Enterprise Password Standard

Revision Notes:	Last Updated: 05/2016	Status: APPROVED
Version 1.0 - 4/2016 *Approved By: ISAC, Cabinet Ratified* Version 1.01 5/2016 Added sections for format alignment with other approved standards. Revised Privileged User account definitions to include Confidential data access. Revision		

Table of Contents

1. Objective:

The objective of this standard is to clearly define the requirements associated with the management of passwords (see 5.1) utilized for managing, accessing, and supporting University enterprise IT services. This standards meets the requirements outlined in section 4.1 of the University Information Security Policy.

2. Scope:

This standard applies to all accounts associated with enterprise-level (university-wide) IT services (see 5.3).

3. Requirements

3.1 Account Types

All IT service accounts (see 5.2) 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 levels are recognized:

- **User Account** - These are standard permission accounts used to access University information systems and **Non-Confidential** University data (see Data Management Standard).

- **Privileged Account** - Privileged accounts include all University accounts that meet one of the following criteria:
    1. 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.
    2. An account that allows access to read, copy, or modify Confidential University Data (see Data Management Standard).

- **Service Accounts** - Service accounts are system/device accounts used to execute and support IT services. Because of the potential for service disruption associated with changing service account passwords, these complexity requirements and associated password rotation intervals must be greater.

3.2 Password Tiers

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	Expiration	Two-Factor Authentication	Min. Password Length	Password Strength / Scoring
T1	User Account	90 Days	No	>=8 Characters	Contains at least 2 of 4: Number Lowercase Letter Uppercase Letter Symbol **-or-** Equivalent or greater password strength based password scoring algorithm.
T2	User Account	120 Days	No	>=12 Characters	Contains at least 3 of 4: Number Lowercase Letter Uppercase Letter Symbol **-or-** Equivalent or greater password strength based

					password scoring algorithm.
T3	User Account	180 Days	No	>=14	Contains 4 of 4: Number Uppercase Letter Lowercase Letter Symbol
T4	Privileged Account	90 Days	No	>=14 Characters	Contains 4 of 4: Number Uppercase Letter Lowercase Letter Symbol
T5	Service Accounts	365 days	No	16 Characters	Contains at least one: Number Uppercase Letter Lowercase Letter Symbol

3.3 Password Creation

3.3.1 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.

3.3.2 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.

3.3.3 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).

3.4 Password Managers

The utilization of password managers applications for all account types is allowed and encouraged so long as the application meets the following criteria:

- The password manager applications encrypts stored password using AES and a 128-bit or greater key length.
- The master key used to unlock or access stored passwords meets or exceeds the highest password tier requirements associated with the accounts stored.

3.5 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 to the University **Encryption Standard**.

3.6 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**.

4.0 Enforcement, Exemptions, and Advisement

4.1 Authority and Enforceability - This standard is established under the authority of the Chief Information Security Officer (Information Security Policy 4.3.3). In the event of violation of this standard, the Chief Information Security 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 University Cabinet, Information Security Advisory Committee, and Information Security Liaisons.

5. Definitions

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

5.2 **"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.

5.3**"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.

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

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

5.6 **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.

5.7 **Password Cracking / Offline Attempts**- Password cracking refers to attempts to uncover account passwords by trying automated password guessing attempts against authentication Databases.

5.8 **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

5.1 University Information Security Policy **(Key Control Requirements 4.1)**

5.2 University Data Management Standard

5.3 University Encryption Standard

5.2 University Statement of Confidentiality

5.3 University Identity Theft Prevention Plan

5.4 University Payment Card Services Policy