UF UNIVERSITY of FLORIDA
Information Technology

Standard: Identity Management Service Provider Standard

Purpose:

To establish requirements for services that make use of the university's central identity registry to perform authentication and authorization that will ensure the security and integrity of identity information.

Scope:

Any Service Provider that uses information from the central identity registry to authenticate and authorize users. Examples of technologies that incorporate information from the central identity registry for use by Service Providers include: Shibboleth, UF Active Directory, UF LDAP, and UF Kerberos. A Service Provider in this context is an application or web site that is authenticated by using the GatorLink account and password credentials.

Standard:

1. Service Providers must never commit user passwords to persistent storage.
2. Shibboleth is the preferred authentication and authorization technology for web applications.
3. Inclusion in the central identity registry provides no assurance of a person's standing with the university. Authentication of credentials should be augmented with authorization assertions.
4. Service Providers should use appropriate authorization techniques and attribute assertions available from the UF identity provider to verify that users are eligible to access the provided resources. Examples include checking level of assurance, affiliations, granted roles or group memberships.
5. Service Providers should not use any login screen that is not provided by the central identity provider at UF. Exceptions to this may be granted after review of a Service Providers specific situation. Requests for exceptions can be made to the Identity & Access Management Office.

References:

Identity Management Policy

Procedure for requests exceptions: http://identity.it.ufl.edu/technical/gatorlink-authentication-setup-request/request-exception-to-identity-management-service-provider-standard/

NIST 800-63 Electronic Authentication Guideline

InCommon Identity Assurance Profiles (Bronze & Silver) 1.1

Federal Identity, Credentialing and Access Management Trust Framework Provider for Adoption Process (TFPAP) For Levels of Assurance 1, 2, and Non-PKI 3 Version 1.0.1

Revision History:

November 6, 2014: Specified handling of requests for exceptions, added link in reference section.