AGENDA

1. (2:00-3:00): Online Education Project (John Mamer/Jim Davis)  
   [Status: Endorsement Context]

2. (3:00-3:05): Approval of October 28, 2011 Meeting Summary

3. (3:05-3:15): Policy on Online Voting & Vote on Policy 403 (Jerry Kang)

4. (3:15-3:30): Faculty Digital Presence (Jackie Reynolds)  
   [Status: Update]

5. (3:30-3:45): Wireless in Classroom (Mark Bower)  
   [Status: Information]

6. (3:45-3:50): Next meeting and adjournment (Jerry Kang)
Information Technology Planning Board  
Meeting Summary  
Friday, October 28, 2011  
Faculty Center – Redwood Room

ITPB Attendees:  Julie Austin (for Tom Phelan), Jim Davis, Jonathan Furner, Jerry Kang, Sara Kim, Christopher Lee, Chon Noriega, Susan Parker (for Gary Strong), Jack Powazek, Linda Sarna, Vincent Riggs, John Riley, Guy Rodgers, Joseph Rudnick

Michelle Chen, recorder

Absent:  Dana Cuff, Deborah Estrin, Franklin D. Gilliam, Jr., Jonathan Kuo, John Mamer, Warren Mori, Neil Netanel, Janice Reiff

Invited Guests:  Julie Austin, Arash Naeim, Kristina Sidrak

Resources:  Ross Bollens, Larry Loeher, Jackie Reynolds, Libbie Stephenson, Kent Wada, Andrew Wissmiller

Chair Jerry Kang called the meeting to order at 9:07 AM.

Agenda Item #1: Introduction of New Members and Approval of June 20, 2011

The summary from the June 20, 2011 meeting was approved.

Agenda Item #2: ITPB Orientation (Jerry Kang)

Jerry gave a brief introduction of the role that ITPB plays in IT Governance at UCLA. The ITPB is a committee appointed by both Administration and the Academic Senate. It is the primary governance and oversight body for information technology, and was created in part to be the one-stop shop for high level faculty and administrative vetting for strategic-based decisions in IT policy.

There are two other major groups in IT Governance: CITI and CSG. CITI members are appointed by the EVC alone, and the group makes recommendations on how money is used for infrastructure and investments. Gary Strong and Steve Olsen are co-chairs of that committee. CSG is a systematically selected group that is made up of the directors of IT in every box on the university org chart. They provide ITPB with expert technical advice that helps ITPB make better decisions.

ITPB members will be provided via email with a PDF containing meeting materials prior to all meetings and the Board will try to do voting online if the issue is not too complex. However, the option of bringing the item to an actual meeting is always available.
Agenda Item #3: Payroll Personnel System (Jack Powazek)

The materials associated with this item can be found at:

The UC Payroll Personnel System Initiative is a UC-wide project, and affects all staff and faculty, the medical center, and ASUCLA. This project is part of the UC “Working Smarter” initiative. The project began October 2011, with the intent to go live in January 2013. However, if the system is not ready to go live at this date, the project would rather delay the deadline than have a non fully-functioning system.

In this initiative, there will be a single payroll system for the campuses. PeopleSoft/Oracle has been selected as the vendor for the system. UCLA has volunteered to be a part of first implementation wave, which means we will have more of a say in the process. The new paradigm for providing individual support only deals with issues regarding pay and personnel (transaction processing), and does not deal with higher level HR issues such as employee relations and benefits counseling. This support will still be handled at the local level.

One implication for faculty that was discussed is that someone within each department, whether it is the faculty or an administrator, will need to indicate that a faculty member needs to be paid every month in order for the faculty member to receive a check.*

*Update from Allison Baird-James: “Subsequent to the meeting, we are working on providing more appropriate options for faculty time and attendance. We should have a firm answer within a month or so.”

Faculty who have questions or concerns can bring them to their CSG representative (http://www.csg.ucla.edu/people/) who will work with the implementation team to figure out a suitable solution.

