Identity And Access Management Standard DRAFT

Revision Notes:	**Last Updated: 12/2019**	Status: APPROVED Feedback Link
Version 1.0 - 4/2019 Supersedes Enterprise Password Standard Version 1.0.1 12/2019 Integrates feedback and recommendations from governance review.		

Table of Contents

1. Objective:
The objective of this standard is to clearly define requirements that must be met to consistently and securely identify, authenticate, and authorize users of University IT services. This standard meets the requirements outlined in section 4.4.4 of the University Information Security Policy**.**

2. Scope:
This standard applies to all IT services employed in the conduct of University business.

3. Requirements

3.1 Identification Requirements

3.1.1. Unique Accounts - All non-public IT services, systems, or applications that are operated by, or on behalf of the University, must clearly identify users via the use of unique accounts.

3.1.2 Identity Proofing - The University must establish identity proofing procedures that are maintained by Information Technology Services to reasonably identify individuals and groups prior to the issuance of accounts.

3.1.3 Management of Shared Accounts - The use of shared accounts (see Generic accounts) may be authorized to address particular University business requirements. Requests to create shared accounts must undergo a formal authorization review and may be rejected by ITS for any reason. The creation of shared accounts must be formally documented. Shared accounts must have a designated owner who is responsible for the account including all access and maintaining associated documentation for individuals who may utilize this account. Shared accounts must be reviewed and renewed on a periodic basis. Shared accounts may not access or manage University Confidential Data.

3.2 Authentication Requirements

3.2.1 Required Authentication Methods

- **ITS Approved Authentication Methods**
  Where technically feasible**,** all University IT services (whether internal or hosted by third parties) must utilize an ITS approved and maintained solution that authorizes different account types (see above - 3.1).

  The two approved ITS solutions are:
  - Shibboleth
  - Active Directory (LDS)

- **Solutions That Don't Meet Single Sign On Requirements**
  University IT Systems and Applications which do not integrate with the ITS approved and maintained single sign on solution will be evaluated on a case by case basis and may be approved or disapproved by the University Chief Information Officer or her/his delegates based on relevant risks, benefits, and costs.

3.2.2 Two Factor Authentication Requirements

- **Two Factor Mandatory For Privileged User Accounts**

All University Faculty/Staff that have been designated as Privileged access accounts (inc. generic accounts) are required to utilize ITS approved and maintained Two Factor Authentication solution.

- **Two Factor Recommended For All Faculty/Staff and Students**
  The use of an ITS approved and maintained Two Factor Authentication solution is recommended for use by all University faculty/staff and students.

- **Two Factor Integration Required For Enterprise IT Solutions**
  Where technically feasible, all University IT services, whether internal or procured via third-parties, must be integrated with ITS approved and maintained Two Factor Authentication solution. This is typically accommodated by meeting Single Sign On integration requirements (see 3.21)

3.2.3 Password Requirements

- **Password Expiration + Complexity**

Account types may have multiple password tiers that define associated **password complexity** (see 5.4) and **expiration requirements** (see 5.5). The following password tiers are recognized:

Tier	Account Type	Two-Factor Authentication Required?	User Two-Factor Enrolled?	Expiration	Min. Password Length
T1	Standard Accounts & Special Accounts (see section 3.3.1)	**No**	**No**	180 Days	>=14
T2	Standard Accounts & Special Accounts (see section 3.3.1)	**No**	**Yes**	365 Days	>=14
T3	Privileged Access Accounts	**Yes**	**Yes**	365 Days	>=14

3.2.4 Password Creation

- **Initial Passwords**
  Where technically feasible (see 5.8), initial passwords to new accounts should employ randomly generated passwords. Account holders should be required to change this password following their first successful login to the associated service.

- **Password Reuse**
  Where technically feasible, passwords must be evaluated upon a password reset to ensure that formerly used passwords or derivation of prior passwords are not reused.

