UC Campus Assessment Framework for Email Services

Version 1.2

UCITPS workgroup:
Ross Bollens (UCLA), Russ Harvey (UCR), Stephen Lau (UCSF), Gabe Lawrence (UCSD), Ryan Means (UCB), Russ Opland (UCOP), Janine Roeth (UCSC)

Scope

This Assessment Framework was devised to assist UC Campuses in assessing the relative risks of email service providers relative to their own service offering. There is an inherent risk facing all email services and communications (e.g. http://email.ucdavis.edu/Email_Best_Practices_04_16_08_v4.php). This framework is not intended to consider all possible risks facing the University in regards to email services and communications, but instead to provide guidance for Campuses to make informed decisions.

It is recommended that Campuses review the communication practices for areas with higher sensitivity, e.g. Student Health Systems, IRB, Benefits, and Student Judicial Affairs, for both security and privacy considerations. HIPAA and PCI related information is outside the scope of this Assessment Framework and Campuses should consider these factors when utilizing this framework. Campuses are also advised to consider any additional regulations or laws that may be relevant to their Campus. In some cases, actions may be warranted to reduce the use of email or to use encryption to address the risk.

The workgroup has not included in this assessment framework the areas of cost and features/functions/usability, which a Campus may determine are necessary for a full assessment of an email service provider.

How to Use this Assessment Framework

We have intended this framework to assist with institutional evaluations rather than individual evaluation of email service providers. The workgroup has identified a set of relative questions/concerns that are informed by more detailed questions and reference materials. We expect that a team of campus stakeholders[1] will complete the assessment.

[1] Stakeholders may include faculty, legal, security, privacy, research and human resource (academic and staff) representatives.

UC Campus Assessment Framework for Email Services

Draft – Restricted Distribution

Assessment Category: Service Levels and Terms, Acceptable Use Policies

Question	*Importance (1= highest 2= high)*	*Evaluation (1=Acceptable, 2=Acceptable w/ Mitigation, 3= Not Acceptable)*	*Notes, including Mitigation*
How does the provider's availability (e.g. uptime vs. downtime) compare to the campus email system?			
How does the provider's business continuity for the service compare to the campus email system?			
How does the provider's reliability (e.g. proportion of email that is reliably sent) compare to the campus email system?			
How does the provider's integrity rate (e.g. amount of data corruption) compare to the campus email system's rate?			
Who is the owner of the email data?			
Is the process for data migration (in/out) one that the campus can plan for/implement?			
Are the terms for the termination of email service sufficient for the campus to plan for/implement an alternative?			
How do the provider's required acceptable use policies compare with the UC Electronic Communications Policy?			
How do the procedures or requirements to implement acceptable use policies compare to existing procedures or requirements?			
How does the monitoring of users activity or content compare to the campus email system?			
CATEGORY SUMMARY:			

Assessment Category: Security and Privacy

Question	*Importance (1= highest 2= high)*	*Evaluation (1=Acceptable, 2=Acceptable w/ Mitigation, 3= Not Acceptable)*	*Notes, including Mitigation*
How does the provider's security measures compare to that of the campus email system?			
How does the provider's privacy controls compare to that of the campus email system?			
Given the provider's privacy and security controls, can the campus meet its obligations under privacy and data security laws, including jurisdiction?			
How do the procedures for responding to third party and legal requests, (eDiscovery requests, subpoenas and other court orders) compare to existing procedures?			
Can the campus meet its requirements for evidence preservation under eDiscovery?			
How do the procedures for complying with data protection/breach notification requirements of UC's Appendix DS compare to existing procedures?			
CATEGORY SUMMARY			

Assessment Category: Authorization, Authentication and Audit

Question	*Importance (1= highest 2= high)*	*Evaluation (1=Acceptable, 2=Acceptable w/ Mitigation, 3= Not Acceptable)*	*Notes, including Mitigation*
How do the authentication controls (identity/password) compare to that used by the campus email system?			
How do the authorization controls (access) compare to that used by the campus email system?			
How does account provisioning and deprovisioning compare to that used by the campus email system?			
How does the audit capability (e.g. logging) compare with the campus email system?			
How does the capability to detect account compromise (e.g. due to phishing) compare with the campus email system?			
CATEGORY SUMMARY			

Assessment Detail

Data Ownership/Portability

This set of questions should be considered in order to understand the risks related to vendor lock-in.

- Does the provider offer an interoperable export format for email stored within the system?
- Can the campus perform their own data extraction to verify that the format is universal and email is capable of being migrated to another provider?
- Who is the legal owner of the data? (RFI #6)
- If the provider is merged or sold, what happens to the data (RFI #14)?
- What happens to the data sent to the provider upon termination of the contract?
- Is data available for a defined period of time after the contract is terminated to support data migration?
- When a user removes their data from the provider, does the provider retain any rights to continue using that data? How long will the data remain with the provider (in online and offline storage) (RFI #49)?

