to perfect the ownership rights defined in this Section. For purposes of this Agreement, “Developed Property” will mean intellectual property generated or developed specifically for Client by SADA under an executed Statement of Work and paid for by Client. To qualify as Developed Property under this Agreement, such intellectual property must be explicitly and specifically called out in an executed Statement of Work and such executed Statement of Work must include a written acknowledgement by SADA that the Parties intend to transfer the rights to such intellectual property to Client upon payment by Client.

5.4 Residual Knowledge. Nothing in this Agreement will restrict a Party from using Services-related ideas, concepts, know-how, methodologies, processes, technologies, algorithms or techniques that are general in nature and retained in the unaided mental impressions of the Party’s personnel, which either Party, individually or jointly, develops or discloses under this Agreement; provided that, in doing so, each Party does not breach its obligations under Article 7 or infringe the intellectual property rights of the other Party or third parties who have licensed or provided materials to the other Party. Except for the license rights set forth in this Article, neither this Agreement nor any executed Statement of Work grants any license to either Party under any patents or copyrights of the other Party. The Parties acknowledge that SADA has the right to: (A) provide consulting or other services of any kind or nature to any person or entity as SADA, in its sole discretion, deems appropriate, and (B) use any works of authorship or other intellectual property included in the deliverables (other than Developed Property, if any) to develop for itself, or for others, materials or processes similar to those contemplated or produced under this Agreement.

6. CHARGES AND INVOICES

6.1 General. Subject to the provisions of this Agreement, Client will pay SADA the amounts set forth in each executed Statement of Work (including any Change Orders thereto).

6.2 Reimbursement of Expenses. Client agrees to reimburse SADA for costs and expenses incurred in connection with SADA’s performance of the Services, including reasonable travel expenses, provided Client has approved such expenses in advance. SADA will provide Client with receipts or other documentation substantiating all reimbursable costs and expenses.

6.3 Invoices and Payment. SADA will invoice Client for all amounts due under an executed Statement of Work in accordance with the schedule set forth in such executed Statement of Work. Each invoice submitted to Client pursuant to this Agreement will be due and payable by Client within 30 days of receipt.

6.4 Disputed Fees and Late Payments. Client agrees to notify SADA within 15 days of its receipt of an invoice from SADA, if Client disputes any amount or item in such invoice in good faith. Notwithstanding any dispute, Client will pay the undisputed portion of an invoice when due and payable. If Client withhold any amount associated with disputed amounts pursuant to this Section, Client will provide SADA with a description of the basis for such withholding. Upon resolution of a dispute involving any withheld amounts, Client will pay SADA such portion, if any, of the disputed amount agreed or determined to be owing to SADA within 30 days after resolution of the dispute.

7. CONFIDENTIALITY

7.1 Disclosure of Confidential Information. The Parties agree that in the course of SADA’s performance of the Services, each Party may access, receive or exchange information that is confidential in nature. For purposes of this agreement “Confidential Information” will include all information, in any
form, furnished or made available, directly or indirectly, by one Party ("Disclosing Party") to the other Party ("Recipient") that is marked confidential, restricted, or is otherwise designated as confidential. Confidential Information will also include information that, by virtue of the nature of the information or the circumstances surrounding disclosure, a reasonable party would understand to be proprietary to Disclosing Party or confidential, including without limitation: (A) any personally identifiable information or financial information of any individual; (B) information concerning the operations, affairs and business of a Party, a Party’s financial affairs, or a Party’s relations with its customers and employees; (C) in the case of Client, Client IP; and (D) in the case of SADA, SADA IP.

7.2 Exclusions. Confidential Information does not include, and this Article does not apply to, information that (A) is or subsequently becomes published or available to the public through no fault of Recipient, (B) is received by Recipient from a third party without a duty of confidentiality; (C) is independently developed by Recipient without reference to Disclosing Party’s Confidential Information, or (D) was in Recipient’s possession or was known to Recipient before it was disclosed to Recipient by Disclosing Party.

7.3 Restrictions on Disclosure and Use. The Parties agree:

(A) Neither Party will make any use of the other Party’s Confidential Information or any copies thereof, for any purpose other than those contemplated by this Agreement.

(B) Neither Party will reveal, disclose or provide access to the other Party’s Confidential Information to any third party without the prior consent of such Party, provided that both Parties may share Confidential Information with their responsible employees who have a need to know such Confidential Information to perform their duties. Client understands that all materials provided to Client by SADA are provided solely for Client’s internal use. Notwithstanding anything to the contrary in this paragraph, SADA may disclose Confidential Information to properly authorized entities as and to the extent necessary for performance of the Services, so long as in each such case, the receiving entity first agrees to the obligations described in this Article.

(C) Recipient will take security precautions at least as great as the precautions Recipient takes to protect its own confidential information, and at any rate will take commercially reasonable security precautions to ensure that no one, other than a person authorized pursuant to this Section, gains access to Disclosing Party’s Confidential Information without Disclosing Party’s prior written consent. In the event that Recipient becomes aware of any unauthorized use or disclosure of Disclosing Party’s Confidential Information, Recipient will immediately give notice to Disclosing Party and will assist Disclosing Party in remedying such unauthorized use or disclosure.

(D) Recipient is permitted to disclose Confidential Information as required by law, regulation or subpoena, provided that Recipient will (i) give Disclosing Party prompt notice of any such requirement, which notice must be sufficient to permit Disclosing Party to seek relief to prevent such disclosure, (ii) cooperate with Disclosing Party to secure confidential treatment of the Confidential Information, and (iii) disclose only that portion of Disclosing Party’s Confidential Information that is legally required.

(E) Confidential Information is and will remain the exclusive property of Disclosing Party. Each Party agrees that it will have no proprietary interest in the other Party’s Confidential Information and that nothing contained in this Agreement will be construed to grant either Party any rights, by license or otherwise, to any of the other Party’s Confidential Information disclosed pursuant to this Agreement.

(F) The obligations set forth in this Section will apply to Confidential Information provided, furnished or otherwise disclosed by Disclosing Party to Recipient, whether prior to or following the Effective Date.

7.4 Controlling Provisions. For purposes of this Agreement, each executed Statement of Work, and the Services contemplated by this Agreement and such executed Statements of Work, the provisions
of this Article will have precedence over and supersede any confidentiality or non-disclosure agreement executed by the Parties prior to the Effective Date.

8. REPRESENTATIONS, WARRANTIES AND COVENANTS

8.1 Authorization. Each Party represents and warrants to the other that: (A) it has the requisite corporate power and authority to enter into this Agreement and to carry out the transactions contemplated by this Agreement; and (B) the execution, delivery and performance of this Agreement and the consummation of the transactions contemplated by this Agreement have been duly authorized by the requisite corporate action on the part of such Party.

8.2 Performance of Services. SADA represents, warrants and covenants to Client that the Services will be performed by qualified personnel with promptness and diligence in a workmanlike manner, consistent with applicable industry standards.

8.3 Viruses and Disabling Code. SADA will use commercially reasonable efforts to prevent the coding or introduction of viruses, disabling code or similar items into the Client systems by SADA or its agents; and SADA will, in the event a virus, disabling code or similar item is found to have been introduced into the software Deliverables or Client systems by SADA or its agents, at no additional charge, assist Client in reducing the effects of the virus, disabling code or similar item.

8.4 Disclaimer. OTHER THAN AS PROVIDED IN THIS AGREEMENT, NEITHER PARTY PROVIDES ANY EXPRESS WARRANTIES OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN ADDITION, SADA MAKES NO EXPRESS OR IMPLIED WARRANTIES RELATING TO THIRD PARTY PRODUCTS OR SERVICES.

8.5 Limited Warranty. In the event that any implied warranties, guarantees or conditions implied by local law cannot be waived, then any such implied warranties are limited in duration to 90 days from delivery of the applicable Service or deliverable.

9. Intentionally deleted.

10. INDEMNIFICATION

10.1 By SADA. SADA agrees to indemnify, defend, and hold Client harmless from and against all losses, liabilities, damages, and related costs (including settlement costs and reasonable attorneys' fees) (collectively, “Losses”) arising out of a third party claim that the Services, SADA IP or any deliverables infringe or misappropriate any patent, copyright, trade secret or trademark of a third party. Notwithstanding the foregoing, in no event will SADA have any obligations or liability under this Section arising from: (A) use of any Service or deliverable in a modified form or in combination with materials not furnished or approved by SADA, (B) use by Client or its agents of such item in a manner not reasonably consistent with the applicable specifications, requirements or instructions for such item, and (C) any content, information or data provided by Client or other third parties.

10.2 Infringement. If the Services or any deliverable or item used by SADA to provide the Services or any deliverable becomes, or in SADA's reasonable opinion is likely to become, the subject of an infringement or misappropriation claim or proceeding, SADA will, at its expense: (A) secure the right to continue using the Services, deliverable or item; (B) replace or modify the Services, deliverable or item to make it non-infringing, provided that any such replacement or modification will not degrade the performance or quality of the affected component of the Services or deliverable; or (C) if SADA cannot accomplish either of the foregoing using commercially reasonable efforts, and only in such event, SADA will discontinue providing the Services or remove the deliverable or item and the charges will be equitably adjusted to reflect such removal.

10.3 General. Client will promptly notify SADA of any claim for which it is seeking indemnification and will cooperate with SADA in defending the claim. SADA will have full control and authority over the
defense, provided that: (A) any settlement requiring Client to admit liability or pay any money will require Client’s prior written consent, such consent not to be unreasonable withheld or delayed; and (B) Client may join in the defense of a claim with its own counsel at its own expense.

11. LIABILITY

11.1 Limitation of Liability.

(A) IN NO EVENT WILL EITHER PARTY BE HELD LIABLE UNDER THIS AGREEMENT FOR SPECIAL, INDIRECT, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF DATA, BUSINESS INTERRUPTION OR LOST PROFITS), WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE, OR OTHERWISE, EVEN IF SUCH PARTY IS AWARE OF OR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE AND EVEN IF DIRECT DAMAGES DO NOT SATISFY A REMEDY.

(B) EXCEPT AS PROVIDED IN SECTION 11.2, NEITHER PARTY MAY BE HELD LIABLE UNDER THIS AGREEMENT FOR MORE THAN THE AGGREGATE AMOUNT ACTUALLY PAID TO SADA BY CLIENT UNDER THE APPLICABLE STATEMENT(S) OF WORK GIVING RISE TO SUCH LOSS.

11.2 Exceptions to Limitation of Liability. The limitations set forth in Section 11.1(B) will not apply to: (A) damages occasioned by a Party's breach of its obligations with respect to the other Party's intellectual property rights, (B) Losses that are the subject of indemnification obligations under this Agreement, or (C) Losses determined to be the direct result of a Party's gross negligence or intentional or willful misconduct.

