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 Logon 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)
UCLA Policy 403  UCLA Logon Identity Security Standards

Issuing Officer:  Associate Vice Chancellor, Information Technology Services
Responsible Dept:  Information Technology Services
Effective Date:  TBD
Supersedes:  New

I. REFERENCES
II. INTRODUCTION AND PURPOSE
III. DEFINITIONS
IV. STATEMENT
V. ATTACHMENTS

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 atmynsenate.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.