UCLA Policy 403 UCLA Logon ID Security Standards

Issuing Officer:	Associate Vice Chancellor, Information Technology Services
Responsible Dept:	Information Technology Services
Effective Date:	April 20, 2012
Supersedes:	New

I. REFERENCES

1. UC Business & Finance Bulletin IS-3, Electronic Information Security;
2. UCLA Policy 401, Minimum Security Standards for Network Devices;
3. UC Electronic Communications Policy.

II. INTRODUCTION & PURPOSE

Students, faculty, staff, and guests may be assigned a UCLA Logon ID by the Campus Credential Provider, Information Technology Services. The UCLA Logon ID and associated password serve to electronically identify an individual, enabling access to campus electronic services or resources that are restricted to that individual or to the UCLA community. For example, a student's UCLA Logon ID gives access to his or her student records, class schedules and course web sites, billing information and electronic mail among other resources. A faculty member's UCLA Logon ID gives access to his or her class grade books and profile in "https://senate.ucla.edu,"or to electronic journal subscriptions available to the UCLA community through the UCLA Library.

The UCLA 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 eligible to gain access to electronic resources outside of UCLA.

The purpose of this policy is to establish Security Standards for the UCLA Logon ID and assign responsibility to both users and Service Providers for the proper use and safeguarding of UCLA 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 UCLA Logon IDs for Authentication. This policy is applicable to:

- anyone assigned a UCLA 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.

Campus Credential Provider means UCLA Information Technology Services, which is responsible for issuing a UCLA Logon ID to an eligible UCLA student, faculty or staff member, or other campus visitor when requested in order to access electronic services or resources, and managing Authentication and electronic identity information for the UCLA campus.

Service Provider refers to a specific campus unit that hosts certain campus electronic services or resources and, with approval of the Campus Credential Provider, grants access to such services or resources by means of UCLA Logon ID Authentication. A Service Provider may also be an external InCommon or UCTrust organization that accepts UCLA Logon ID Authentication to grant access to its services or resources to members of the UCLA community.

UCLA Logon ID means a unique username issued by the Campus Credential Provider to an eligible UCLA student, faculty or staff member or other campus visitor for use in accessing certain restricted electronic services and/or resources.

IV. STATEMENT

A. Holders of a UCLA Logon ID

Any individual assigned a UCLA Logon ID by the Campus Credential Provider becomes the Holder of the UCLA Logon ID and the associated password. The Holder is responsible for ensuring that such credentials are kept secure to prevent any unauthorized access to electronic services or resources. Disclosure of a UCLA Logon ID password to any other person except as may be permitted by UC Business and Finance Bulletin IS-3, Electronic Information Security, or the University Electronic Communications Policy, or any successor University policies, is a violation of this Policy.

A UCLA Login ID whose password becomes known to someone other than the assigned Holder or other authorized person will be considered compromised. A Holder of a UCLA Logon ID who suspects that the Holder's password has become compromised is required to change the password, or report the suspected compromise to the Campus Credential Provider who may disable the UCLA Logon ID. A UCLA Logon ID may also be disabled for security purposes at the discretion of the Director, IT Security. UCLA reserves the right to suspend or deny access to its electronic resources, including UCLA Logon IDs, which do not meet its standards for security.

B. Service Providers

A UCLA Logon ID is encouraged as the Authentication mechanism for access to campus web applications and other electronic services and resources. Use of UCLA Logon ID Authentication must first be approved by the Campus Credential Provider. Applications designed to accept UCLA Logon IDs must comply with the "Security Standards for the UCLA Logon ID (Service Providers)" in Attachment A, including:

- 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 for security purposes at the discretion of the Director, IT Security.

A Service Provider may, for a specific electronic resource or service wanting to use the UCLA Logon ID for Authentication, request an exemption from one or more of the Security Standards for the UCLA Logon ID. Such requests must be made in writing to the Director, IT Security; any such request that may be granted does not exempt the Service Provider from complying with all other Security Standards. Any appeals concerning decisions made or actions taken by the Director, IT Security, or by Information Technology 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 the UCLA Logon ID (Service Providers).

Issuing Officer

/s/ Andrew Wissmiller

Associate Vice Chancellor,
Information Technology 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 the UCLA Logon ID (Service Providers)

All Service Providers must comply with the following Security Standards for the UCLA Logon ID.

Degradation

A Service Provider must not degrade the level of security once a UCLA Logon ID user has been Authenticated. As required by UCLA Policy 401, all Authentications must be encrypted. Once a Service Provider has authenticated an individual using Shibboleth or any other Authentication interface, the Service Provider must maintain an encrypted session with that UCLA Logon ID.

Interfaces

A Service Provider must use Authentication interfaces, services, and processes only for their intended purposes. The official Authentication interfaces are:

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

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.

Masquerading

A Service Provider must not masquerade as an official Authentication interface such that a user might confuse with an official interface.

Proxy

A Service Provider must not function as an Authentication proxy by collecting UCLA Logon IDs and passwords and forwarding them on to another authentication interface.

Retransmission

A Service Provider must not retransmit Authentication information.

Storage

A Service Provider must not save Authentication information on permanent storage.