12. FORCE MAJEURE

No Party will be liable for any default or delay in the performance of its obligations under this Agreement if and to the extent such default or delay is caused, directly or indirectly, by fire, flood, earthquake, elements of nature or acts of God, riots, civil disorders, acts of terrorism, or any other similar cause beyond the reasonable control of such Party (each such event, a “Force Majeure Event”). Any Party so delayed in its performance will promptly notify the Party to whom performance is due by telephone (to be confirmed in writing within two days of the inception of such delay) and describe at a reasonable level of detail the circumstances causing such delay.

13. Intentionally deleted.

14. GENERAL PROVISIONS

14.1 Relationship of the Parties. SADA, in furnishing the Services, is acting as an independent contractor. SADA is not an agent of Client and has no authority to represent Client as to any matters, except as expressly authorized in this Agreement.

14.2 Waiver of Default. No delay or omission by either Party to exercise any right or power under this Agreement will be construed to be a waiver thereof. A waiver by either Party of any breach or covenant will not be construed to be a waiver of any succeeding breach thereof or of any other covenant.

14.3 Third Party Beneficiaries and Use of Work. Neither Party intends this Agreement to benefit, or create any right or cause of action in or on behalf of, any person or entity other than the Parties. Client understands and agrees that Services performed by SADA under this Agreement are intended only for the parties specified in the applicable executed Statement of Work and may be misleading if used in another context or for another party and agrees not to use any deliverables or documents produced under this Agreement for any purpose other than the intended purpose without SADA’s prior written consent.
14.4 **Survival.** The provisions of Section 4, Article 5, Section 6.4, Article 7, Section 8.4, Article 10, Article 11, Article 13 and this Article, as well as any other provision of this Agreement that contemplates performance or observance subsequent to termination or expiration of this Agreement will survive expiration or termination of this Agreement and continue in full force and effect for the period set forth therein, or if no period is set forth therein, indefinitely.

14.5 **Severability.** If any provision of this Agreement is found to be illegal or otherwise unenforceable in any respect, that provision will be deemed to be restated to reflect as nearly as possible the original intent of the Parties in accordance with applicable law. The remainder of this Agreement will remain in full force and effect.

14.6 **Entire Agreement; Amendment and Waiver.** This Agreement and each of the executed Statements of Work hereto, including any exhibits referred to herein or therein, each of which is incorporated herein for all purposes, is a part of Contract UCP-TS-C02-12 executed by Client and SADA (the "Standard Contract") and is not a standalone agreement. To the extent that anything contained in this Agreement conflicts or is inconsistent with the terms and conditions contained within Client's RFP #0016512 included in the Standard Contract, the RFP terms shall take precedence. No change, waiver or discharge hereof will be valid unless made in writing and signed by an authorized representative of the Party against which such change, waiver of discharge is sought to be enforced. Notwithstanding the foregoing, the parties agree that the requirements set forth in Section 23.C of the Special Terms and Conditions to the Standard Contract will not apply to SADA.

14.7 **Counterparts.** This Agreement may be executed in any number of counterparts, all of which taken together will constitute one single agreement between the Parties.

**IN WITNESS WHEREOF,** this Agreement has been executed by the Parties through their duly authorized officers as of the date set forth above.

SADA Systems, Inc. Virginia Polytechnic Institute and State University

_____________________________  _____________________________
Tony Safoian, President and CEO  Print name:

Print title:
This Statement of Work is entered into in connection with the Master Professional Services Agreement ("Agreement") by and between SADA Systems Inc. ("SADA") and Virginia Polytechnic Institute and State University ("Client") dated [DATE OF AGREEMENT]. The terms and conditions of the Agreement are incorporated herein by reference. Capitalized terms not defined in this Statement of Work will have the same meaning given to them in the Agreement. This Statement of Work describes certain Services and deliverables that will be provided by SADA to Client pursuant to the terms and conditions of the Agreement.

GENERAL INFORMATION

<table>
<thead>
<tr>
<th>Project Title:</th>
<th>Effective Date:</th>
<th>Term of SOW:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Recipients:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

SADA INFORMATION

<table>
<thead>
<tr>
<th>Project Manager:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SADA Personnel:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SADA sites:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include address of each Client site from which Services will be provided.</td>
</tr>
</tbody>
</table>

PROJECT TRACKING AND OVERSIGHT

<table>
<thead>
<tr>
<th>Reports:</th>
</tr>
</thead>
<tbody>
<tr>
<td>include reporting requirements and the frequency of delivery of the reports.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Meetings:</th>
</tr>
</thead>
<tbody>
<tr>
<td>include a general description of the purpose for such meetings and the Client and SADA personnel required to attend</td>
</tr>
</tbody>
</table>

SERVICES

Scope of Project: Services.

Description of Services

CLIENT RESPONSIBILITIES

[This Section should describe Client's obligations under this Statement of Work.]

Client Facilities.

Client will provide the following facilities or access to the following facilities to SADA in accordance with the terms of the Agreement:
[Enter details concerning the work space, computer equipment, and access provided by Client to SADA personnel performing Services under this Statement of Work.]

PRICING

The following charges apply to the Services to be performed under this Statement of Work.
This MAINTENANCE AND SUPPORT AGREEMENT ("Agreement"), is made and entered into as of [EFFECTIVE DATE] (the "Effective Date"), and sets forth the terms and conditions governing the maintenance and support services to be provided by SADA Systems Inc., a corporation organized under the laws of California ("SADA") to _________________________, a state government agency and educational institute of the Commonwealth of Virginia ("Client") with respect to the SADA software products identified in the table below (together, "Software"), which Software is being provided to Client under the Statement of Work to the Master Professional Services Agreement between the parties, each dated the effective date of the signed Statement of Work (SOW).

<table>
<thead>
<tr>
<th>SADA Software Product(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-Premise Sync for Google Apps</td>
</tr>
<tr>
<td>Hosted Sync for Google Apps</td>
</tr>
<tr>
<td>AuthMagic for Google Apps (Password Sync)</td>
</tr>
<tr>
<td>On-premise Single Sign On for Google Apps</td>
</tr>
<tr>
<td>Hosted Single Sign On for Google Apps</td>
</tr>
</tbody>
</table>

1. TERM AND RENEWAL

1.1 Term. The term of this Agreement will begin on the date set forth in the preamble, subject to provision of payment, and will continue in effect for the period of time Contract UCP-TS-C02-12 is active (the "Initial Term"). The Agreement expires at the end of the term unless renewed.

1.2 Renewal. Within 60 days of expiration of the Initial Term or any renewal term, SADA will provide notification to Client with instructions for renewal. SADA may modify the fees for any renewal term upon written notice to Client at least 30 days prior to expiration of the then-current term.

1.3 Termination for Non-Payment. If undisputed invoices under this Agreement are at any time outstanding and unpaid for 45 days, and Client fails to make such payment within 30 days of receiving a written reminder notice from SADA of its failure to make such payment in a timely manner, SADA may, by giving written notice to Client, terminate this Agreement as of the date specified in the notice of termination.

2. MAINTENANCE AND SUPPORT SERVICES

2.1 Support Services. For so long as this Agreement is in effect, SADA will provide basic maintenance and support services (the "Support Services") consisting of:

(A) Error Correction and Resolution. SADA will be responsible for using all reasonable diligence to correct verifiable and reproducible failures of the Software to conform in any material respect to its published specifications ("Errors") when reported in accordance with SADA’s standard reporting procedures, as set forth in Exhibit A. An "Error Correction" means either a modification or addition that, when made or added to the Software, brings the Software into material conformity with its published specifications, or a mutually agreed upon procedure or routine that, when observed in the regular operation of the Software, avoids the practical adverse effect of such nonconformity. An Error Correction, when completed, may be provided in the form of a "temporary fix," consisting of sufficient programming and operating instructions to implement the Error Correction. Such temporary fixes shall be permanently resolved no later than the next release.
(B) **Staff.** SADA will maintain a trained staff capable of rendering the services set forth in this Agreement.

2.2 **Cooperation of the Customer.** Client agrees to notify SADA promptly following the discovery of any Error. Further, upon discovery of an Error, Client agrees, if requested by SADA, to submit to SADA a listing of output and any other reasonable and necessary data that SADA may require in order to reproduce the Error and the operating conditions under which the Error occurred or was discovered. In addition, Client is responsible for procuring, installing, and maintaining all equipment, telephone lines, communication interfaces, and other hardware necessary to operate the Software. SADA will not be responsible for delays caused by events or circumstances beyond its reasonable control.

Client acknowledges and agrees that SADA’s provision of Support Services is subject to the following:

- **(A)** Client will provide SADA with necessary access to personnel and equipment;
- **(B)** Client will provide supervision, control and management of the use of the Software. In addition, Client will implement procedures for the protection of information and the implementation of backup facilities in the event of errors or malfunction of the Software or equipment;
- **(C)** Client will document and promptly report detected errors or malfunctions of the Software to SADA and take commercially reasonable steps necessary to carry out procedures for the rectification of errors or malfunctions within a reasonable time after such procedures have been received from SADA;
- **(D)** Client is responsible for backup of all programs and data;
- **(E)** Client will properly train its personnel in the use and application of the Software; and
- **(F)** Client will retain responsibility for all change management, risk management and governance controls that Client deems appropriate or are required by Client’s internal policies and practices.

2.3 **Exceptions.** This Agreement does not include services requested as a result of, or with respect to, causes which are not attributable to SADA. Causes which are not attributable to SADA include, but are not limited to, the matters, which are not covered by the Support Services:

- **(A)** Any problem resulting from the misuse, improper use, alteration or damage of the Software;
- **(B)** Any problem caused by modifications in any version of the Software not made or authorized by SADA;
- **(C)** Any problem resulting from programming other than the Software or equipment; or
- **(D)** Any problem resulting from the combination of the Software with such other programming or equipment to the extent such combination has not been approved by SADA.

If Client requires support for any of the foregoing exceptions, Client will be responsible to pay SADA's normal charges and expenses for time or other resources provided by SADA to diagnose or attempt to correct any such problem.

3. **MAINTENANCE AND SUPPORT FEES**

In consideration of the Support Services detailed in an executed SOW, if any, and subject to the terms and conditions of this Agreement, Client agrees to pay SADA a fee based on Contract UCP-TS-C02-12.

4. **INCIDENT REPORTING, CATEGORIZATION, RESPONSE TIMES AND ESCALATION**
SADA will manage Error Correction and Resolution in terms of incident reporting, categorization, response time and escalation as set forth in the service level agreement attached as Exhibit A. SADA may change its policies with respect to the matters set forth in Exhibit A from time to time, provided that SADA will provide Client with at least 30 days advance written notice of any material changes to such policies. If the proposed change has a material adverse effect on Client and Client does not agree to the change, Client will notify SADA prior to the implementation of a planned change. If Client notifies SADA as required, then Client will remain governed by the terms in effect immediately prior to the change (or any other arrangement agreed by the parties) until the end of the then-current term. If this Agreement is renewed, it will be renewed under SADA’s then current policies. SADA will undertake to implement any proposed changes to the matters set forth in Exhibit A in such a manner as to minimize an adverse impact to the level of service provided under the terms of this Agreement.

