Repositioning IT Status

Networking, Email and Calendaring, Data Center, and Applied Security

Working Document

Repositioning IT Objective:

The long term objective of the Repositioning IT initiative is to build the next generation of infrastructure services - email, network, security and data centers - within an integrated campus architecture that preserves and enhances high quality IT services and extends the same to the entire campus. Through appropriate campus design and where rationale exists to reduce replication, the initiative will consolidate network, email and data centers and improve overall security. Efficiencies gained through consolidation can be locally re-deployed or emphasized to support the direct IT needs of researchers, educators, students and the administrative staff who support them.

Strategy:

Engage, enable and build upon campus expertise to be helpful and solve existing problems. Look for opportunities (natural transitions, new buildings, technology refresh cycles) that marry practical, needed and meaningful work with initiative objectives.

Project Status:

Network

• Next Generation Network (NGN) teams formed around two applied pilot projects – Murphy Hall and CNSI (membership below)

Email

• UCLA eMail, Messaging and Calendaring System – service improvements and expansions over the past several years including the build out of an Exchange service (see Attachment 1 diagram)
• Current service components of UCLA Campus eMail, Messaging and Calendaring System part of TIF
• Eleven unit Exchange installations primarily within Business and Administrative Services converted to the UCLA Campus eMail, Messaging and Calendaring System; Ten units (both academic and administrative) in exploratory phases (see Attachment 3 schedule)

Data Center

• Analysis on-hold until Summer 2006
• Identified funding needed for the Math Science and CSNI Data Center improvements
Security

- Applied Security Task Force formed (membership below)
- IT Security Officer position posted - now accepting resumes
- Advanced Services Network white paper (www.csg.ucla.edu - February 2006 documents)

Funding

- Connected funding (2.1 M) that is part of the current TIF now aligned with Repositioning IT
  - Letter from EVC Neuman expected in March

Next Steps

NGN - Architecture and Service Design Team

- Create and fund campus internal network architecture and service design team; build out project management
- Create an internal and external advisory role

UCLA eMail, Messaging, and Calendaring System

- Develop campus roll-out strategy and plan
  - Quality Assurance Questions/FAQs (see Attachment 2)
  - Create schedule of potential and confirmed conversions
  - Clarification and augmentation of analysis and migration teams
    - One time funding to increase technical migration analysis and execution capacity under review
- Validate entire conversion protocol with two units Murphy Hall Summer Sessions in March 2006 and OIT-ATS in May 2006
- Work with “early adopter” units to better understand the functional requirements and service level agreements for individual units and campus roll-out
- Based upon confirmed conversions and timeframe and analysis of existing capacity build out technical migration and client analysis teams as appropriate
- Begin “opt-in” campus roll-out July 2006

Applied Security

- Integrate a IT security communications and tracking system for early alerts
- Create an authoritative web-site
- Re-engage the eEYE pilot and extend to Task Force member units to understand the software capabilities and experiment with reporting
- Announce ASTF along with the official distribution of minimum standards (March)
Internal Repositioning IT Teams

**NGN - Murphy Hall Project**
Mitra Ashtari, Student Affairs
Jeff Barnes, AIS
Martin Bjel, Registrar's Office
Mike Nguyen, College
Ken Davis, External Affairs
Chris Thomas, ATS
Mike Van Norman, CTS
Janice Bundy, CTS
Jon Phillips, CTS
Marsha Smith, OIT

**CNSI Project**
John Haghighi, Humanities
Mitra Ashtari, Student Affairs
Jeff Barnes, AIS
Max Kopelevich, Physical Sciences
Babak Saberi, Life Sciences
Steve Woods, Engineering
David Snow, School of Medicine
Ann Chang, Molecular and Medical Pharmacology
Jeff Barnes, AIS
Chris Thomas, ATS
Mike Van Norman, CTS
Marsha Smith, OIT

**Applied Security Task Force Members**
Ken Davis, External Affairs
Steve Woods, Engineering
John Haghighi, Humanities
Aaron Seligman, Social Sciences
Victor Mendez, School of Public Affairs
Andre Dieudonne, Anderson School
Cliff Maraschino, Graduate School of Education and Information Studies
Chris Thomas, ATS
Mike Van Norman, CTS
Kent Wada, OIT
Marsha Smith, OIT

