Account Authentication Standard

University at Albany User Account Authentication Requirements

I. Authentication options for software systems hosted within the University network

A. Identifiers

1. The University uses one primary identifier for use by all University systems as the basis for user authentication for all established University community members. This identifier is created by a system operated by the University At Albany's Division of Information Technology Services (ITS). Within the University community, this identifier is called the “NetID”. University management processes ensure that NetIDs are never reused. The NetID is an alphanumeric string of varying lengths.
2. A person's University at Albany email address can also serve as an acceptable identifier.

B. Authentication Methods

The University makes available three authentication methods, which are listed in order of preference. If an application supports Web SSO it must be used.

1. Web SSO authentication via Shibboleth
    a. Web SSO is the preferred authentication method for applications within the University network. If an application supports Shibboleth, it is required to use it, unless the service has been granted an exception by the CISO. Single Sign-On is most effective if it is adopted by the largest number of applications. It is also a more secure method of handling the NetID and password since the application itself never sees it.
    b. Web SSO provides two-factor, which provides a greater level of security.
    c. New applications must operate within this Web SSO environment. If the standard product cannot operate in this way, an exception request must be submitted to the CISO along with a rationale about why this product is the preferred solution.
2. Active Directory authentication
    a. The definition of the central Active Directory schema is managed by ITS.
    b. Schools and divisions may not operate a dedicated AD Domain or Forest for authentication.
    c. The application software must not require superuser or write access to the Active Directory in order to authenticate users and retrieve attributes.
    d. All connections to Active Directory must be completed in a secure fashion, using SSL or something that provides a comparable security level.
3. LDAP authentication via 389
    a. Access to LDAP Registry authentication services are by request only and are limited to specific application credentials at specific IP addresses. Anonymous binding to the LDAP Registry is not supported.
    b. Connection to the LDAP Registry must be over an LDAPS (SSL protected) protocol link.
    c. The definition of the LDAP Registry schema is managed by ITS and extension to accommodate additional data elements is reviewed on a case-by-case basis.

II. Authentication requirements for services outside the University network.

1. The University and the Solution Provider will determine a secure access identity infrastructure process for the solution, including a unique login identity and password that is encrypted in storage and at rest for account users. When possible, this should always be the University NetID. The University and Solution Provider will determine the best practices for issuing login accounts, password attributes, password resets, and other access identity management processes using standard industry practices for security and privacy, with the University solely responsible for the final solution decision.
2. The University requires that the proposed solution meet University identity access management standards. Login processes can authenticate using one of the following methods.

    a. Single Sign-On for InCommon Federation,
    b. Shibboleth IDP Version 3.3x or higher

> **Preferred Authentication**
>
> Solution Provider must indicate whether the firm is a member of the InCommon Federation. If not a member of InCommon, describe the login management process using Shibboleth Version IDP 3.3.x or higher.

3. If none of the preferred processes are feasible, the Solution Provider must submit a detailed description of the proposed process. If the Solution Provider is providing identity access accounts for the solution, they must supply a unique login identity and password that is encrypted in storage and at rest. Solution Provider will manage issuing login accounts, password attributes, password resets, minimum password length, password generation guidelines, password expiration, and other access identity management processes using standard industry practices for security and privacy. The description should include details about the following processes:

    a. Creating new accounts
    b. Suspending accounts for temporary security reasons
    c. Terminating accounts
    d. Password resets
    e. Password security protocols
    f. Name changes

The Solution Provider is required to change system default and system administration passwords on implementation, and regularly thereafter following standard security best practices.

III. General statements about personal information, security and privacy

Regardless of the method of authentication, applications may have need for additional information about the user for authorization decisions and customization of the user experience. This information is housed in PeopleSoft, with subsets mirrored in our LDAP Registry database and the Active Directory domain. This information is considered private and access to it must be specifically requested and granted to the application. Please see the link to our Approved InCommon Attribute Release Policy

Due to government regulations, the University closely monitors how information is collected, stored, exposed, and used in its academic, research, and administrative processes. This affects the use of software systems in at least the following ways:

a. If a database holds relevant demographic information for a person, an application should request access to and retrieve that information when it is needed. If the application must store the information, it must be done in a way in that meets current security standards.
b. Depending upon the demographic information requested, the application may have to conform to the University privacy policies about how data is exposed to classes of users or the Internet at large. Determination will be made when access to the information is requested.
c. Information collected by the application within its intended function may fall under governmental regulation. In this case, the University may have specific operational and audit requirements.
d. The application Service Owner is responsible for providing detailed information on request about what information the application has access to and stores.

For any new or modified/upgraded applications that do not meet the requirements stated above, an exception must be requested by contacting the ITS Identity and Access Management Group.

This Standard is in support of the CIS Critical Controls.