5. LIMITED WARRANTY AND DISCLAIMER

5.1 SADA will perform its services under this Agreement in a professional and workmanlike manner.

5.2 OTHER THAN AS EXPRESSLY PROVIDED IN THIS AGREEMENT, SADA DOES NOT PROVIDE ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR OTHERWISE. EXCEPT AS SET FORTH IN SECTION 5.1, WITH RESPECT TO ANY SOFTWARE TO BE PROVIDED UNDER THIS AGREEMENT, THE SOFTWARE IS BEING DELIVERED TO CLIENT AS-IS AND SADA MAKES NO WARRANTY AS TO ITS USE OR PERFORMANCE. SADA DOES NOT WARRANT THAT THE SOFTWARE WILL MEET CLIENT’S REQUIREMENTS; THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. SADA CANNOT WARRANT THE PERFORMANCE OR RESULTS CLIENT MAY OBTAIN BY USING THE SOFTWARE. IN ADDITION, SADA MAKES NO EXPRESS OR IMPLIED WARRANTIES RELATING TO ANY THIRD PARTY PRODUCTS OR SERVICES.

6. LIMITATION OF LIABILITY

6.1 IN NO EVENT, WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING BREACH OF WARRANTY, NEGLIGENCE, AND STRICT LIABILITY IN TORT), WILL SADA BE HELD LIABLE UNDER THIS AGREEMENT FOR LOSS OF DATA OR DATA STORAGE, SYSTEMS OR BUSINESS INTERRUPTION, COMPUTER FAILURE OR MALFUNCTION, OR FOR INDIRECT OR CONSEQUENTIAL (INCLUDING LOST PROFITS), EXEMPLARY, PUNITIVE OR SPECIAL DAMAGES ARISING IN ANY WAY OUT OF THIS AGREEMENT, EVEN IF SUCH PARTY IS AWARE OF OR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE, OR FOR ANY CLAIM BY ANY THIRD PARTY; PROVIDED, HOWEVER, THAT THIS LIMITATION DOES NOT APPLY WITH RESPECT TO DAMAGES DETERMINED TO BE THE DIRECT RESULT OF SADA’S GROSS NEGLIGENCE OR INTENTIONAL OR WILLFUL MISCONDUCT.

6.2 ANY DAMAGES THAT SADA IS REQUIRED TO PAY FOR ANY PURPOSE WHATSOEVER UNDER THIS AGREEMENT WILL BE LIMITED TO THE AGGREGATE FEE PAID UNDER THIS AGREEMENT.

7. MISCELLANEOUS

7.1 Waiver. No delay or omission by either party to exercise any right or power under this Agreement will be construed to be a waiver thereof. A waiver by either party of any breach or covenant will not be construed to be a waiver of any succeeding breach thereof or of any other covenant.

7.2 Severability. If any provision of this Agreement is found to be illegal or otherwise unenforceable in any respect, that provision will be deemed to be restated to reflect as nearly as possible the original intent of the parties in accordance with applicable law. The remainder of this Agreement will remain in full force and effect.
7.3 **Survival.** Sections 5 (Limited Warranty and Disclaimer), 6 (Limitation of Liability), and 7 (Miscellaneous) will survive any expiration or termination of this Agreement and continue in full force and effect.

7.4 **Force Majeure.** No Party will be liable for any default or delay in the performance of its obligations under this Agreement if and to the extent such default or delay is caused, directly or indirectly, by fire, flood, earthquake, elements of nature or acts of God, riots, civil disorders, acts of terrorism, or any other similar cause beyond the reasonable control of such Party (each such event, a "Force Majeure Event"). Any Party so delayed in its performance will promptly notify the Party to whom performance is due by telephone (to be confirmed in writing within two days of the inception of such delay) and describe at a reasonable level of detail the circumstances causing such delay.

7.5 **Entire Agreement; Amendment and Waiver.** This Agreement and its Exhibit A is a part of Contract #UCP-TS-C02-12 executed by Client and SADA (the "Standard Contract") and is not a standalone agreement. To the extent that anything contained in this Agreement conflicts or is inconsistent with the terms and conditions contained within Client's RFP #0016512 included in the Standard Contract, the RFP terms shall take precedence. No change, waiver or discharge hereof will be valid unless made in writing and signed by an authorized representative of the party against which such change, waiver of discharge is sought to be enforced.

IN WITNESS WHEREOF, this Agreement has been executed by the parties through their duly authorized officers as of the date set forth above.

SADA Systems, Inc. 
_____________________________  By:  ________________________________

Tony Safoian, President and CEO  Name:

Title:

CLIENT
Exhibit A: Service Level Agreement

Introduction

This exhibit sets forth the method by which SADA Systems, Inc. (SADA) determines incident prioritization, manages response times and escalates support requests in connection with the services it provides.

Priority Definition & Establishment

When a client notifies SADA of an incident, SADA will prioritize the incident in accordance with the following definitions, which are based on business impact. Incident prioritization is at the sole discretion of SADA. Any incidents which have been set above their allotted Priority will be dropped to the appropriate Priority by an authorized member at SADA, which will also reset the response time for the incident.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Definition</th>
<th>Example</th>
</tr>
</thead>
</table>
| Level 1  | • Defect causing the software product to be unusable or inoperable  
           • Major function is unavailable with no acceptable bypass/workaround  
           • Response time not being met | • Server crash/failure  
           • Network failure |
| Level 2  | • Major function is unavailable but acceptable bypass/workaround is available | • Important file unavailable  
           • Application fault |
| Level 3  | • Defect causing a minor function to be disabled.  
           • Some function is not working correctly  
           • Minimal impact on the user community | • Important meeting  
           • File unavailable  
           • Printer problem |
| Level 4  | • Defect is not time-critical  
           • Single user impact  
           • Defect causing no function to be disabled  
           • Does not impact user community | • How do I…?  
           • How much would …cost?  
           • Non critical info requests |

Response & Resolution Timeframes

SADA’s incident management process includes triage, documentation and prioritization, and is designed to deliver the following elements:

- A clear agreement between SADA and the client as to what the incident is about
- An owner for the problem both at SADA and your company.
- A clear summary from SADA as to what the next steps are.
- An expected time frame to temporary and/or permanent resolution of the problem.

In furnishing you with this information SADA satisfies the ‘Response’ as constituted by this service level agreement. The response times set out by this service level agreement begin only after an incident has been reported, captured, triaged and prioritized. Target response times are as follows:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Max. Response Time</th>
<th>Workaround Resolution Time</th>
<th>Status Updates</th>
<th>Permanent Resolution Times</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>60 minutes</td>
<td>4 clock hours</td>
<td>2 Hours</td>
<td>2 days</td>
</tr>
<tr>
<td>Level 2</td>
<td>90 minutes</td>
<td>8 clock hours</td>
<td>6 hours</td>
<td>4 days</td>
</tr>
<tr>
<td>Level 3</td>
<td>4 Hours</td>
<td>2 business days</td>
<td>1 business day</td>
<td>15 days</td>
</tr>
<tr>
<td>Level 4</td>
<td>8 Hours</td>
<td>7 business days</td>
<td>1 business day</td>
<td>30 days</td>
</tr>
</tbody>
</table>
Response times applied to support incidents that are reported outside SADA’s normal business hours (Monday through Friday, 9:00am – 6:00pm pacific time, excluding national holidays) must be initiated by way of SADA’s emergency telephone system. Incidents reported by email and/or the Client Portal outside SADA’s regular business hours will be responded to on the start of the next business day (at which time the response time for the incident will begin), under the guidelines provided above.

Escalation & Remediation

An incident can be anything that degrades or interrupts the client’s information technology supported business processes, activities and workflows. The following process describes the means in which SADA will handle all incidents.

1. Support request is received
2. Service request is created
3. Issue is identified, documented, triaged, prioritized and assigned within the incident management system.
4. Issue is qualified to determine if it can be resolved through Tier 1 Support

**If issue can be resolved through Tier 1 Support:**
5. Level 1 Resolution - issue is worked to successful resolution.
6. Quality Control - Issue resolution is verified with client
7. Service request is closed, after complete resolution details have been updated in the incident management system.

**If issue cannot be resolved through Tier 1 Support:**
6. Issue is escalated to Tier 2 Support
7. Issue is qualified to determine if it can be resolved by Tier 2 Support

**If issue can be resolved through Tier 2 Support:**
8. Level 2 Resolution - issue is worked to successful resolution
9. Quality Control – Issue resolution is verified with client
10. Service request is closed, after complete resolution details have been updated in the incident management system.

**If issue cannot be resolved through Tier 2 Support:**
9. Issue is escalated to Tier 3 Support
10. Issue is qualified to determine if it can be resolved through Tier 3

**If issue can be resolved through Tier 3 Support:**
11. Level 3 Resolution - issue is worked to successful resolution
12. Quality Control – Issue resolution is verified with client.
13. Service request is closed, after complete resolution details have been updated in the incident management system.

**If issue cannot be resolved through Tier 3 Support:**
12. Issue is escalated to onsite support (dispatch)
13. Issue is qualified to determine if it can be resolved through onsite support

**If issue can be resolved through Onsite Support:**
14. Onsite resolution - issue is worked to successful Resolution.
15. Quality Control – Issue resolution is verified with client
16. Service request is closed, after complete resolution details have been updated in the incident management system.

**If issue cannot be resolved through Onsite Support:**
17. Management Decision Point – request is updated with complete details of all activity performed. Next actionable step based on facts at hand and available resources.
18. Possible outcomes may include:
   i. Re-entry into the Incident Management process
   ii. Escalation/entry into the Problem Management process
   iii. Service Credits (as defined below)
vi. Client negotiation or compromise

Support Tiers

SADA has established the following Tiered support model for IT Service Desk (Helpdesk) operations. The SADA Helpdesk (including the emergency telephone system for incidents reported outside SADA’s normal business hours) is the single point of contact (SPOC) for all issues reported, which are then identified, documented, prioritized and assigned to internal resources for troubleshooting and resolution prior to the performance of any quality assurance activities and final closure. This service level agreement is only in effect when incident requests are reported through the Helpdesk support system, via phone, email or the Client Portal.

SADA has developed this support Tier structure as the foundation of an incident management process/escalation path. The Tiered structure supports a scalable approach to incident management and problem management. It is important to understand that incidents can be escalated between and among these Tiers during maintenance, incident and problem management resolution. Furthermore, specific individuals can, at times, conduct all incident and problem management activities through several levels of escalation.