**UCLA eMail, Messaging and Calendaring, Campus Roll-out Team**
Michael Schilling, CTS
Brent Gilmore, CTS
Esther Woo-Benjamin, OIT
Karen Ribback, OIT
Marsha Smith, OIT
Early Adopter Units (Summer Sessions, OIT-ATS, Library, Nursing and Dentistry)
Attachment 1 - UCLA eMail, Messaging and Calendaring System

UCLA eMail, Messaging and Calendaring System

Strategy

Client Interface Services
(Transition planning, Training, Help Desk)

BOL Current Services
- E-mail: including server-side filtering, calendaring, and task lists
- Spam identification
- Virus identification and removal
- Web-hosting services
- Network access: wireless, proxy, VPN, and dial-up
- Mailing lists
- News
- Anti-spyware
- Software and client support (integrated with residential program)
- Service-level agreements
- Client survey process

Future Planned Enhancements
- Cross-calendaring
- Affinity department naming
- Web mail interface for PDAs & cell phones
- Increased e-mail quota to 100MB
- Guest logon tool
- Bruin Kerberos
- Web hosting:
  - password-protected folders
  - database and scripting access
  - digital locker
  - Metrics/reporting process

Enterprise Exchange Current Services
- Email, calendaring, tasks, server side filtering
- Cross calendaring, calendar sharing, delegation
- Integrated directory
- PDA & smartphone connectivity
- Shared resources & folders
- AntiSPAM service options
- Storage
- Help Desk management
- Migration program
- Service-level agreements
- Client survey process
- Metrics/reporting process

Future Planned Enhancements
- Web-based monitoring tools
- Web-based applications/utilities
- Email archiving
- Fax services
- Offsite disaster recovery
- Integrated messaging

Managed Infrastructure
(Air, power, fire suppression, security, and Storage Area Network)
Operational Quality Assurance Questions
UCLA eMail, Messaging and Calendaring System

Overview/Design

1. For basic email and exchange services and back/up storage, please describe the design from a failure point analysis and expected system failover behaviors.
2. In what data centers do these operations reside? What are the security, operations, HVAC, power/UPS, back up power, fire protection, etc. capabilities of the data center?
3. Is there a disaster recovery plan?
4. How many mailboxes are active in the basic email system? How many are faculty/staff and how many are students? Please describe how calendaring is being used.
5. With respect to all Bruin mail services, what campus units are currently using which email services?
6. Do they support moving current email data from departmental system to central Exchange system? If so, how? PST export/import?
7. What is the default email domain for the central Exchange system? Will they support existing departmental email domains?
8. What encryption capabilities will be provided to protect communication of sensitive/confidential data to meet state and federal regulatory compliance requirements?
9. What is the expected cost per user?

Services/Policies and Procedures

Messaging Accounts

10. What are Mailbox size limits? How were they determined? Will there be different sizes for different categories of users? What mechanism will be used to limit resource consumption or to allocate scarce resources? What happens when users exceed quotas? What will be the procedure to get a quota increased?
11. What are email attachment size limits? Is there a way to “opt out” of the limitation?
12. Will reports be provided to departments on email utilization (# active accounts, size of accounts, etc.)?
13. How long will accounts remain active after employees leave? What will the procedure be to disable accounts?
14. Will dormant accounts be deleted? If so, what is the process?
15. What is the procedure to request consensual or non-consensual access to another person's email account?
16. Will passwords need to change on a regular basis?
17. Will there be 7/24 password resets? Will local support staff be able to do password resets for their own users?
18. What are the distributed management capabilities for local units? What is the SLA for account management (Create/Update/Delete)? What is the procedure (online request, email, etc.)?
19. What attributes are they capturing when creating new accounts (e.g. Phone Number, Office, Employee or University ID, Title Code, Dept. Code, Bargaining Unit, etc.). Which attributes are mandatory?
20. Will there be provision for user-less accounts for conference registration, admissions, etc.? What is the process for adding temporary accounts?
21. Will there be provision for accounts for non-employees (visiting scholars, contractors, etc.)?