This topic will be brought to ITPB again for future updates.

Agenda Item #4: Outsourcing Email/Collaboration Tools (Julie Austin)

This is a topic that has continued from the previous meeting. The materials associated with this item can be found at:

Julie Austin has been in charge of the Email Outsourcing Task Force since 2009. The task force produced a report in April 2011 with the recommendation to outsource student and alumni email to Google. Julie presented the report and recommendations to ITPB in June 2011, and the ITPB requested more information before it could make a decision.
Over the summer, three groups were created to analyze the risk with respect to legal/security/privacy, student risk, and implications for implementation:

The result from the Student Assessment is that the students still want us to go to Google Apps for Education.

The Institutional Assessment was concerned that Google has their facilities in different countries, so there might not be the same data protection policies as the United States. Also, outsourcing to Google violates the ECP, because for alumni, Google will scan through emails and display targeted ads. However, Legal stated that this is not a relevant issue for students in their capacity as students. It was recommended that UCLA develop a policy for faculty and staff stating that they cannot use Gmail for research and educational purposes because no one has assessed the risk for these uses, and that students cannot use Gmail in their capacity as staff.

For the Implementation Assessment, the biggest issue is that UCLA would need to give students a new domain name. It was suggested that the domain name be: @bruins.ucla.edu. The plan for outsourcing would include all Google Apps, but the university would only provide help desk support for email and calendaring. All other questions will be directed to Google or local departments.

An additional consideration that was discussed among the groups was the implications for faculty and staff if UCLA were to outsource student email. The groups believe that faculty and staff will also want to go to the cloud, and recommend developing a policy on what is acceptable for faculty and staff use. In conjunction, the groups should also begin the process of investigating and evaluating options for faculty and staff use of the cloud in a way that is secure and meets university requirements. There is a UC-level RFP that is looking into private and public cloud solutions for faculty, staff, and health system email.

**Action Item: Motion passed to endorse outsourcing email and collaboration tools to Google for undergraduate students, alumni, and retirees.**

The Implementation team now needs to put together an implementation plan and timeline. This topic will be brought to ITPB again for future updates.

**Agenda Item #5: Research Informatics Planning Initiative (Jim Davis)**

The materials associated with this item can be found at:

UCLA is proposing to start a process focused on strategic planning for research informatics. There will be a multi-phased approach, and Deans of each school and the Academic Senate will recommend faculty to participate in the planning process.

This topic will be brought to ITPB again for future updates
Agenda Item #6: Next meeting and adjournment (Jerry Kang)

The meeting was adjourned at 11:03 AM.
Policy for Online Voting

At their discretion, the Chair and Vice-Chair may decide to conduct an endorsement vote online. Members will receive electronic notice of the vote and have 2 weeks to respond. One of the voting options will include a request to bring the item to a future meeting for further discussion.

A quorum is considered to be one more than half of the number of voting members. ITPB currently has 22 voting members, so 12 online votes are needed for a quorum to be reached.

If a quorum is reached, then the result of the vote will be announced at the next meeting. If a quorum is not reached, the matter will be brought up at the beginning of the very next meeting for an expeditious vote.
IT Governance
Committee Review and Recommendation

**Desired Change:** Approval of this policy will establish Security Standards for the UCLA Logon Identity for anyone assigned a UCLA Logon ID/password and for service providers furnishing services to someone assigned a UCLA Logon ID/password.

**Why:** These standards serve to protect students, faculty, staff, and guests, the university’s electronic resources, and resources outside the UCLA campus. This policy identifies those with principal responsibility for compliance with the standards, and for the enforcement of this policy, including taking corrective action.

**Recommendation:** Approve Policy 403, such that users must ensure their password remains a secret known only to them. If it is determined that a password has been shared, the UCLA Logon ID will be considered compromised and may be suspended.

