Information System Account, Identity, and Authentication Management

OVERVIEW

The discipline of information systems security relies on the practice of controlling access between information system users and digital resources. Controlling access generally relies upon establishing an identity (e.g., user ID) for each information system user and device. Identity information, in conjunction with some form of authentication, is used as the basis for determining whether each individual access request for a digital resource has been authorized.

Information system security depends upon authentication information being kept secret. The proper provisioning, use, and protection of identifier and authenticator information is fundamental to an organization's defense against unauthorized access to digital resources.

User identifiers are typically tied to user accounts. The user account holds a record of all of the access privileges which are currently authorized for that user. User accounts and access privileges must be managed diligently to ensure that only authorized access to digital resources is allowed.

See *BPPM* 87.01 for definitions related to this section. See also the Role-Based Access Control Standard, Tier Based Administrative Standard, Account and Identity Management Standard, Authentication Management Standard.

Purpose

This policy is intended to reduce the risk of unauthorized access to information resources at Washington State University (WSU) by:

- Establishing minimum identification and authentication requirements for all WSU information systems;
- Establishing minimum requirements for authorization, provisioning, and deprovisioning of information system user accounts and access privileges; and
- Ensuring that sound and secure identification, authentication, and access management practices are consistent University-wide.

Scope

This policy applies to all institutional business units, workforce members, and institutional information systems that collect, store, process, share, or transmit institutional data.

Information System Account, Identity, and Authentication Management

POLICY

The Office of the Chief Information Officer (CIO) is authorized to create, distribute, and maintain institutional accounts, identifiers, and authentication credentials for authorized institutional information system users for the purposes of:

- Enabling and supporting University mission and business objectives, and
- Protecting institutional user accounts, identifiers, authenticators, and information resources.

Institutional information system users may be organizational users (i.e., faculty, staff, and students) or non-organizational users (e.g., alumni, business partners, vendors, contractors, customers, and other third-party affiliates),

Where operationally feasible, information systems must leverage centralized account, identity, and authentication management systems and processes. This may include federation with external identity providers through central WSU account, identity, authentication, and access management services.

Information owners are accountable for developing appropriate procedures for the implementation of this policy.

Information owners must develop procedures to implement this policy (*BPPM* 87.05) in a reasonable amount of time, not to exceed 12 months after this policy goes into effect.

Institutional information systems must uniquely identify and authenticate institutional information system users, or processes acting on their behalf.

Activities associated with the monitoring and use of information system user and/or device accounts, identifiers, and authenticators are subject to monitoring and logging in accordance with WSU auditing, logging, and monitoring policies and standards.

Account and Identity Management

The following requirements apply to account and identity management:

Account Types

Institutional, business unit, and information system owners must identify and assign the appropriate types of information system accounts to support the mission and business functions of organizations that are applicable to their respective areas of responsibility.

Information System Account, Identity, and Authentication Management

Account Types (cont.)

Account types may include:

- Individual user;
- System (privileged);
- Service;
- Customer;
- Vendor;
- Contractor; or
- Other third-party affiliates.

All information system accounts are associated with a human-based account, a business process, or a business owner.

Shared Accounts and Generic Identifiers Prohibited

Shared information system user accounts or the use of generic user identifiers are prohibited.

Information Owner Authority

The appropriate business unit head or their designee gives information system owners the authority to create, manage, and maintain information system accounts and identifiers that are appropriate for their organization and their areas of responsibility.

User and Group/Role Membership and Access

The information system owner and/or data custodian must specify the following as appropriate for each information system they are responsible:

- Authorized users;
- Group/role membership; and
- Access authorizations.

Conditions for group/role membership must be established and documented.

User and Group/Role Identifiers

The information system owner or appropriate information system manager must select and assign identifiers to authorized information system users and groups/roles.

Standard Management Processes

Information system owners must create standard processes for their respective areas of responsibility for:

- Auditing and monitoring the use of information system accounts;
- Disabling information system accounts (with their associated identifiers); and

Standard Management (cont.)

- Notifying affected institutional information system owners when an institutional information system user:
  - Is terminated;
  - Is transferred;
  - Has a change of responsibilities and/or privileges; or
  - Is no longer required.

Access Requirements

Access to institutional information systems and services must e based on:

- A valid access authorization request;
- The intended system usage; and
- Other attributes as required by the organization based on the institutional or business unit mission and business need.

Periodic Review

Information system owners and/or data custodians are to review no less than annually all accounts and associated access rights for information systems under their responsibility.

Authentication Management

The following requirements apply to authentication management.

Authenticator Content and Verification

The Office of the CIO must define authenticator content and requirements for verifying institutional information system users. Individual authenticators may include the following to authenticate information system user identities:

- Passwords;
- Tokens;
- Passcodes;
- PINs (personal identification numbers);
- Biometrics; or
- Digital certificates.

In cases where multi-factor authentication is required, at least two of the factors used in the authentication method must be of different factor types.

Authentication Credentials

An information system user's authentication credentials must be assigned by the appropriate institutional or business unit Information Technology Services (ITS) department. When initial and replacement authentication credentials are distributed to an individual user, group, or device, the identity of the user, group, or device receiving the authentication credentials must be verified.

Information System Account, Identity, and Authentication Management

Confidential Information

Authentication credentials are considered University confidential information. Stored, cached, or transmitted authentication credentials must be protected from unauthorized disclosure or modification. See also *BPPM* 90.01 and 90.05.

User Responsibility

It is the responsibility of each account holder to keep their authentication credentials secret. Account holders must not share or transfer their authentication credentials to others.

Access Expiration

A user's password will be expired if:

- It has not been changed according to the maximum password age requirements; or
- It has been lost, stolen, or compromised.

A user's access is revoked if their password has expired until their password has been changed. The identity of information system users is verified prior to providing replacement authentication credentials.

ENFORCEMENT

The Office of the Chief Information Officer (CIO) is responsible and has the authority for enforcing compliance with this policy.

Violations

Persons determined to have violated this policy are subject to sanctions imposed using the procedures set forth in applicable University or state policies and handbooks (e.g., the WSU *Faculty Manual*, the *Administrative Professional Handbook*, *WAC* 357-40 (civil service employees), applicable collective bargaining agreements, or the WSU Standards of Conduct for Students, *WAC* 504-26).

Exceptions

The Office of the CIO manages and maintains exceptions to this policy, under the guidance of the Chief Information Security Officer.

The Office of the CIO must document and maintain all policy exceptions in writing for the life of the exception. Approval for policy exceptions are effective for a specific period of time and must be reviewed by the Office of the CIO on a periodic basis.

MAINTENANCE

The Office of the CIO is to review this policy every three years or on an as-needed basis due to changes to technology environments, business operations, standards, or regulatory requirements.