<table>
<thead>
<tr>
<th>Support Tier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1 Support</td>
<td>All support incidents begin in Tier 1, where the initial ticket is created, the issue is identified and clearly documented, and a basic hardware/software troubleshooting is initiated.</td>
</tr>
<tr>
<td>Tier 2 Support</td>
<td>All support incidents that cannot be resolved with Tier 1 Support are escalated to Tier 2, where more complex support on hardware/software issues can be provided by more experienced engineers.</td>
</tr>
<tr>
<td>Tier 3 Support</td>
<td>Support incidents that cannot be resolved by Tier 2 Support are escalated to Tier 3, where support is provided by the most qualified and experienced engineers who have the ability to resolve the most complex issues, and/or can collaborate with 3rd party (vendor) support engineers.</td>
</tr>
</tbody>
</table>

Service Downtime and Service Credits

For purposes of this service level agreement, “Service Downtime” is any unplanned interruption in service availability during which the Client is unable to access the services or software, provided the interruption is determined (and confirmed by SADA) to have been caused by a problem within the service or software provided by SADA. Service Downtime will be measured as the total length of time of the unplanned interruption in service availability during a calendar month. Scheduled downtime will not count toward Service Downtime and SADA will have no responsibility for any unplanned outages arising from third-party hardware or software failures. **Response and Resolution Time Credit Schedule:**

For any breach of SADA’s obligations under “Response and Resolution Time Frames” above, the following credits will apply:

<table>
<thead>
<tr>
<th>Type of Breach</th>
<th>Number of times</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Time Breach</td>
<td>1-2 times in any calendar month</td>
<td>10 day extension to current term of Maintenance and Support Agreement</td>
</tr>
<tr>
<td>Response Time Breach</td>
<td>3-4 times in any calendar month</td>
<td>20 day extension to current term of Maintenance and Support Agreement</td>
</tr>
<tr>
<td>Response Time Breach</td>
<td>5 or more times in any calendar month</td>
<td>30 day extension to current term of Maintenance and Support Agreement</td>
</tr>
<tr>
<td>Consecutive Response Time Breaches</td>
<td>1 or more Response Time breaches in each month of any consecutive 3- month period</td>
<td>30 day ADDITIONAL extension to current term of Maintenance and Support Agreement</td>
</tr>
<tr>
<td>Any Resolution Time Breach</td>
<td>N/A</td>
<td>30 day extension to current term of Maintenance and Support Agreement</td>
</tr>
</tbody>
</table>
Claiming Service Credits; Maximum Service Credits:

In order to receive any Service Credit described above, a client must notify SADA in writing that it is electing to claim such Service Credit within 30 days of the time client becomes eligible to receive a Service Credit. In the case of Service Credits tied to a Response Time breach, such notice will be timely if given within 30 days following the close of the calendar month in which such breach occurred. Any such notice should be sent to servicecredits@sadasystems.com along with incident details including the date and time of the first report to SADA, the ticket # assigned by SADA, and the reason for the credit request. Failure to comply with this requirement in a timely manner will forfeit Customer’s right to receive a Service Credit for a period as to which the notice requirement has expired. In no event will the aggregate number of Service Credits extended by SADA to a client for breaches occurring in a single calendar month exceed two months or 60 days (whichever is less) extension to the current term of the Maintenance and Support Agreement. Service Credits may not be exchanged for, or converted to, monetary amounts.

Credit Calculation Examples:

**Response Time Breach:**
- Response Time breach on Jan 1st and Jan 15th,
  Breach Count = 2, Extension Credit = 10 days (2x in one calendar month)
- Response Time breach on Jan 31st and Feb 1st,
  Breach Count = 2, Extension Credit = 20 days (1x in each of two calendar months)
- Response Time breach on June 30th, July 30th and August 30th
  Breach Count = 3, Extension Credit = 60 days (1x in June; 1x in July and 1x August + 30 days for repeated breaches over consecutive 3-month period)

**Resolution Time Breach:**
- Resolution Time breach on Jan 1st,
  Breach Count = 1, Extension Credit = 30 days
- Resolution Time breach on April 1st and April 5th,
  Breach Count = 2, Extension Credit = 60 days

**Response & Resolution Time Breaches:**
- Response Time breach on August 1st, August 15th, August 20th,
  Resolution Time breach on August 25th,
  Extension Credit: 50 days (3 x Response in one calendar month, 1x Resolution)
SADA Systems, Inc.
GOOGLE APPS CUSTOMER AGREEMENT

This GOOGLE APPS CUSTOMER AGREEMENT (this “Agreement”), is made and entered into as of [EFFECTIVE DATE] (the “Effective Date”), between SADA Systems Inc., a corporation organized under the laws of the state of California, with offices at 5250 Lankershim Blvd., Suite 620, North Hollywood, CA 91601 (“SADA”), and _________________________, a state government agency and educational institute of the Commonwealth of Virginia, with offices at _________________________ (“Customer”).

1. SERVICES AND TERMS OF SERVICE

1.1 Service. This Agreement establishes the terms under which SADA, as an authorized reseller of Google, Inc. (“Google”), will provide Customer with access to the Google hosted services set forth in Exhibit A (the “Services”).

1.2 Support. Customer will respond to questions and complaints from the individuals Customer permits to use the Services (such individuals, “End Users”) or third parties relating to Customer’s or End Users’ use of the Services. SADA will provide front-line technical support directly to Customer’s technology administrators with respect to questions, complaints and other support issues that Customer cannot resolve, and SADA is hereby authorized by Customer to submit Customer support issues to Google on behalf of Customer. Customer may also contact Google with respect to technical support issues in accordance with Google’s technical support guidelines (the “TSSG”) available at http://www.google.com/apps/intl/en/terms/tssg.html or such other URL as may be provided by Google.

1.3 Google Apps Terms of Service. Customer understands and agrees that the End Users will be required to agree to Google’s Terms of Service before using the Services, which will be presented by Google upon End User’s first log in. The Terms of Service govern End User’s access to and use of the Services.

1.4 Service Levels. The Google Apps Covered Services (as defined in the Google SLA) will meet the requirements set forth in the Google Apps Service Level Agreement found at http://www.google.com/apps/intl/en/terms/sla.html (the “Google SLA”). In the event of a breach of such service levels, as Customer’s sole and exclusive remedy, Customer will be provided the remedies set forth in the Google SLA.

2. CUSTOMER OBLIGATIONS, During the term of this Agreement, Customer will have the following obligations, in addition to those set forth elsewhere in this Agreement.

2.1 Compliance with Law; Compliance with Agreement. Customer will comply with all laws, rules and regulations applicable to its use of the Services, including those regarding the management and administration of its electronic messaging system. Customer acknowledges and agrees that SADA and Google are serving as a data processor and their responsibilities and liability do not extend to the internal management or administration of Customer’s electronic messaging system or messages. Customer is responsible for ensuring that it and its End Users use the Services in accordance with the Terms of Service and Acceptable Use Policy, as set forth in Section 1.3 and Section 2.5.

2.2 Customer Administration of the Services. Customer is responsible for: (A) maintaining the confidentiality of the password and administrative account provided to Customer by Google for the purpose of administering End User accounts; (B) designating those of Customer’s employees and SADA’s employees who are authorized to access the administrative account; and (C) ensuring that all activities that occur in connection with Customer’s administrative account comply with the Terms of Service.
2.3 **Privacy.** Customer agrees to protect the privacy rights of its End Users in accordance with all applicable laws and regulations.

2.4 **Unauthorized Use.** Customer will use commercially reasonable efforts to prevent unauthorized use of the Services, and to terminate any unauthorized use. Customer will promptly notify SADA or Google of any unauthorized use of, or access to, the Services of which it becomes aware.

2.5 **Acceptable Use Policy.** Customer agrees that its use of the Services is subject to its compliance with Google’s Acceptable Use Policy, which is available at http://www.google.com/apps/intl/en/terms/use_policy.html (or such URL as Google may provide) and which may be updated from time to time.

2.6 **Intended Use; Email Accounts.** The Services are for use with normal business messaging traffic only, and may not be used for any other purpose, including use of the message encryption services (if applicable) with machine generated message encryption and delivery. For each End User for which Customer will be routing email and/or archiving email, if any, through the Services, Customer shall establish an email account in Google’s identity management systems. Failure to abide by the terms of this Section may be considered a material breach of this Agreement and, if not cured by Customer following notice by SADA, may result in a suspension of Services until such failure is remedied.

3. **CHARGES AND PAYMENT**

3.1 **Fees.** Customer will pay SADA the fee(s) set forth on Exhibit A to this Agreement in accordance with Section 3.3. Following the Initial Term, SADA has the right to change the fee, effective as of the next renewal date, provided that SADA will notify Customer of any fee increase prior to the expiration of the then-current term.

3.2 **Support Charges.** Any support to be provided by SADA under Section 1.3 of this Agreement will be performed on business days between the hours of 9:00 a.m. to 6:00 p.m. Pacific Time, at no additional cost. Any support services requested by Customer outside these hours will be billed to Customer at an hourly rate of $292.50.

3.3 **Payment Options.** Customer will pay for the Services on a full prepaid basis for the Initial Term of this Agreement and each succeeding 12-month renewal term, to the extent applicable.

(A) Fees for prepaid orders where SADA issues an invoice are due within thirty (30) days after Customer’s receipt of the invoice, and are considered delinquent 30 days after the due date of the applicable invoice.

3.4 **Currency.** Customer will make all payments in U.S. dollars.

4. **TERM, TERMINATION AND ADDITIONAL END USER ACCOUNTS**

4.1 **Term.** The term of this Agreement will begin on the Effective Date and will continue for an initial period as set forth in Exhibit A (such period, the “Initial Term”). At the end of the Initial Term, the parties may agree to renew this Agreement. All terms and conditions of this Agreement shall apply during each renewal term, except for the fees. The fee for each renewal term will be the rates then in effect, as described in Section 3.1.

4.2 **Termination.** This Agreement will terminate: (A) immediately upon termination or expiration of Customer’s right to use the Services as a result of a termination of the Terms of Service by Google or Customer; (B) upon expiration of the then-current term if Customer has not chosen to renew this Agreement prior to the expiration of the then-current term; or (C) upon expiration of the then-current term if SADA has provided at least 60 days’ advance written notice of termination to Customer.

4.3 **Effects of Termination.** If this Agreement terminates, then the rights granted hereunder by any party to the other will cease immediately and Customer’s access to the Services will cease.
4.4 Additional End User Accounts. Customer may alter the number of End User Accounts per Customer domain at any time. For End User Accounts added during the Initial Term or any Renewal Term, the initial term for such End User Accounts will be pro-rated, beginning on the date of the applicable order and ending on the expiration of the applicable term. Customer may request End User Accounts by notifying its designated SADA account manager. For each purchase of End User Accounts, SADA will issue a quote to Customer. End User Accounts automatically renew in accordance with the terms of this Agreement, unless terminated by either party in accordance with the terms of this Agreement. SADA cannot transfer End User Accounts from one Customer domain name to another.

4.5 Archived Messages. If the Services include archiving functionality, Customer messages will be retained for up to the period set forth in Exhibit A, provided that Customer renews the applicable Services with SADA for each year of such retention period. The retention period will apply to all data archived under the Services. Failure to renew the applicable Services during the retention period will terminate SADA’s and Google’s obligation to retain any of Customer’s data or indexes.