---

**Driving Forces**
(Those which currently exist & support or drive the desired change)

For Students, Faculty, Staff, and Guests:
1. Improved security for the campus
2. Reduced ability for passwords to be misused or unknowingly stolen
3. Clearer rules on logon/password usage

For Service Providers:
1. **Approval:** Must be approved to offer electronic resources to someone with a UCLA Logon Identity.
2. **Interfaces:** Must use authentication interfaces, services, and processes only for their intended purposes.
3. **Proxies:** Must not function as an authentication proxy by collecting UCLA Logon Identities and passwords and forwarding them on to another authentication interface.
4. **Storage:** Must not save authentication information on permanent storage.
5. **Retransmission:** Must not retransmit authentication information.
6. **Masquerading:** Must not masquerade as an official authentication interface such that a user might confuse it with an official interface.
7. **Degradation:** Must not degrade the level of security once someone has identified themselves using a UCLA Logon Identity.

**Restraining Forces**
(Forces that may inhibit the implementation of the desired change.)

1. Applications that use UCLA Logon IDs to authenticate users must install SSL certificates. (Mitigation: Certificates are free to any UCLA organization.)
2. A few applications that currently cache UCLA Login ID credentials must be changed. (Mitigation: MyUCLA’s use of credentials becomes unnecessary in moving to Google Apps Educational Edition.)
3. A few applications need to be changed to allow for 3rd party access. (Note: The applications need to be identified.)
4. Faculty and managers who currently delegate work by giving their logon and password access credentials to someone else will need to change that practice and use official 3rd party access procedures.

---

**Actions To Be Taken:**

1) Define the desired change or action (agree on a simple statement).
2) Brainstorm the driving forces & restraining forces (identify the critical few)
3) Rank the driving forces & restraining forces based on the strength of the force (5 = strong, 1 = weak)
4) List actions to be taken (focusing on the critical few driving & restraining forces)
I. REFERENCES
1. UC Business & Finance Bulletin IS-3, Electronic Information Security;
2. UCLA Student Conduct Code;
3. UCLA Policy 401, Minimum Security Standards for Network Devices;
4. UC Electronic Communications Policy.

II. INTRODUCTION AND PURPOSE
Students, faculty, staff, and guests may be assigned a UCLA Logon Identity (UCLA Logon ID or Logon ID). The Logon ID and associated Password electronically identify an individual, which can be used to obtain access to campus electronic services or resources that are restricted to UCLA. For example, a student’s Logon ID gives access to his or her student records, class schedules and course web sites, billing information and electronic mail among others resources. A faculty member’s Logon ID gives access to his or her class grade books and profile in atmysenate.ucla.edu among others. The Logon ID also satisfies the standards of the InCommon Federation and the University of California’s UCTrust, and can therefore be used to identify an individual as a member of the UCLA community and thus to gain access to electronic resources outside of UCLA.

UCLA encourages the use of its electronic resources in support of the University’s mission. The UCLA Logon ID is an important element of maintaining the security of these resources and must be properly protected to safeguard against unauthorized access. UCLA reserves the right to suspend or deny access to its electronic resources, including Logon IDs, which do not meet its standards for security.

The purpose of this policy is to establish Security Standards for the Logon ID and assign responsibility to both users and Service Providers for the proper use and safeguarding of Logon IDs. The standards serve to protect members of the UCLA community, the University’s electronic resources and electronic resources beyond the campus that accept Logon IDs for authentication.

This policy is applicable to:
- anyone assigned a Logon ID and password; and
- all Service Providers as defined in Section III, Definitions.
III. DEFINITIONS

For the purposes of this Policy, the following definitions apply:

**Authentication** means the process by which an individual electronically identifies themself and/or as a member of the UCLA community through use of a UCLA Logon ID and associated Password.

**Service Provider** means a campus unit or external entity that, with approval, grants access to electronic services or resources based on UCLA Logon ID Authentication.

**Password** means a string of letters, numbers and/or special characters.

**UCLA Logon ID (Logon ID)** means a string of letters, numbers and/or special characters that uniquely identifies a UCLA student, faculty, staff or guest eligible to be assigned a Logon ID.