Additional References:

Vendor contract (as applicable)	
Service termination	RFI #14
Data Ownership	RFI #6
Data migration standards/tools	
Data disposition policies, including deleted information	RFI #49, #56

Service Levels, Acceptable Use Policies

- What are the Acceptable Use Polices or other Terms of Service that end users are required to follow?
- Is the campus required to monitor for compliance with the providers policies or terms of service?
- Will the campus be notified if the policies or terms of service change?

- Under what circumstances will a user be denied access to their own email by the provider?
- What guarantees are provided for response time and resolution time? (RFI #8)
- Are service outages reported to the campus? Is there a web page or other means by which end users and/or support personnel can monitor system availability and response? (RFI #12)
- What are the uptime reports for the previous six months (RFI #52)?
- Does the system provide reporting to verify that specific email messages were delivered to a specific individual mailbox? (RFI #3)
- Does the system provide reporting to verify that specific email messages were read by the specific mailbox account holder/recipient?
  Additional References:

Vendor contract (as applicable)	
Service level Agreement and Acceptable Use Policies	RFI #1
Availability/Uptime Information	RFI #8, #12, #52
Incident Management Procedures	RFI #8

Security

- Does the provider have a risk assessment program and information security policy to address those risks?
- Is there an information security function within the provider's organization? What are the responsibilities of that position?
- Are security roles and responsibilities defined and documented in accordance with the provider's information security policy?
- Is there a mandatory Acceptable Use Policy for the provider's employees? What is it?
- Does the provider have a security awareness training program? If so, who is required to complete security awareness training? Is this a one-time training event or is participation in the training on at least an annual basis?
- Does the provider have a disciplinary process for non-compliance with the security policy?

- When the provider engages with third-parties to provide components of the email service are those third-parties' security and privacy policies required to be "as stringent as" the provider's?
- What assurances, including standards, does the provider offer to the campus regarding the physical security of the location?
- Is there an independent audit function within the provider's organization? If so, describe the role of the audit function within the email service.
- Does the provider develop any portion of the application used to provide email service or administer that service?
    - Is this application development independently evaluated or certified by a third-party for security?
    - Does the application development process explicitly address the risks identified by the Open Web Application Security Project (OWASP) Top Ten?
    - Is there a software development lifecycle process for application development?

Additional References:

Information Security and Privacy programs, including responsible individuals	
Information Security Policies and Procedures	
Information Security audits/certifications	

Business Continuity

Given the extraordinary importance of email as the primary communication channel for campus users, unexpected interruptions in service pose a significant risk. The following questions evaluate the provider's ability to recover from such an interruption.

- Does the provider perform backups? How frequently? How long are they retained? Where are the backups stored? Are the backups encrypted? (RFI #56)
- Does the provider maintain a documented method that details the impact of a disruption?
- What are the RPO (recovery point objective) and RTO (recovery time objective) for services? Detail according to the criticality of the service.
- Are the same information security policies and procedures followed in the restoration process as in the normal operation of the service?

- What are the lines of communication to end customers in the event of a disruption?
- What is the line of management communication within the provider for the university in the event of a disruption?
- Is there a disaster recover and/or business continuity plan? If so, how often does the provider test disaster recovery and business continuity plans?
- Has the provider categorized the priority for recovery, and if so, what would be our relative priority to be restored?

Additional References:

BC/DR plans/practices	RFI #56

Information Security Incident Management and Response

To evaluate the capacity of an organization to minimize the probability of occurrence or reduce the negative impact of an information security incident, the following questions should be asked to a cloud provider.

- Does the provider have a formal process in place for detecting, identifying, analyzing and responding to information security incidents?
- Is this process rehearsed to check that incident handling processes are effective? Does the provider ensure, during the rehearsal, that everyone within the provider's support organization is aware of the processes and of their roles during incident handling (both during the incident and post analysis)?
- How are the detection capabilities structured?
- For how long are the security logs retained? Are those logs securely stored? Who has access to the logs? How are log events selected for review/investigation?
- How can the campus report anomalies and security events to the provider?
- How are incidents documented and evidence collected by the provider?
- Are incidents involving campus users or data reported to the campus by the provider? In what time frame?
- How many security incidents that resulted in unauthorized access to email communications has the provider experienced in the last year (excluding those that are a result of credential theft through phishing)?
- Besides authentication, accounting and audit, what other controls are in place to prevent (or minimize the impact of) malicious activities by insiders?

- Does the provider carry out vulnerability testing? How often and who performs it? Are the results shareable by the provider under an NDA?
- Does the provider carry out penetration testing? How often and who performs it? Are the results shareable by the provider under an NDA?
- Does the provider have documented procedures for notifying users whose Personally Identifiable Information has been compromised, per California state law?
    - If the compromise is a result of negligence on the provider's behalf, will the provider or the campus be responsible for this notification and related expenses?
- Does the provider agree to the data protection/breach notification requirements of UC's Appendix DS which was developed by the UCITPS for use in certain UC contracts?