5. CUSTOMER DATA AND CONFIDENTIAL INFORMATION

5.1 Customer Data. SADA will treat all Customer Data in accordance with laws and regulations applicable to the data and will implement policies and procedures with respect to the Customer Data no less protective of the rights of Customer or its End Users as those found in Google’s Privacy Policy (located at http://www.google.com/intl/en/privacy/privacy-policy.html) or Google’s Privacy Notice (located at http://www.google.com/apps/intl/en/terms/users_privacy.html). Changes to the Privacy Policy and Privacy Notice will be made as stated in the applicable policy. For purposes of this Agreement, “Customer Data” means all data and information provided by Customer’s End Users via the sign up process for the Services, as well as data, including electronic messages and any attachments provided, generated, transmitted or displayed via the Services by Customer or its End Users.

5.2 Confidential Information. Each party will: (A) protect the other party’s Confidential Information with the same standard of care it uses to protect its own Confidential Information, but in no event less than reasonable care; and (B) not disclose the other party’s Confidential Information, except to affiliates, employees, agents and professional advisors who need to know it (and, in the case of non-employees, who have agreed in writing or are otherwise bound, to keep it confidential). Each party (and any affiliates, employees and agents to whom the Confidential Information was disclosed) may use such Confidential Information only to exercise rights and fulfill obligations under this Agreement, while using reasonable care to protect it. SADA is responsible for any actions of its affiliates, employees and agents in violation of this Section. Customer is responsible for any actions of its employees and agents in violation of this Section. For purposes of this Agreement, “Confidential Information” is information disclosed by one party to the other party under this Agreement that is marked as confidential or would normally be considered confidential under the circumstances. In particular, Customer Data and SADA’s pricing are Confidential Information.

5.3 Exceptions. Confidential Information does not include information that: (A) is or subsequently becomes published or available to the public through no fault of the recipient, (B) is received by the recipient from a third party without a duty of confidentiality; (C) is independently developed by recipient, or (D) was in the recipient’s possession or was known to the recipient before it was disclosed to the recipient by the disclosing party.

5.4 Required Disclosure. Each party may disclose the other party’s Confidential Information when required by law but only after it, if legally permissible: (A) uses commercially reasonable efforts to notify the other party; and (B) gives the other party the chance to challenge the disclosure.

6. INTELLECTUAL PROPERTY RIGHTS. Except as expressly set forth herein, this Agreement does not grant either party any rights, implied or otherwise, to the other’s content or any of the other’s intellectual property. As between the parties, Customer owns all Intellectual Property Rights in Customer
Data. The parties acknowledge and agree that Google owns all Intellectual Property Rights in the Services. For purposes of this Agreement, “Intellectual Property Rights” means current and future worldwide rights under patent law, copyright law, trade secret law, trademark law, moral rights law and other similar rights.

7. DISCLAIMER OF WARRANTIES. SADA and Google make no warranty of any kind, whether express, implied, statutory or otherwise, including without limitation warranties of merchantability, fitness for a particular purpose, accuracy or noninfringement. SADA and Google make no representation about any content or information made accessible by or through the Service. Customer acknowledges that the Services are not a telephony service and that the Services are not capable of placing or receiving any calls, including emergency calls, over publicly switched telephone networks.

8. Intentionally deleted.

9. LIMITATION OF LIABILITY. In no event, whether in contract, tort or otherwise (including breach of warranty, negligence and strict liability in tort), will either party be held liable under this Agreement for indirect or consequential, exemplary, punitive or special damages (including, without limitation, lost profits, loss of use or loss of data), even if such party is aware of or has been advised of the possibility of such damages in advance and even if direct damages do not satisfy a remedy. In no event will either party be held liable under this Agreement for more than the amount paid by Customer to SADA for the Services during the 12 months prior to the event giving rise to liability. In no event will Google be held liable for any damages, whether direct, indirect, incidental or consequential, arising from SADA’s distribution and resale of the Services. These limitations of liability do not apply to a party’s indemnification obligations.

10. GENERAL PROVISIONS

10.1 Third Party Beneficiary. The parties agree that Google is a third party beneficiary of this Agreement. There are no other third party beneficiaries to this Agreement.

10.2 Waiver of Default. No delay or omission by either party to exercise any right or power under this Agreement will be construed to be a waiver thereof. A waiver by either party of any breach or covenant will not be construed to be a waiver of any succeeding breach thereof or of any other covenant.

10.3 Survival. The provisions of Section 3.6, Article 5, Article 6, Article 7, Article 8, Article 9 and this Article, as well as any other provision of this Agreement that contemplates performance or observance subsequent to termination or expiration of this Agreement will survive expiration or termination of this Agreement and continue in full force and effect for the period set forth therein, or if no period is set forth therein, indefinitely.

10.4 Force Majeure. Neither SADA nor Google shall be liable for inadequate performance to the extent caused by a circumstance beyond its reasonable control, including, without limitation, domain name server issues outside its direct control, labor strikes or shortages, riots, insurrection, fires, flood, storm, explosions, acts of God, war, terrorism, governmental action, labor conditions, earthquakes and material shortage.

10.5 Severability. If any provision of this Agreement is found to be illegal or otherwise unenforceable in any respect, that provision will be deemed to be restated to reflect as nearly as possible the original
intent of the parties in accordance with applicable law. The remainder of this Agreement will remain in full force and effect.

10.6 Entire Agreement; Amendment and Waiver. This Agreement and any exhibits referred to herein, each of which is incorporated herein for all purposes, is a part of Contract # UCP-TS-C02-12 executed by Client and SADA (the "Standard Contract") and is not a standalone agreement. To the extent that anything contained in this Agreement conflicts or is inconsistent with the terms and conditions contained within Client’s RFP #0016512 included in the Standard Contract, the RFP terms shall take precedence. No change, waiver or discharge hereof will be valid unless made in writing and signed by an authorized representative of the party against which such change, waiver or discharge is sought to be enforced.

10.7 Counterparts. The parties may enter into this Agreement in counterparts which taken together will constitute one instrument.

IN WITNESS WHEREOF, this Agreement has been executed by the parties through their duly authorized officers as of the date set forth above.

SADA Systems, Inc.  

_____________________________  _____________________________

Tony Safoian, President and CEO  Name:

Title:
EXHIBIT A

Under the terms of the Agreement of which this Exhibit is a party, SADA will provide the following Google products to Customer in the indicated quantity and at the indicated pricing:

<table>
<thead>
<tr>
<th>Item</th>
<th>Quantity</th>
<th>Price Per Item</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Apps Postini GMD 1-Year</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Apps Postini GMD 10-Year</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Message Encryption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Message Security only</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Apps End User Accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Initial Term of this Agreement will be _______ months.

Customer opts to pay for the Services:

- [ ] On a prepaid basis
- [ ] On a month-to-month or other periodic basis using SADA’s Cloud Subscription service

Customer understands that in order to qualify for periodic financing payments using SADA’s Cloud Subscription service, Customer must satisfy a credit check and enter into a loan and financing agreement with [FINANCING ENTITY]. If Customer does not qualify for such month-to-month payments, Customer must pay for the Services on a prepaid basis.

**Overage Charge**

Customer shall notify SADA in the event that Customer exceeds the number of mailboxes/units set forth above for any Postini, message encryption or message security product, such notice to be provided to SADA within 10 days of the occurrence of such overage. Upon becoming aware of any such overage (whether from Customer or otherwise), SADA will charge Customer an “Overage Charge” for each month during which an overage exists. Such Overage Charge will be equal to the product of (A) the number of excess mailboxes and (B) 1/12 of the annual charge per mailbox, which Overage Charge will be invoiced to Customer by SADA monthly in arrears.
Google Apps for Education Agreement

This Google Apps for Education Agreement (the "Agreement") is entered into by and between Google Inc. ("Google"), with offices at 1600 Amphitheatre Parkway, Mountain View, California 94043 and Virginia Polytechnic Institute and State University, with an address at 1700 Pratt Drive Blacksburg, VA 24060 ("Customer"). This Agreement governs Customer's access to and use of the Services and will be effective as of the Effective Date.

1. Services.

1.1 General. Google will provide the Services to Customer during the Term.

1.2 Facilities and Data Transfer. All facilities used to store and process Customer Data will adhere to reasonable security standards no less protective than the security standards at facilities where Google stores and processes its own information of a similar type. Google has implemented at least industry standard systems and procedures to ensure the security and confidentiality of Customer Data, protect against anticipated threats or hazards to the security or integrity of Customer Data, and protect against unauthorized access to or use of Customer Data. As part of providing the Services, Google may transfer, store and process Customer Data in the United States or any other country in which Google or its agents maintain facilities. By using the Services, Customer consents to this transfer, processing and storage of Customer Data.

1.3 Modifications.

(a) To the Services. Google may make commercially reasonable changes to the Services from time to time. If Google makes a material change to the Services, Google will inform Customer, provided that Customer has subscribed with Google to be informed about such material change.

(b) To URL Terms. Google may make commercially reasonable changes to the URL Terms from time to time. If Google makes a material change to the URL Terms, Google will inform Customer by either sending an email to the Notification Email Address or alerting Customer via the Admin Console. If the change has a material adverse impact on Customer and Customer does not agree to the change, Customer must so notify Google via the Help Center within thirty days after receiving notice of the change. If Customer notifies Google as required, then Customer will remain governed by the terms in effect immediately prior to the change until the end of the then-current Term. If the Services are renewed, they will be renewed under Google's then current URL Terms.

1.4 Aliases. Customer is solely responsible for monitoring, responding to, and otherwise processing emails sent to the "abuse" and "postmaster" aliases for Customer Domain Names but Google may monitor emails sent to these aliases for Customer Domain Names to allow Google to identify Services abuse.

1.5 Ads.

(a) Default. The default setting for the Services is one that does not allow Google to serve Ads. Customer may change this setting in the Admin Console, which constitutes Customer's authorization for Google to serve Ads. If Customer enables the serving of Ads, it may revert to the default setting at any time and Google will cease serving Ads.

(b) Selectively Showing Ads. Notwithstanding Section 1.5(a), if Customer separates different classifications of End Users by domain or Google provides the capability for Customer to show Ads only to particular sets of End Users within the same domain, then Customer must enable the serving of Ads to End Users who are alumni.

1.6 End User Accounts. Customer may request End User Accounts by: (i) requesting them online via the Admin Console; or (ii) after the Services Commencement Date, contacting Google support personnel. Customer can suspend or delete End User Accounts at any point in time through the Admin Console.

2. Customer Obligations.

2.1 Permitted Uses. The Services are permitted for use only by (a) non-profit educational institutions and (b) other non-profit entities (as defined under the relevant state statutes) with 3,000 or less End User Accounts.

2.2 Compliance. Customer will use the Services in accordance with the Acceptable Use Policy. Google may make new applications, features or functionality for the Services available from time to time, the use of which may be contingent upon Customer's agreement to additional terms. In addition, Google will make other Non-Google Apps Products (beyond the Services) available to Customer and its End Users in accordance with the Non-Google Apps Product Terms and the applicable product-specific Google terms of service. If Customer does not desire to enable any of the Non-Google Apps Products, Customer can enable or disable them at any time through the Admin Console.