- **Dictionary Terms**
  Where technically feasible, passwords must be evaluated to prohibit single dictionary terms from being employed in a manner that might be easily guessed or recovered via password cracking (see 5.7).

3.2.5 Password Changes

In addition to periodic password changes as defined as requirements for password tiers (see 3.3), password must be updated in the following circumstances:

- If the account credentials of a user or system have been disclosed or otherwise compromised, the password shall be changed immediately.
- The University reserves the right to change passwords to protect the security, stability, or integrity of institutional resources and operations.

3.2.6 Secure Password Transmission

The transmission of passwords over networks must always be encrypted whether used for authentication or other purposes. The encryption used for this transmission must conform with relevant requirements specified in the **University Encryption Standard**.

3.2.7 Secure Password Storage

Individual Passwords must never be stored in clear-text electronic or physical formats. Password authentication databases or files must be hashed and conform with the **University Encryption Standard**.

3.3 Authorization

In order to facilitate the provisioning of IT services, ITS will create and maintain a variety of electronic identities and accounts.

3.3.1 Account Types

All accounts (see 5.2) used to facilitate University business will be associated with an account type. User accounts types are differentiated based on the role and degree of access or capability they provide.

The following account types will be established and maintained:

- Standard Accounts:
  - Faculty/Staff, Applicant and Student Accounts - These are standard permission accounts used to access University information systems and Non-Confidential University data (see Data Management Standard).

  - NonEmployee Administrative Accounts - These are standard accounts with specific requested access to University information systems. They are requested by the Dean, Department Chair, Director, or other departmental administrator for use by non-employee individuals. This role has several subroles that are defined below:
    - Academic Off Campus
    - On Campus without Departmental Access
    - On Campus with Departmental Access

- Privileged Access Accounts - Privileged access accounts include all University accounts that meet one of the following criteria:
    - An account that has elevated rights that allow for actions that can alter the performance, security, or operation of University systems and services and impact other users.

        - Any account that allows access to read, copy, or modify Confidential University Data (see Data Management Standard).
        - Any account utilized by a part-time or full-time employee who works in a designated Secure Data Environment (see Secure Data Handling Standard - section 3.1)

- Special Accounts:
    - Generic Accounts - Generic accounts are special email accounts or google groups owned by individual users on campus for sending and receiving email on behalf of a department or organization.

    - Vendor Accounts - Vendor accounts include all organizations and individuals who may utilize accounts to perform work on behalf of the University but are not University employees. These accounts will move to Non Employee Administrative accounts with specific granular access needed.

    - Service Accounts - Service accounts are system/device accounts used to execute and support IT services.

3.3.2 Account Life Cycle Management

Initiation of Accounts

- Standard Accounts (see 3.3.1) will be automatically created based on electronic records pertaining to employment, application, admissions, contractual arrangement, or other relationships pertaining to University business.
- Issued accounts may not be utilized without acceptance of relevant University policies and agreements including but not limited to the Acceptable Use of Computing and Electronic Resources Policy and University Statement of Confidentiality. If not accepted, access to email and all other applications is denied.

- Access to multi-user systems containing University data must be authorized. Requests for privileged access authorization must be made according to established processes for each system and be based on

business or academic need for access. Authorization of access may be granted by the appropriate data steward and/or their designated security officer (see Data Management Standard) in consultation with the CIO and CISO. The Chancellor has sole final discretion in access decisions.

Modification of Accounts

- Authorization for access to critical systems or those containing Confidential University Data (see Data Management Standard) must be revoked when an individual's change in employment status, job function, or responsibilities no longer requires specialized access privileges.
- All additions, changes, and deletions to individual access must be approved by the individual(s) responsible for the management of each system's access and must have a valid business justification.
- Administrative and system technical support account authorization must be approved by (at a minimum) the individual(s) responsible for technical management of the system. Every system and service account must have a designated responsible individual. If that individual changes, a new individual must be designated.
- Individuals may not authorize their own access.

