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.