Apps for Education (10.02.2011, FF)
2.3 Customer Administration of the Services. Customer may specify one or more Administrators through the Admin Console who will have the rights to access Admin Account(s) and to administer the End User Accounts. Customer is responsible for: (a) maintaining the confidentiality of the password and Admin Account(s); (b) designating those individuals who are authorized to access the Admin Account(s); and (c) ensuring that all activities that occur in connection with the Admin Account(s) comply with the Agreement. Customer agrees that Google's responsibilities do not extend to the internal management or administration of the Services for Customer and that Google is merely a data-processor.

2.4 End User Consent. Customer’s Administrators may have the ability to access, monitor, use, or disclose data available to End Users within the End User Accounts. Customer will obtain and maintain all required consents from End Users to allow: (i) Customer's access, monitoring, use and disclosure of this data and Google providing Customer with the ability to do so and (ii) Google to provide the Services.

2.5 Unauthorized Use. Customer will use commercially reasonable efforts to prevent unauthorized use of the Services and to terminate any unauthorized use. Customer will promptly notify Google of any unauthorized use of, or access to, the Services of which it becomes aware.

2.6 Restrictions on Use. Unless Google specifically agrees in writing, Customer will not, and will use commercially reasonable efforts to make sure a third party does not: (a) sell, resell, lease, or the functional equivalent, the Services to a third party (unless expressly authorized in this Agreement); (b) attempt to reverse engineer the Services or any component; (c) attempt to create a substitute or similar service through use of, or access to, the Services; (d) use the Services for High Risk Activities; or (e) use the Services to store or transfer any Customer Data that is controlled for export under Export Control Laws. Customer is solely responsible for any applicable compliance with HIPAA.

2.7 Third Party Requests. Customer is responsible for responding to Third Party Requests. Google will, to the extent allowed by law and by the terms of the Third Party Request: (a) promptly notify Customer of its receipt of a Third Party Request; (b) comply with Customer’s reasonable requests regarding its efforts to oppose a Third Party Request; and (c) provide Customer with the information or tools required for Customer to respond to the Third Party Request. Customer will first seek to obtain the information required to respond to the Third Party Request on its own, and will contact Google only if it cannot reasonably obtain such information.


3.1 By Customer. Customer will, at its own expense, respond to questions and complaints from End Users or third parties relating to Customer’s or End Users’ use of the Services. Customer will use commercially reasonable efforts to resolve support issues before escalating them to Google.

3.2 By Google. If Customer cannot resolve a support issue consistent with the above, then Customer may escalate the issue to Google in accordance with the TSS Guidelines. Google will provide TSS to Customer in accordance with the TSS Guidelines.

4. Suspension.

4.1 Of End User Accounts by Google. If Google becomes aware of an End User’s violation of the Agreement, then Google may specifically request that Customer Suspend the applicable End User Account. If Customer fails to comply with Google’s request to Suspend an End User Account, then Google may do so. The duration of any Suspension by Google will be until the applicable End User has cured the breach, which caused the Suspension.

4.2 Emergency Security Issues. Notwithstanding the foregoing, if there is an Emergency Security Issue, then Google may automatically Suspend the offending use. Suspension will be to the minimum extent and of the minimum duration required to prevent or terminate the Emergency Security Issue. If Google Suspends an End User Account for any reason without prior notice to Customer, at Customer’s request, Google will provide Customer the reason for the Suspension as soon as is reasonably possible.

5. Confidential Information.

5.1 Obligations. Each party will: (a) protect the other party’s Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to Affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential. Each party (and any Affiliates, employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill its obligations under this Agreement, while using reasonable care to protect it. Each party is responsible for any actions of its Affiliates, employees and agents in violation of this Section.

5.2 Exceptions. Confidential Information does not include information that: (a) the recipient of the Confidential Information already knew; (b) becomes public through no fault of the recipient; (c) was independently developed by the recipient; or (d) was rightfully given to the recipient by another party.
5.3 **Required Disclosure.** Each party may disclose the other party’s Confidential Information when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.

5.4 **FERPA.** The parties acknowledge that (a) Customer Data may include personally identifiable information from education records that are subject to FERPA ("FERPA Records"); and (b) to the extent that Customer Data includes FERPA Records, Google will be considered a “School Official” (as that term is used in FERPA and its implementing regulations) and will comply with FERPA.

6. **Intellectual Property Rights; Brand Features.**

6.1 **Intellectual Property Rights.** Except as expressly set forth herein, this Agreement does not grant either party any rights, implied or otherwise, to the other’s content or any of the other’s intellectual property. As between the parties, Customer owns all Intellectual Property Rights in Customer Data, and Google owns all Intellectual Property Rights in the Services.

6.2 **Display of Brand Features.** Google may display those Customer Brand Features authorized by Customer (such authorization is provided by Customer uploading its Brand Features into the Services) within designated areas of the Services Pages. Customer may specify the nature of this use using the Admin Console. Google may also display Google Brand Features on the Services Pages to indicate that Google provides the Services. Neither party may display or use the other party’s Brand Features beyond what is allowed in this Agreement without the other party’s prior written consent.

6.3 **Brand Features Limitation.** Any use of a party’s Brand Features will inure to the benefit of the party holding Intellectual Property Rights in those Brand Features. A party may revoke the other party’s right to use its Brand Features pursuant to this Agreement with written notice to the other and a reasonable period to stop the use.

7. **Publicity.** Neither party may make any public statement regarding the relationship contemplated by this Agreement without the other party’s prior written consent. Notwithstanding the foregoing, (a) Customer is permitted to state publicly that it is a customer of the Services, consistent with the Trademark Guidelines, and (b) Customer consents to Google’s use of Customer’s name in a general customer list, but only if Customer is not the only Customer appearing on the list. For clarification, Customer does not need to seek approval from Google if Customer is repeating a public statement that is substantially similar to a public statement that has been previously approved by Google in accordance with the provisions of this Agreement.

8. **Representations, Warranties and Disclaimers.**

8.1 **Representations and Warranties.** Each party represents that it has full power and authority to enter into the Agreement. Each party warrants that it will comply with all laws and regulations applicable to its provision, or use, of the Services, as applicable (including applicable security breach notification law). Google warrants that it will provide the Services in accordance with the applicable SLA. Customer acknowledges and agrees that it is solely responsible for compliance with the Children’s Online Privacy Protection Act of 1998, including, but not limited to, obtaining parental consent concerning collection of students’ personal information used in connection with the provisioning and use of the Services by the Customer and End Users.

8.2 **Disclaimers.** TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS EXPRESSLY PROVIDED FOR HEREIN, NEITHER PARTY MAKES ANY OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE AND NONINFRINGEMENT. GOOGLE MAKES NO REPRESENTATIONS ABOUT ANY CONTENT OR INFORMATION MADE ACCESSIBLE BY OR THROUGH THE SERVICES, CUSTOMER ACKNOWLEDGES THAT THE SERVICES ARE NOT A TELEPHONY SERVICE AND THAT THE SERVICES ARE NOT CAPABLE OF PLACING OR RECEIVING ANY CALLS, INCLUDING EMERGENCY SERVICES CALLS, OVER PUBLICLY SWITCHED TELEPHONE NETWORKS. THE SERVICES ARE NEITHER DESIGNED NOR INTENDED FOR HIGH RISK ACTIVITIES.

9. **Term; No Fees.**

9.1 **Term.** This Agreement will remain in effect for the Term.

9.2 **Auto Renewal.** At the end of the Initial Term and each renewal term, the Services will automatically renew for an additional term of twelve months. If either party does not want the Services to renew, then it must notify the other party in writing at least 15 days prior to the end of the then current term. This notice of non-renewal will be effective upon the conclusion of the then current term.

9.3 **No Fees.** During the Initial Term, Google will not charge Customer fees for the Services. Upon the parties’ mutual written agreement, (a) Google may charge Customer fees for the Services after the Initial Term and (b) Google may
charge Customer fees for a premium version of the Services or for optional functionality or enhancements that may be added to the Services by Google.

9.4 Services Use. Customer has no obligation to use the Services and may cease using the Services at any time for any reason (or no reason).

10. Termination.

10.1 Termination for Breach. Either party may suspend performance or terminate this Agreement if: (i) the other party is in material breach of the Agreement and fails to cure that breach within thirty days after receipt of written notice; (ii) the other party ceases its business operations or becomes subject to insolvency proceedings and the proceedings are not dismissed within ninety days; or (iii) the other party is in material breach of this Agreement more than two times notwithstanding any cure of such breaches.

10.2 Other Termination. Customer may terminate this Agreement for any reason (or no reason) with thirty days prior written notice to Google.

10.3 Effects of Termination. If this Agreement terminates, then: (i) the rights granted by one party to the other will cease immediately (except as set forth in this Section); (ii) Google will provide Customer access to, and the ability to export, the Customer Data for a commercially reasonable period of time at Google’s then-current rates, if applicable, for the Services; (iii) after a commercially reasonable period of time, Google will delete Customer Data by removing pointers to it on Google’s active servers and overwriting it over time; and (iv) upon request each party will promptly use commercially reasonable efforts to return or destroy all other Confidential Information of the other party.

11. Indemnification.

11.1 By Google. Google will indemnify, defend, and hold harmless Customer from and against all liabilities, damages, and costs (including settlement costs and reasonable attorneys’ fees) arising out of a third party claim that Google’s technology used to provide the Services or any Google Brand Feature infringe or misappropriate any patent, copyright, trade secret or trademark of such third party. Notwithstanding the foregoing, in no event shall Google have any obligations or liability under this Section arising from: (i) use of the Services or Google Brand Features in a modified form or in combination with materials not furnished by Google, and (ii) any content, information or data provided by Customer, End Users or other third parties.

11.2 Possible Infringement.

(a) Repair, Replace, or Modify. If Google reasonably believes the Services infringe a third party’s Intellectual Property Rights, then Google will: (a) obtain the right for Customer, at Google’s expense, to continue using the Services; (b) provide a non-infringing functionally equivalent replacement; or (c) modify the Services so that they no longer infringe.

(b) Suspension or Termination. If Google does not believe the foregoing options are commercially reasonable, then Google may suspend or terminate Customer’s use of the Services with a minimum of six months written notice to Customer, unless prohibited by a court of competent jurisdiction.

11.3 General. Customer will promptly notify Google of the claim and cooperate with Google in defending the claim. Google has full control and authority over the defense, except that: (a) any settlement requiring Customer to admit liability or to pay any money will require Customer’s prior written consent, such consent not to be unreasonably withheld or delayed; and (b) Customer may join in the defense with its own counsel at its own expense. THE INDEMNITY ABOVE IS CUSTOMER’S ONLY REMEDY UNDER THIS AGREEMENT FOR VIOLATION BY GOOGLE OF A THIRD PARTY’S INTELLECTUAL PROPERTY RIGHTS.

12. Limitation of Liability.

12.1 Limitation on Indirect Liability. NEITHER PARTY WILL BE LIABLE UNDER THIS AGREEMENT FOR LOST REVENUES OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES, EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN THAT SUCH DAMAGES WERE POSSIBLE AND EVEN IF DIRECT DAMAGES DO NOT SATISFY A REMEDY.