Termination of Accounts

- Access privileges must be revoked when access is no longer justified by an approved relationship between the University and the account holder.
- In certain cases, access privileges may be temporarily extended beyond a change in relationship to allow for continuity of communication and data transfer. The case for extension includes but is not limited to retiree user accounts.
- Individuals responsible for access control for each system must review and approve all requests for access modifications.
- The University reserves the right to deny, revoke, or terminate UserIDs at will in a consistent manner with other related University policies, standards, and procedures.

4.0 Enforcement, Exemptions, and Advisement

4.1 Authority and Enforceability - This standard is established under the authority of the Chief Information Officer (Information Security Policy 4.3.3). In the event of violation of this standard, the Chief Information Officer may require that non-compliant University

IT services or practices be temporarily suspended or discontinued until relevant requirements (see section 3.0) are established and/or verified.

4.2 Exemptions - Exemptions to this standard must be undergo a formal risk evaluation and receive signed approval by the University Chief Information Officer.

4.3 Review and Advisement - Collaborative advisement concerning these standards are provided by the Information Security Advisory Council, IT Executive Council, IT Board of Directors, and IT Implementation Group.

5. Definitions

5.1 "IT Services" - IT services refers to the application of business and technical expertise to enable the creation, management and optimization of or access to information and business processes and includes business process services, application services and infrastructure services.

5.2 "Electronic Identity" - An electronic identity is a representation of a known individual or group.

5.3 **"Identification"** - Processes related to the attestation of a legitimate association to a University electronic identity.

5.4 "Authentication" - Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

5.5 "Access" - Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.

5.6 "Access Controls"- Access controls determine who is authorized to have an account on Information Technology systems, what they are authorized to do with their account, and how they are to proceed with accessing the systems which they have permission to use. Access controls are designed to protect both individual and University information.

5.7 "Authorization"- Access privileges granted to an authenticated user, program, or process or the act of granting those privileges. Privileges are no longer "authorized" when a user leaves a role upon which the authorization was based (for example, leaving a job or changing to a new position with different responsibilities).

5.8 "Password" - A secret word or phrase that is used to gain access to computer systems, applications, databases, or other information resources.

5.9 "Accounts" - Accounts are used to identify individuals, groups, or processes that are allowed to utilize non-public IT services and systems.These accounts are tied to a unique UserID that when utilized with an appropriate password (and/or other authentication factor) provides authentication.

5.10 "Enterprise IT Solutions" - A server or other system providing access or services for more than one concurrent user. Typically, a system that multiple people rely upon to be reliably available for use.(Multi-User system)

5.11 "Password Complexity" - Password complexity is an overall measurement of both the length of passwords and the diversity of the character sets that comprise them.

5.12 "Password Expiration" - Password expiration denotes the amount of time that passwords remain valid before requiring a password reset and utilization of a new password.

5.13 "Two Factor Authentication" - Two factor authentication refers to authentication methods that utilize more than one type of authentication factor. This multi-factor authentication methods use a combination of something you know (i.e. passwords), something you have (i.e. physical access token), or something that you are (i.e. biometric information) to identify authorized users.

5.14 "Password Cracking / Offline Attempts"- Password cracking refers to attempts to uncover account passwords by trying automated password guessing attempts against authentication databases.

5.15 "Technically Feasible" - Something that is technically possible and does not materially impact the ability of the technology or user to complete mission-critical tasks.

6. References

6.1 University Information Security Policy (Key Control Requirements 4.1)

6.2 University Data Management Standard

6.3 University Encryption Standard

6.2 University Statement of Confidentiality

6.3 University Identity Theft Prevention Plan

6.4 University Payment Card Services Policy

7. Contacts for Questions or Information About this Standard

Office contact	Phone	Online/Email
Chief Information Officer	828-262-6278	cio@appstate.edu