**File Storage, Backup, Archival and Restorations**

22. Can accidentally deleted email be restored? How far back can email be restored? How long does it take to get an email restored? Will deleted email be removed from backups, if so how quickly?
23. Is message retention supported (i.e. after a message is deleted from the Deleted Items folder, can it be recovered using "Recover Deleted Items" option in Outlook)? If so, how many days are messages kept?
24. How will they verify their backups?

**Public Folders/Distribution Lists/Directory**

25. Will public folders/departmental accounts (Conference Rooms, General utility accounts, etc.) be supported?
26. Will there be support for distribution lists in the GAL? Can external addresses be added to the GAL?
27. Are there plans to synchronize Active Directory with any other databases (e.g. Employee/Payroll database, campus directory, etc.)?

**Spam Identification/Virus Detection and Removal**

28. Will there be spam protection? If so, how will it be implemented (quarantine, black lists, etc.)?
29. Virus checking, spam filtering and blacklisting have all caused problems in conducting University business. Will there be a way to “opt out” of these services (at the account level)?

**Support and Licensing for Desktop, Laptop and Mobile Devices**

30. Many units already have Exchange “CALS”, will they be given credit for these if they “opt in” to the service?
31. Will PDAs be supported? Which ones? How many are being supported now? Will support include ‘front end’ as well as server support?
32. How will adoption of new devices be evaluated and decided upon?

**On-Campus/Remote Access**

33. What protocols will be supported for mailbox access (MAPI, POP3, IMAP, HTTP/HTTPS) from within UCLA?
34. What protocols are supported remotely (i.e. is VPN required)?
35. Will Outlook Web Access (OWA) be supported? If so, is SSL required? (The Change Password option of OWA does not work if SSL is not used.)
Enterprise Messaging Support

Standard Operational Support/Trouble Reporting/Incident Response

36. What are the maintenance and support contracts in place for these systems especially in terms of contracted response?
37. What is the monitoring and operations support structure for these systems – what constitutes 24/7 monitoring and support?
38. What will be the relationship between the BOL and Exchange Helpdesks? Will the BOL helpdesk be expanded to cover the Exchange service or will a new helpdesk be created?
39. What is the support structure established between the client support staff and BOL email operations team? This question is about how exactly you have structured the support relations, communications, etc to ensure an SLA. Who contacts who and how? How is this currently working?
40. How will the local support organizations interact with the Exchange helpdesk? Will the faculty get “preferential treatment”?
41. If central email goes down, how are you going to notify the UCLA community of problems?

Service Levels

System Integrity/Equipment Maintenance and Upgrades

42. What have been the planned and unplanned downtimes for the basic email services over the past year? What is its calculated availability? Is there a scheduled downtime for maintenance (reboot, online defrag, patches, etc.)? If so, what frequency?
43. From the point that the service stabilized, what have been the planned and unplanned downtimes for the exchange services. What is its calculated availability?
44. What have been the planned and unplanned downtimes for the PDA services?
45. How is security managed? How will patch management be managed?

Metrics

46. What are the results of user surveys formal or informal in units that have converted to the campus service?
47. For all of the services, what are the industrial practice benchmarks that you have used for service design? Especially for basic email and exchange services, what are the actual performance metrics with reference to these practice benchmarks?
48. Will there be metrics kept (e.g. worst case latency) on the timely delivery of email?
## Status

<table>
<thead>
<tr>
<th>Status</th>
<th>Group</th>
<th>Potential Numbers</th>
<th>Type of Conversion</th>
<th>Potential Conversion Date</th>
<th>Exploration</th>
<th>Introductory Meeting</th>
<th>Dept. Questionnaire</th>
<th>Functional Gap Analysis</th>
<th>Technical Mtg</th>
<th>Decision To Proceed</th>
<th>Training</th>
<th>Pre-Cutover Meeting</th>
<th>SLA</th>
<th>Migration</th>
<th>Completed</th>
<th>Post Migration Meeting</th>
<th>Conversion Followup</th>
<th>SLA Addendum Followup</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIT Status and Action Plan.doc - P1407 - 3/29/06 8 of 8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>