12.2 Limitation on Amount of Liability. NEITHER PARTY MAY BE HELD LIABLE UNDER THIS AGREEMENT FOR MORE THAN ONE THOUSAND DOLLARS.

12.3 Exceptions to Limitations. These limitations of liability apply to the fullest extent permitted by applicable law, but do not apply to breaches of confidentiality obligations, violations of a party’s Intellectual Property Rights by the other party, or indemnification obligations.
13.1 **Notices.** Unless specified otherwise herein: (a) all notices must be in writing and addressed to the attention of the other party's legal department and primary point of contact; and (b) notice will be deemed given: (i) when verified by written receipt if sent by personal courier, overnight courier, or when received if sent by mail without verification of receipt; or (ii) when verified by automated receipt or electronic logs if sent by facsimile or email.

13.2 **Assignment.** Neither party may assign or transfer any part of this Agreement without the written consent of the other party, except to an Affiliate, but only if: (a) the assignee agrees in writing to be bound by the terms of this Agreement; and (b) the assigning party remains liable for obligations incurred under the Agreement prior to the assignment. Any other attempt to transfer or assign is void.

13.3 **Change of Control.** Upon a change of control (for example, through a stock purchase or sale, merger, or other form of corporate transaction): (a) the party experiencing the change of control will provide written notice to the other party within thirty days after the change of control; and (b) the other party may immediately terminate this Agreement any time between the change of control and thirty days after it receives the written notice in subsection (a).

13.4 **Force Majeure.** Neither party will be liable for inadequate performance to the extent caused by a condition (for example, natural disaster, act of war or terrorism, riot, labor condition, governmental action, and Internet disturbance) that was beyond the party's reasonable control.

13.5 **No Waiver.** Failure to enforce any provision of this Agreement will not constitute a waiver.

13.6 **Severability.** If any provision of this Agreement is found unenforceable, the balance of the Agreement will remain in full force and effect.

13.7 **No Agency.** The parties are independent contractors, and this Agreement does not create an agency, partnership or joint venture.

13.8 **No Third-Party Beneficiaries.** There are no third-party beneficiaries to this Agreement.

13.9 **Equitable Relief.** Nothing in this Agreement will limit either party's ability to seek equitable relief.

13.10 **Governing Law.**

a. **For State and City Government Entities.** If Customer is a city or state government entity, then the parties agree to remain silent regarding governing law and venue.

b. **For All other Entities.** If Customer is any entity not set forth in Section 13.10(a) then the following applies: This Agreement is governed by California law, excluding that state's choice of law rules. FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS AGREEMENT, THE PARTIES CONSENT TO PERSONAL JURISDICTION IN, AND THE EXCLUSIVE VENUE OF, THE COURTS IN SANTA CLARA COUNTY, CALIFORNIA.

13.11 **Amendments.** Any amendment must be in writing and expressly state that it is amending this Agreement.

13.12 **Survival.** The following Sections will survive expiration or termination of this Agreement: 5 (Confidential Information), 6.1 (Intellectual Property Rights), 10.3 (Effects of Termination), 11 (Indemnification), 12 (Limitation of Liability), 13 (Miscellaneous) and 15 (Definitions).

13.13 ** Entire Agreement.** This Agreement, and all documents referenced herein, is the parties' entire agreement relating to its subject and supersedes any prior or contemporaneous agreements on that subject. If Customer is presented with a similar agreement on the same subject matter upon its log in to use the Services, this Agreement supersedes and replaces that agreement. The terms located at a URL and referenced in this Agreement are hereby incorporated by this reference.

13.14 ** Interpretation of Conflicting Terms.** If there is a conflict between this Agreement and the URL Terms, this Agreement will control.

13.15 **Counterparts.** The parties may enter into this Agreement in counterparts, including facsimile, PDF or other electronic copies, which taken together will constitute one instrument.

14. **Definitions.**

"Acceptable Use Policy" means the acceptable use policy for the Services available at http://www.google.com/a/help/intl/en/admins/use_policy.html or such other URL as may be provided by Google.
“Admin Account(s)” means the administrative account(s) provided to Customer by Google for the purpose of administering the Services. The use of the Admin Account(s) requires a password, which Google will provide to Customer.

“Admin Console” means the online tool provided by Google to Customer for use in reporting and certain other administration functions.

“Administrators” mean the Customer-designated technical personnel who administer the Services to End Users on Customer’s behalf.

“Ads” means online advertisements displayed by Google to End Users.

“Affiliate” means any entity that directly or indirectly controls, is controlled by, or is under common control with a party.

“Agreement” means this Google Apps for Education Agreement.

“Brand Features” means the trade names, trademarks, Services marks, logos, domain names, and other distinctive brand features of each party, respectively, as secured by such party from time to time.

“Confidential Information” means information disclosed by a party to the other party under this Agreement that is marked as confidential or would normally be considered confidential under the circumstances. Customer Data is considered Customer’s Confidential Information.

“Customer Data” means data, including email, provided, generated, transmitted or displayed via the Services by Customer or End Users.

“Customer Domain Names” means the following domain names owned or controlled by Customer, which will be used in connection with the Services: v.edu. Customer may provide the Services to any of its sub-domains (for example, if Customer Domain Name is “edu.com”, a sub-domain may include “alumni.edu.com”) without written approval from Google.

“Effective Date” means the date this Agreement is countersigned.

“Emergency Security Issue” means either: (a) Customer’s use of the Services in violation of the Acceptable Use Policy, which could disrupt: (i) the Services; (ii) other customers’ use of the Services; or (iii) the Google network or servers used to provide the Services; or (b) unauthorized third party access to the Services.

“End Users” means the individuals Customer permits to use the Services.

“End User Account” means a Google-hosted account established by Customer through the Services for an End User.

“Export Control Laws” means all applicable export and re-export control laws and regulations, including the Export Administration Regulations (“EAR”) maintained by the U.S. Department of Commerce, trade and economic sanctions maintained by the Treasury Department’s Office of Foreign Assets Control, and the International Traffic in Arms Regulations (“ITAR”) maintained by the Department of State.

“FERPA” means the Family Educational Rights and Privacy Act (20 U.S.C. 1232g) and the Family Educational Rights and Privacy Act Regulations (34 CFR Part 99), as amended or otherwise modified from time to time.

“Help Center” means the Google help center accessible at http://www.google.com/support/, or other such URL as Google may provide.

“High Risk Activities” means uses such as the operation of nuclear facilities, air traffic control, or life support systems, where the use or failure of the Services could lead to death, personal injury, or environmental damage.

“HIPAA” means the Health Insurance Portability and Accountability Act of 1996, as may be amended from time to time, and any regulations issued thereunder.

“Intellectual Property Rights” means current and future worldwide rights under patent law, copyright law, trade secret law, trademark law, moral rights law, and other similar rights.

“Initial Term” means the term that begins on the Effective Date and continues for 5 years.

“Non-Google Apps Products” means Google products which are not part of the Services, but which may be accessed by End Users using their End User Account login and password. The Non-Google Apps Products are set forth at the following URL: http://www.google.com/support/a/bin/answer.py?hl=en&answer=181865, or such other URL as Google may provide.
"Non-Google Apps Product Terms" means the terms found at the following URL:
http://www.google.com/apps/intl/en/terms/additional_services.html, or such other URL as Google may provide from time to time.

"Notification Email Address" means the email address designated by Customer to receive email notifications from Google. Customer may change this email address through the Admin Console.

"Services" means the Google Apps for Education Services provided by Google and used by Customer under this Agreement. The Services are described here: http://www.google.com/a/help/intl/en/users/user_features.html, or such other URL as Google may provide.

"Services Commencement Date" is the date upon which Google makes the Services available to Customer.

"Services Pages" mean the web pages displaying the Services to End Users.

"SLA" means the Services Level Agreement located here: http://www.google.com/a/help/intl/enadmins/sla.html, or other such URL as Google may provide.

"Suspend" means the immediate disabling of access to the Services, or components of the Services, as applicable, to prevent further use of the Services.

"Term" means the term of this Agreement, which begins on the Effective Date and continues until the earlier of: (a) the end of the applicable term for the Services or (b) the Agreement is terminated as set forth herein.

"Trademark Guidelines" means Google's Guidelines for Third Party Use of Google Brand Features, located at the following URL: http://www.google.com/permissions/guidelines.html, or other such URL as Google may provide.

"Third Party Request" means a request from a third party for records relating to an End User's use of the Services. Third Party Requests can be a lawful search warrant, court order, subpoena, other valid legal order, or written consent from the End User permitting the disclosure.

"TSS" means the technical support services provided by Google to the Administrators during the Term pursuant to the TSS Guidelines.

"TSS Guidelines" means Google's technical support services guidelines then in effect for the Services. TSS Guidelines are at the following URL: http://www.google.com/a/help/intl/enadmins/tssg.html or such other URL as Google may provide.

"URL Terms" means the Acceptable Use Policy, the SLA, and the TSS Guidelines.

IN WITNESS WHEREOF, the parties have executed this Agreement by persons duly authorized as of the Effective Date.

Google
By: [Signature]
Authorized Signature
Title: [Title]
Date: [Date]

Customer
By: [Signature]
Authorized Signature
Title: [Title]
Date: [Date]
Addendum

This Addendum (the "Addendum") is incorporated by reference into the Google Apps Enterprise Agreement, Google Apps for Education Agreement, Google Apps for Government Agreement, Google Apps for Business via Reseller Agreement, Google Apps for Government via Reseller Agreement, or Google Apps Enterprise via Reseller Agreement attached to this Addendum between Google and the Customer (as applicable, the "Agreement"). The provisions of this Addendum shall amend or supplement the referenced section(s) of the Agreement as indicated below.

WHEREAS, the parties desire to modify certain provision(s) of the Agreement;

NOW, THEREFORE, for good and valuable consideration, the parties hereto agree as follows:

1. Security Breach Notification. The following is added to the Agreement:

   "Security Breach Notification. To the extent a state or federal security breach law applies to a Security Breach, Google will comply with the applicable law. To the extent no such law applies to a Security Breach, Google will notify Customer of a Security Breach, following the discovery or notification of such Security Breach, in the most expedient time possible under the circumstances, without unreasonable delay, consistent with the legitimate needs of applicable law enforcement, and after taking any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. Google will send any applicable notifications regarding a Security Breach to the Notification Email Address. "Security Breach" means an actual disclosure, or reasonable belief that there has been a disclosure, by Google of Customer Data to any unauthorized person or entity."

2. Security Standards. The following is added to the Agreement:

   "Security Standards. As of the Effective Date, Google abides by the security standards set forth on Exhibit A attached to this Addendum ("Security Standards"). During the Term of the Agreement, the Security Standards may change but Google agrees that any such change shall not cause a material degradation in the security of the Services."

