

Identity and Access Management Policy

Purpose

The purpose of this policy is to define required access control measures to all University systems and applications to protect the privacy, security, and confidentiality of University information assets and systems, especially highly sensitive systems.

Scope

This policy is applicable to those responsible for the management of user accounts or access to shared information or network devices. Such information can be held within a database, application or shared file space. This policy covers departmental accounts as well as those managed centrally.

Definitions

Access- The ability to use, modify or manipulate an information resource or to gain entry to a physical area or location.

Access Control- The process of granting or denying specific requests for obtaining and using information. The purpose of access controls is to prevent unauthorized access to IT systems.

Availability- Protection of IT systems and data to ensure timely and reliable access to and use of information to authorized users.

Confidentiality- Protection of sensitive information so that it is not disclosed to unauthorized individuals, entities or processes.

Principle of Least Privilege- Access privileges for any user should be limited to resources absolutely essential for completion of assigned duties or functions, and nothing more.

Principle of Separation of Duties- Whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse, or other harm.

Identification

Identification is the process of assigning an identifier to every individual or system to enable decisions about the levels of access that should be given. Identifiers must contain the following:

- Uniqueness- Each identifier (e.g. user ID or University M Number) is unique; that is, each identifier is associated with a single person or other entity
- One Identifier per Individual- An individual may have no more than one University identification number

- Non-Reassignment- Once an identifier is assigned to a particular person it is always associated with that person. It is never subsequently reassigned to identify another person or entity.

Authentication

The authentication process determines whether someone or something is, in fact, who or what it is declared to be. Authentication validates the identity of the person. Authentication methods involve presenting both a public identifier (such as a user name or identification number) and private authentication information, such as a Personal Identification Number (PIN) or password.

All systems and applications must use encrypted authentication mechanisms and abide by the following:

- Authentication credentials will not be coded into programs or queries unless they are encrypted, and only when no other reasonable option exists.
- Unique initial passwords must be provided through a secure and confidential manner and initial passwords must be changed upon first logon
- Passwords must not be stored in clear text or in any easily reversible form.
- Vendor-supplied default and/or blank passwords shall be immediately identified and reset upon installation of the affected application, device, or operating system.

To ensure that passwords are of adequate strength, passwords for users, systems, applications, and devices must meet, to the degree technically feasible, the following Information Security requirements:

Password Requirements	
Password Expiration	Every 90 days
Minimum Length	8 characters
Password Complexity	Enabled
Password History	Last 4 passwords
Account Lockout	After 5 unsuccessful consecutive logon attempts
Lock-Out Duration	30 minutes
Renewed Log In	After 30 minutes of inactivity or by a system administrator
Screensaver	Idle after 10 minutes, password protected

All privileged accounts (root, super user, and administrator passwords for servers, databases, infrastructure devices and other systems) must adhere to the requirements listed above and where possible and appropriate:

- Support authentication of individual users, not groups
 - In situations where group accounts for administrative purposes and shared passwords for those accounts is required, the password must be changed every ninety days and immediately upon any personnel change within the group.
- Configure devices with separate accounts for privileged and unprivileged access
- Authenticate users with an unprivileged account rather than a privileged account

Authorization

Authorization is the process used to grant permissions to authenticated users. Authorization grants the user, through technology or process, the right to use the information assets and determines what type of access is allowed (read-only, create, delete, and/or modify). The system or application should determine if the user has permission to perform the requested operation.

Users are not permitted to access sensitive data unless the *Data Owner* has given written permission through established business processes. Data Owners are individually responsible for establishing data access procedures that must include, at a minimum, the following:

- Access request forms must be used to request, change, or delete existing access privileges to University systems that contain sensitive information.
- To maintain the requirements of minimum necessary and least privilege, when a user transfers, all accounts should first be disabled, privileges removed, then accounts re-enabled and privileges added that are required in the user's new role.
- For new accounts and changes to existing accounts, portions of the form must be completed and authorized by the:
 - Person who is requesting access to the system
 - User's supervisor and/or department head (or designated representative)
 - Data Owner
- For account deletions, report separations in a timely manner when workforce members are reassigned, promoted, or separated. For Termination with cause, deactivation must occur immediately.
- Periodic review of user privileges to ensure access is commensurate with user's current responsibilities, as well as modification, removal or inactivation of accounts when access is no longer required.

It is the manager's responsibility to ensure that all users with access to sensitive data attend proper training as well as read and acknowledge the University Confidentiality Agreement.

Segregation of Duties

Access privileges granted to each individual user will adhere to the principles of separation of duties. Technical or administrative users, such as programmers, system administrators, database administrators, security administrators of systems and applications must have an additional, separate end-user account to access the system as an end-user to conduct their personal business.

Compliance

System owners must have documented procedures for access control and must be able to produce the documented procedures when required for auditing purposes. Evidence of account approval, termination, and disabling must be available when required for auditing purposes.

END OF DOCUMENT