WAYNE STATE UNIVERSITY
Computing & Information Technology

Standards for Access, Authentication and Authorization

Purpose
This standard establishes the need for the University to institute consistent controls for identification of information system users, as well as the secure authentication of approved users for normal and administrative system functions.

Scope
The scope of this policy covers all electronic systems that provide computer services, store or process university data, whether managed centrally by C&IT or at a departmental support level.

Roles and Responsibilities
University IT staff will design and deploy information systems using centrally-managed AccessID

University IT staff will configure information systems under their authority with the requisite settings, scripts, or programs to ensure that computing events deemed necessary for security purposes are properly generated, stored, monitored, and reviewed, and that these audit records are made readily available to the C&IT Information Security Office.

University management will include minimum requirements as defined by this policy and related policy materials for audit records and logging as prerequisites for any information system or application which is purchased, procured, developed, or implemented.

The C&IT Information Security office will assist system administrators in ensuring their systems and applications are applying appropriate identification and authentication methods that meet the minimum standards as defined by this standard and related materials.

Access, Authentication and Authorization, Procedures, and Guidelines
Detailed procedures, standards, and guidelines will be authored and maintained by the C&IT Information Security Office outlining the specific identification and authentication security controls to be developed and implemented, along with appropriate guidance. New or modified procedures, standards and guidelines will be communicated to all University IT staff once approved by the C&IT Risk & Security Oversight Committee.

Organizational Coordination
The C&IT Information Security Office will solicit feedback from on-campus IT units regarding the effectiveness and applicability of this policy and related standards, taking it into consideration during periodic policy review. This policy and associated documents will be openly published and communicated to all IT staff at a minimum of an annual basis.

Compliance
All university units are required to be in compliance with this policy and any associated standards. Any exceptions to this policy must be approved by the C&IT Information Security office, will be given a deadline for proper compliance, and will be reviewed on an annual basis.

Standard Review
This standard and any associated procedures, standards, and guidelines will be reviewed at a minimum on an annual basis by the C&IT Risk & Security Oversight Committee.

Definitions
As used in this standard, *"enterprise systems"* are electronic information systems maintained by C&IT that contain institutional data that is defined by the Data Governance Committee. Current examples of enterprise systems include Banner, Cognos, and Imaging.

As used in this standard, "two-factor authentication" is a combination of two or more factors 1) something you know 2) something you have 3) something you are.

Access and Authorization Standards
The following standards should be enforced for all clients, servers, and network-based devices in the University environment:

1. **Passwords Required**
   Interactive usage of any system shall be restricted until an authorized user authenticates successfully. This should occur on system startup, powerup, or wakeup from sleep or hibernation mode.

2. **User Identification**
   All user-level credentials must be unique and issued to a single person in a method that allows for auditing of access and activity.
   - Passwords should never be shared or known by anyone other than the user assigned the credentials.

3. **Minimum Privilege & Elevation**
   Users should access and operate systems at the minimum security level needed in order to perform their work. Where possible, elevated system access (such as "root" or "administrator") should occur only after primary authentication utilizing AccessID credentials has taken place. Examples of this include "Run As" in Windows systems or "sudo" on Linux based systems.

4. **Administrative Privileges**
   Where possible, an approve form of two-factor authentication should be used for all administrative access. Access to systems that require administrative privileges must be configured on a separate account. Separate administrative-level accounts should be configured and utilized only when administrative tasks must be performed.
   - If an administrative account's role, such as "root" or "administrator", cannot be assigned to an individual user account passwords may be only shared using an approved Enterprise Password Manager.

5. **Password Complexity**
    - All passwords should meet the Wayne State Strong Password Standard.
    - All cloud services that are used for processing or storing WSU data should use SSO when possible, if not possible the WSU strong password standard must be followed, unless restricted by agreement with the external provider.

6. **Password Cycling and Reuse**
   All user and administrative passwords should be changed and cycled every 180 days at minimum unless using a password of significant complexity as defined in the password standards. User passwords should not be reused for at least three cycles, and administrative passwords should never be reused.

7. **Session Termination and System Termination**
   Inactivity timeouts must be used for systems and applications that are performed in an automated fashion.
    - Desktop and Severs should lock or utilize a password-protected screensaver after 15 minutes of inactivity.
    - Web and native applications should lock or time out after 30 minutes of inactivity.
    - Applications sessions should be terminated as soon as possible after completing a process or transaction.

8. **Shared Accounts**
   Using accounts that require a shared password are prohibited from use for normal user authentication and should only be used for authentication of an application or service.
    - All shared accounts must have an owner and passwords must be stored in an approved Enterprise Password Manager.
    - Any shared account must follow the same standards as any other account, shared accounts with privileged access must follow the additional requirements of administrative access.
    - Any situation that must require sharing of a password for user access must be stored and only shared through an approved Enterprise Password Manager.

Authentication Standards

The following standards should be enforced for all clients, servers, and network-based devices in the University environment:

1. **Central authentication**
   Credentials should utilize central LDAP or Active Directory sources for authentication. Where possible, the central Single-Sign-On (SSO) system should be used.

2. **two-factor authentication**
    - Two-factor or multi-factor authentication should be used whenever technically feasible.
    - If not using SSO, multi-factor authentication should be used, where offered, for any cloud service that processes or stores WSU data.

3. **Prohibited Accounts**

Commonly utilized default accounts such as a "guest" account should be permanently disabled.

Additional Standards for Enterprise Systems

Enterprise systems that store or process confidential data are subject to a higher standard of system auditing and require the following additional security controls:

1. **Training**
   Must complete all necessary training and agreements before system access is granted
   - Access to certain types of information may require special training and certification before granting access to the data. In cases where business needs dictate immediate access, training must be completed within 60 days of gaining access to any enterprise system.

2. **Approval**
   Must follow an approved authorization process for system access and role management
   - Access data must be granted by the data owner and approved based on business need to access the data.

3. **Separation of duties**
   Must follow an approved process that allows for separation of duties
   - No one person should be allowed to approve access and perform the implementation of that access.

4. **Least privilege**
   Must follow a process that grants access following the concept of least privilege
   - Access must be granted at the minimum level necessary to before a business process
5. Must complete an attestation of system access on at least an annual basis
   - An annual review of system access must be performed by each business unit to attest to the need for a business processes need to continue to have access to previously granted data.
   - When using role based access, an annual review must be performed by the data owner to attest to the proper level of access has been granted to each role based on the business functions requirements.

6. **Access termination**
   Must follow a process that ensures system access is removed when business requirements change.
   - When an individual is no longer employed or affiliated with the University access to enterprise systems must be removed in a timely manner.
   - When a user changes job responsibilities or moves from one department to another system access must be remove in a timely manner.

Non-Compliance

The C&IT Information Security Office may limit access to or from a system if it does not meet the above guidelines.

Exceptions

Exceptions to these standards may be granted by the Information Security Office given business justification and a satisfactory risk assessment. In such cases, the system owner shall acknowledge the risk and take responsibility for any breaches, incidents, or compromises that occur as a result of not utilizing a supported operating system.