Additional References:

Incident management procedures	
Data breach notification procedures	

Privacy

- What is the provider's information privacy program?
- Is there a change management process for this program? Will the campus be notified if the program changes before they are implemented?
- What is the company's privacy policy that covers the contents of an individual's account (RFI #58)?
- In what country is the provider's business organization located?
- Is the provider's infrastructure located in the same country or in different countries? Which countries?
- Will the provider use other companies whose infrastructure is located outside that of the provider?
- Where will the data be physically located? (RFI #59)
- Will jurisdiction over the contract terms and over the data be divided?
- Are privacy protections in the countries where data is physically located equal to or stronger than privacy protections in the U.S.?

- Are there users whose communications, because of their content matter, be subject to additional risk if their data is stored extraterritorially?
    - *Example:* It may be a risk to store communications of a faculty researching a politically sensitive topic on servers physically located in that country and under that country's jurisdiction.
    - If these users exist, how will their data be protected by the provider?
    - Are these users aware that this risk is also borne by the collaborators with whom they exchange email communications?
    - Will the provider inform the campus or user where their data is physically stored?
- Are communications monitored by the provider? If so:
    - For what purpose?
    - Can users opt-out of this monitoring?
    - Does the provider acquire users' consent? For inbound and outbound email traffic?
- Is stored email data mined by the provider? If so:
    - For what purpose?
    - Can users opt-out of this monitoring or analysis?
    - Does the provider acquire users' consent?
- Under what conditions will the provider use University information in order to target the users with advertising or other marketing (RFI #15)?
- Will demographic or personal information ever be transferred to a third party without the express written consent of the University, including browsing preferences collected by cookies on advertisements? (RFI #16)?
- When the provider engages with third-parties to provide components of the email service, are those third-parties' security and privacy policies required to be "as stringent as" the provider's?

Additional References:

Information Security and Privacy programs, including responsible individuals	RFI #58
Privacy policies/notices	RFI #58

Collection and use of information	RFI #15, #166
Storage/Data Centers	RFI #59

Third-Pary Requests/Access without Consent

- Under what circumstances will the provider access email content without the consent of the user?
    - What mechanisms are in place to facilitate this access? (backdoors, administrative tools)
    - Is the use of these tools audited and reported to the campus?
- Under what circumstances will the provider allow third-parties (business partners, contractors, government officials, law enforcement) to access email content without the consent of the user? (RFI #6, #65)
    - What mechanisms are in place to facilitate this access? (backdoors, administrative tools)
    - Is the use of these tools audited and reported to the campus?
- What administrative tools/access does the provider offer for the campus to access email content without the consent of the user?
- Does the provider offer evidence preservation services? (RFI #57, #64)
- Is the provider required to cooperate with UC in responding to e-discovery requests, subpoenas and court orders?
- What is the provider's process for complying with subpoenas and search warrants? (RFI #63)
- What are the time frames that the provider will agree to respond to legal requests?
- If the provider receives a subpoena or search warrant with a gag order, or a National Security Letter, will the campus or UC receive any notification prior to information being released?

Additional References:

Vendor contract (as applicable)	
Third-party requests procedure	RFI #65
Legal requests procedures (eDiscovery,	RFI #57, #63,

subpoena, warrant practices, e.g.)	#64
Administrative tools to access email	RFI #9, #64

Authentication, Authorization, Audit

- Can account creation and deletion be synchronized with local directory or identity management services? (RFI #5b)
- Do the authentication controls meet Campus minimum authentication requirements (e.g. password strength, length, etc.) (RFI #26)?
- Is two-factor authentication supported?
- What are the mechanisms for resetting authentications?
- Who is responsible for authorization controls?
- Does the service provide non-repudiation and if so, how?
- Are there different levels of authorization controls and are they flexible?
- Are there mechanisms to detect and report anomalous authentication attempts or account compromise? (RFI #60)
    - What are the provider's anti-spam/anti-phishing capabilities (RFI #28-30)?
- Does the audit capability provide a complete session profile, meaning that transactions can be audited through all of the infrastructure components (such as load balancers) back to an individual session?
- Is there an ability to identify which messages were accessed during a session? (RFI #13)
- How long are audit logs kept? Describe methods to protect the availability and integrity of audit logs.

Additional References:

Identity management/access control (authentication)	RFI #5
Password policies	RFI #26
Anti-spam and anti-phishing capabilities	RFI *28-#30
Account Compromise procedures	RFI #60

Provider Reputation/Peer Adoption

- In the past 12 months, have there been any regulatory or legal findings that are available regarding data security or privacy related to the provider? What are those findings?
- In the past 12 months, have there been other newsworthy stories related to this provider? What are those findings?
- Are peer institutions adopting this provider's services? What are the findings of satisfaction or concern?