IV. STATEMENT

A. Holders of a UCLA Logon ID

Individuals assigned a UCLA Logon ID must ensure their Password is kept secure. Disclosure of a Password to any other person is a violation of this Policy and of UC Business and Finance Bulletin IS-3, Electronic Information Security. If it is determined that a Password is known to someone other than the holder of the Logon ID, whether shared intentionally or obtained maliciously, the Logon ID will be considered compromised and may be disabled at the discretion of the Director, IT Security. A student in violation of this Policy may also be in violation of the Student Conduct Code and be subject to discipline by the Dean of Students Office.

B. Service Providers

Logon IDs are encouraged as the Authentication mechanism for access to campus web applications and other electronic services and resources. Service Providers whose applications are designed to accept Logon IDs must comply with the Security Standards for UCLA Logon Identity in Attachment A, including:

- being approved by the Director, Middleware Services, prior to accepting Logon IDs;
- using the associated Authentication interfaces, services, and processes only for their intended purposes; and
- not proxying, storing or retransmitting Authentication information.

A Service Provider found to be in violation of this Policy may have access blocked to the non-compliant service or resource at the discretion of the Director, IT Security.

A Service Provider may, for a specific electronic resource or service wanting to use the Logon ID for Authentication, request an exemption from one or more of the Security Standards for UCLA Logon Identity. Such requests must be made in writing to the Director, IT Security; any requests that are granted do not exempt the Service Provider from any Standards not so exempted. All requests and outcomes will be kept on file by the Director, IT Security for as long as the granted exemption exists.

C. Recourse

Appeals concerning decisions made or actions taken by the Director, IT Security, or the Director, Middleware Services, can be made to the Associate Vice Chancellor, IT Services, who will consult with other campus officials, as appropriate, to make the final determination.
V. ATTACHMENTS
   A. Security Standards for UCLA Logon Identity (Service Providers).

   Issuing Officer

   /s/ Andrew Wissmiller
   Associate Vice Chancellor, IT Services

   Questions concerning this policy or procedure should be referred to
   the Responsible Department listed at the top of this document.
ATTACHMENT A

Security Standards for UCLA Logon Identity (Service Providers)

All Service Providers must comply with the following Security Standards for UCLA Logon Identities. A Service Provider must:

Approval
be approved by the Director, Middleware Services prior to offering access to electronic services and resources based on UCLA Logon Identity Authentication.

Interfaces
use Authentication interfaces, services, and processes only for their intended purposes. The official Authentication interfaces are:

- **Shibboleth**: Shibboleth is UCLA’s web single sign-on interfaces. Web applications leveraging Logon ID credentials must integrate with Shibboleth.
- **RADIUS**: RADIUS is available for departmental network applications in certain limited circumstances. Applications are evaluated at the time of request for compliance with Logon ID and network standards.
- **Kerberos**: Kerberos is a trusted third-party authentication mechanism available in certain limited circumstances. Applications making use of the Kerberos framework are evaluated at the time of request for compliance with Logon ID and application security standards.
- **Active Directory**: Active Directory authentication services allow campus computing labs to leverage the Logon ID and provide a single sign-on environment. Applications making use of the Kerberos framework are evaluated at the time of request for compliance with Logon ID and application security standards.

Institutional communications services (e.g., POP or IMAP) may make use of the above and additional internal interfaces to meet technical requirements of certain communications protocols.

Proxies
not function as an Authentication proxy by collecting UCLA Logon Identities and passwords and forwarding them on to another authentication interface.

Storage
not save Authentication information on permanent storage.

Retransmission
not retransmit Authentication information.

Masquerading
not masquerade as an official Authentication interface such that a user might confuse it with an official interface.
Degradation

not degrade the level of security once someone has identified themself using a UCLA Logon Identity. UCLA Policy 401 mandates that all authentications be encrypted, therefore, once a Service Provider has Authenticated an individual using a UCLA Logon Identity, they must maintain encrypted communications with that UCLA Logon Identity.