3. Miscellaneous. All other terms and conditions of the Agreement shall remain unchanged and in full force and effect. In the event of a conflict between the terms and conditions of the Agreement and the terms and conditions of this Addendum, the terms and conditions of this Addendum shall govern.
Google Enterprise Products Security Standards

1. Personnel. Google has, and will maintain, a security policy for its security personnel, and requires security training as part of the training package for Google security personnel. Google’s security personnel are responsible for the ongoing monitoring of Google’s security infrastructure, the review of Google products and services, and for responding to security incidents.

2. Data Storage and Handling. Google will maintain all data on Google-owned servers and disks. Google will replicate data across multiple systems, and will store all decommissioned disks in a secure facility until wiped or destroyed.

3. Data Transmission. Google will transfer all data via internet standard protocols. Gmail, Calendar, Docs and Spreadsheet, and Google Talk offer Customer the ability to encrypt data during transmission using SSL and TLS.

4. Business Continuity Planning/Disaster Recovery. Google will replicate data across multiple separate systems to enhance business continuity in the event of disaster and system failure. Google will maintain a data center infrastructure that is geographically distributed to enhance system redundancy. Google will also maintain a geographically distributed staff to augment system availability in the event of a disaster.

5. Incident Response. Google will monitor a variety of communication channels for security incidents, and Google’s security team will react promptly to known incidents.

6. Computer Room Access. Google will store all production data in physically secure datacenters. Google will restrict access to the datacenters on a need-to-know basis to authorized staff.

7. Data and Application Security. Google will logically separate data from different End Users from each other, and only data for an authenticated End User will be displayed to that End User. A central authentication facility is used across all applications to increase uniform security of data.

8. Data Isolation and Architecture. Google will store data in a multi-tenant environment on Google servers. Google will logically isolate data on a per End User basis at the application layer. Google will also logically isolate data on a per organization basis, and each organization will be given control over specific data sharing policies.

9. Change Management. Google will continue to employ a code review process to increase the security of the code used to provide the Services. Google will also continue to employ a security review process to enhance the security products in production environments.

10. Server Operating Systems. Google servers will use a hardened Linux implementation customized for the Google application environment. Google data is stored using Google proprietary algorithms to augment data security and redundancy.

11. Access Control and Privilege Management. Google employs a centralized access management system to control personnel access to Google production servers, and will only provide access to a limited number of authorized personnel. Customers or End Users must authenticate themselves via a central authentication system or via a Customer’s single sign on system in order to use the Services. Each application checks credentials in order to allow the display of authorized data to that End User.

12. User Accounts. Customer will have control over the creation, deletion, and suspension of End User accounts on Google infrastructure.

13. Password Policy. Customers can use their own password and authentication policy in conjunction with Service using the Google single sign on functionality.

14. Network Connectivity Security Requirements. Google will protect its infrastructure with multiple levels of network devices at multiple layers.

15. S3AF 16. Google has obtained a Standards for Attestation Engagements No. 16 Type II audit report.

16. Data Center Environment and Physical Security. The following is a general description of Google’s various data center environments and efforts to ensure physical security in these environments.

   a. Google Data Center Infrastructure. Google maintains a vast number of geographically distributed data centers located primarily in the USA and the European Union.

   b. Physical Security Staffing. Each Google data center maintains a security organization responsible for all data center security functions 24 hours a day, 7 days a week. The security organization monitors Closed Circuit TV (CCTV) cameras and all alarm systems. Internal and external patrols of the data center are performed regularly. The data centers are housed in facilities that require electronic key access, with alarms that are linked to guard stations.

   c. Physical Security Access Procedures. Formal access procedures exist for allowing physical access to the data centers. All entrants to the data center are required to identify themselves as well as show proof of identity to security operations. Valid proof of identity is a photo identification issued by Google and a governmental entity. Only authorized Google employees and contractors are allowed entry to the data centers. Data center managers must approve any visitor in advance for the specific data center and internal areas they wish to visit. Only authorized Google employees and contractors who permanently work at the data centers are permitted to request card access to these facilities. Data center card access requests must be made through e-mail, and requires the approval of the requestor’s manager and the data

(9-15-11)
center director. All other Google employees and authorized contractors requiring temporary data center access must sign in at the guard station, present a Google badge (Google employees or contractors) or ID issued by their employer (authorized contractors) and reference an approved data center access record identifying the individual as approved.

d. Physical Security Devices. Data centers employ electronic card key and biometric access control system that are linked to a system alarm. The access control system monitors and records each individual’s access to perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual’s job responsibilities. All entrants to the data centers must pass through a mantrap. The fire doors at the data centers are alarmed and can only be opened from the inside. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. Security operations personnel manage the CCTV monitoring, recording and control equipment. The CCTV equipment is connected by secure cables throughout the data centers. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 90 days based on activity.

e. Environmental Safeguards.

i. Redundancy. The data centers are designed with resiliency and redundancy. The redundancy is intended to minimize the impact of common equipment failures and environmental risks. Infrastructure systems have been designed to eliminate single points of failure. Dual circuits, switches, networks or other necessary devices are utilized to provide this redundancy. Critical facilities infrastructure at the data centers have been designed to be robust, fault tolerant and concurrently maintainable. Preventative and corrective maintenance is designed to be performed without interruption of services. All environmental equipment and facilities have documented preventative maintenance procedures that detail the procedure and frequency of performance in accordance with the manufacturer’s or internal specifications. Preventative and corrective maintenance of the Google data center equipment is scheduled through a standard change process. Preventative maintenance is performed on all infrastructure systems according to documented procedures.

ii. Power.

a. The data center electrical power systems are designed to be fully redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for every critical infrastructure component in the data center. This redundancy begins with dual utility power feeds, primary and alternate, to parallel utility switchboards sized so that any one can provide power to the entire facility. The output power is routed to supply all building loads including uninterruptible power supplies (UPS), building and mechanical services, and heating, ventilation and air conditioning systems.

b. Backup power is provided by various mechanisms including, but not limited to UPS batteries. Backup power is designed to supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted for any reason, backup power is designed to provide transitory power until the diesel generator systems take over. In the event of unavailability of both electrical utility and diesel generators, backup power can provide emergency electrical power to run the data center at full capacity for up to 10 minutes.

c. Diesel engine generators are in place to provide power to critical equipment and customer loads. The generators are capable of providing enough emergency electrical power to run the data center at full capacity typically for a period of days. These generators automatically startup and are able to provide power within seconds in the event of a power outage.

17. Firewalls and Intrusion Detection.

a. Google employs multiple layers of network devices and intrusion detection to ensure that our external attack surface is protected.

b. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Many companies make extensive use of third-party technologies (e.g., Network Intrusion Detection Systems - NIDS, Host-based Intrusion Detection Systems - HIDS) to look for known attacks against commonly-installed software, and Security Operations Centers (SOCs) to respond when they arise. We take a different approach by:

i. Tightly controlling the size and make-up of our attack surface through preventative measures;
ii. Employing intelligent detect controls at data entry points; and
iii. Employing technologies that automatically remedy dangerous situations.

c. Most of our Internet-exposed attack surface is comprised of Google-created software and the environment involves a large number of servers. Traditional IDS products are not economical, efficient or useful in these situations and we rely on smarter methods of detecting exploitation.

d. When we approach intrusion detection concepts, we break down our attack surface according to anticipated input vectors (i.e., how hackers will attempt to break in). Google’s hosting infrastructure is custom-built so we have the ability to tightly define our perimeter and the entrance points into our network. Some of the major areas of coverage that achieve the goals above are as follows:

i. As mentioned previously, the OS on every system is stripped down, modified, and hardened to minimize third party vulnerabilities on running systems;
ii. All IP traffic is routed through custom front end servers that detect and stop malicious requests;
iii. Traffic is examined for exploitation of programming errors via methods such as cross-site scripting, and high priority alerts are generated when such an exploit is found;
iv. To prevent buffer overflow attacks, all open source software that is Internet facing or that processes external data goes through several levels of code review, audit, and modification before allowed into production. All changes are contributed back to the open source community.
v. ACLs are checked continually for binary modifications, and any unrecognized modifications are purged;
vi. Router ACLs are used to provide perimeter defense, and an internally routable IP space is used to make sure external connections are never made to internal systems;
vii. Layer 3 filtering is used to mitigate packet-level attacks.

18. **Internal Data Access Processes and Policies – Access Policy.** LDAP, Kerberos and a Google proprietary system utilizing RSA keys provides Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, customer information and configuration information. We require the use of unique user IDs, strong passwords, and carefully monitored access lists to minimize the potential for inappropriate usage of accounts. The granting or modification of access rights is based on a user’s job responsibilities on a need to know basis and must be approved by data owners. Approvals are managed by workflow tools that maintain audit records of all changes. Furthermore, it is Google’s policy to provide system access to individuals who have been trained and require this level of access to perform authorized tasks. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication at Google (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., Credit Card data), Google uses hardware tokens.

19. **Data Replication, Disaster Recovery, and Data Disposal.**

a. **Data Replication.** Data redundancy is built into all database and file system architectures, and all data that is written to disk is replicated on separate systems. Docs, Spreadsheets and Postini database data is also replicated between multiple data centers to prepare for full data center loss. Such protections help ensure that a customer’s data is protected in the event of a disaster. In most cases, customers can also perform their own backups for individual message recovery or archival purposes. Through the mail gateway, a customer can intercept all incoming and outgoing mail, and these can be archived based on any customer criteria. Additionally, each component of the service generally has an API. As a result, an organization can typically pull data out of the service into their own backup whenever needed.

b. **Distributed Data Center Architecture.** Google does not rely on just one datacenter to run our applications. We operate a geographically distributed set of datacenters to keep services running in the event of incidents and disasters at a single datacenter. All datacenters are connected via high-speed private links to ensure secure and fast data transfer between datacenters. Datacenter locations are undisclosed to the public, and data centers are unmarked to ensure optimal data security. Google’s data center management staff is also distributed in multiple geographies to ensure around the clock coverage and system administration that is not location dependent.

c. **Deleted data.** After an End User confirms deletion of a message, the message in question is immediately deleted from the customer’s Google interface and the data is no longer accessible or recoverable by the End User. Pointers to the data on Google’s active and replication servers are removed. Derefenced data will be overwritten with other customer data over time.

d. **Media disposal.** When retired from Google’s systems, every disk containing customer information is subject to a series of data destruction processes before leaving Google’s premises. Operational disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the drive’s serial number for tracking. Finally, the erased drive is released to inventory for reuse and redeployment. If, due to hardware failure, the drive cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the disk erase policy.

e. **Customer Data Removal from Google Enterprise Products.** At any time, an Administrator can delete an End User and their data from Google. Alternatively, an Administrator can suspend an End User or change their password such that their data is accessible to the organization but not the End User. Google provides APIs to most of its Enterprise applications so an Administrator may migrate End Users and data off of Google Enterprise Products at any point. For customer protection, a Google Enterprise product domain can only be cancelled and deleted by calling our support center. The support staff will verify the caller’s status as an Administrator and will delete the account. The account can take up to five days to delete within the system.