



| | |
|-------------------------------|-----------------------------|
| Subject: | Password Standards |
| Standards Number: | 501 |
| Effective Date: | 10-01-10 |
| Revised Date: | 06-04-18 |
| Responsible Authority: | Information Security Office |
| Pages: | 7 |

ACCOUNTABILITY/APPLICABILITY:

This standard applies to all technology and systems that are technically and logically capable of supporting the standard. This includes but is not limited to: university owned desktop computers, laptops, cell phones with UCF provisioned email accounts, small factor computing devices, UCF's electronic services, systems, and servers. The standard covers all university resources.

STANDARDS STATEMENT:

Passwords are the most frequently utilized form of authentication for accessing a computing resource. Due to the use of weak passwords, the proliferation of automated password-cracking programs, and the activity of malicious hackers and spammers, they are very often also the weakest link in securing data. Greater risks require a heightened level of protection. Passwords must therefore follow the standards listed below.

Consult with the UCF Information Security Office if questions arise regarding the compliance of a system with regard to any of the following standards.

STANDARDS:**General Account Password Standards**

1. All passwords (e.g., NID, email, web, desktop computer, etc.) should be strong passwords. Privileged accounts have stricter password requirements. In general, a password's strength will increase with length and complexity. (*For additional information on strong passwords, refer to step two*).

2. All passwords should meet the following standards:
 - a. Be at least eight (8) alphanumeric characters long (longer passwords are encouraged because they are often harder to guess or crack).
 - b. Use all of the following character types at least once:
 - i. Uppercase letter (A/a through Z/z)
 - ii. Lowercase letter (A/a through Z/z)
 - iii. Number (0-9)
 - iv. Special character (e.g., !,\$,#,%)
 - c. Passwords should not be words from any dictionary, in any language, slang, dialect, jargon, based on easily guessed personal information, (e.g., names of family members, friends, pets, etc.), birthdates, or other personal information such as an address or telephone number.
 - d. Passwords should also not contain three or more consecutive characters from an account's name or username (e.g., Joe Smith with username jo123456 cannot include joe, oes, esm, smi, mit, ith, o12, or 456 in his password).
 - e. Blank passwords should not be used and are not permitted.
3. Passwords must be encrypted both in storage and in transit.
 - a. Passwords in storage, including those stored in password management tools, should be encrypted using at least 256-bit industry accepted encryption (e.g., Advanced Encryption Standard [AES], Blowfish)
 - b. Passwords in transit should be encrypted via TLS protocol.
4. The same password should not be used for access that is external to UCF (e.g., online banking, personal email accounts, personal desktop and/or laptop computers, etc.)
5. Systems should observe these password age and history standards via technical controls:
 - a. Maximum password age should be no more than 60 days.
 - b. Activate password history and store at least the last 24 passwords.
6. Attempts to guess a password should be limited to ten (10) incorrect guesses. Any attempts over ten (10) guesses within 15 minutes (lockout counter reset time period) should automatically disable/lock the account. Account should remain locked (lockout time) for 15 minutes before a password can be attempted again.
7. UCF user account passwords should not be shared with anyone, including administrative assistants or IT administrators.
8. If a password is suspected to have been compromised, it should be changed immediately and the security incident reported to the IT manager, and the Security Incident Response Team (SIRT.) SIRT contact information: sirt@ucf.edu.
9. Audit log or log files must never contain password information.

501 Password Standards 2

10. Default or preconfigured passwords should never be used (e.g., manufacturer default passwords, default SNMP strings).

Privileged Account Password Standards

In addition to the general password standards listed above, the following standards apply to any administrative account passwords (such as those that maintain the access of other accounts, or provide access to a security infrastructure):

1. All privileged accounts must be protected using multi-factor authentication where technically feasible.
2. Attempts to guess a password should be limited to three (3) incorrect guesses. Any attempts over three (3) guesses within 15 minutes (lockout counter reset time period) should automatically disable/lock the account. The account should remain locked (lockout time) for 15 minutes before a password can be attempted again.
3. All passwords should be at least fifteen (15) alphanumeric characters long (longer passwords are encouraged because they are often harder to guess or crack).
4. Privileged account passwords should be configured to not expire, provided the other more stringent standards described in this section are implemented.
5. Failed attempts should be logged, unless such action results in the display of a failed password. It is recommended that these logs be retained for a minimum of 30 days. Administrators should regularly inspect these logs and immediately report any irregularities or compromises to SIRT.

DEFINITIONS:

Access password: A password used to authorize access to data and distributed to all those who are authorized similar access to that data.

Audit logs: A registry that shows the identifier, date, and time that stored data is accessed.

Authentication. The process of establishing confidence in user identities electronically presented to an information system.

Authorization process: The actions involving (1) obtaining an access password from a system user (whose identity has already been authenticated, perhaps using a personal password); (2) comparing the access password with the password associated with the protected data; and (3) authorizing access to the data if the entered password and the stored password are the same (see note above).

Compromise: Disclosing a password, or part of a password, to someone not authorized to know, have or use the password.

Data: Numerical or other information represented either in a physical form or in a form suitable for electronic processing or storage.

DSC: Acronym for College or Departmental Security Coordinator. The website <http://www.infosec.ucf.edu> contains more information on the role of a DSC.

Employees: Individuals acting on behalf of the university in processing, storing, and retrieving data. This includes any paid or volunteer acting on behalf of the university.

Encrypted or truncated. Data converted to a code or shortened for security purposes.

Encryption: The process of transforming data to an unintelligible form in such a way that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process (two-way encryption).

FERPA: The Family Educational Rights and Privacy Act of 1974. Also known as the Buckley Amendment. FERPA is a federal law that protects the privacy of student academic records.

Information Security Office (ISO): The mission of the Information Security Office is to provide a secure infrastructure that protects the confidentiality, integrity, and availability of information resources. To this end, the ISO develops security best practices, coordinates security issues, conducts investigations, and works with Information Technology (IT) and other campus departments to minimize security risks and assure compliance with security policies and procedures.

Multi-Factor Authentication: A security technology system that requires users to verify or prove their claimed identity using more than one validation procedure (method of authentication) from independent categories of credentials when accessing an electronic service. Categories may include, but are not limited to some combination of physical, logical/knowledge, and/or biometric validation techniques.

Network Identification: (Also abbreviated NID) A UCF-issued credential, which may also be part of one's email account, to be used by university employees and students to access systems.

Passphrase: A sequence of characters, longer than the acceptable length of a password that is transformed by a password system into a virtual password of acceptable length.

Password system: A system that uses a password or passphrase to authenticate a person's identity or to authorize a person's access to data and which consists of a means for performing one or more of the following password operations: generation, distribution, entry, storage, authentication, replacement, encryption and/or decryption of pass-words.

Personal identifier: A data item associated with a specific individual which represents the identity of that individual and may be known by other individuals.

Personal password: A password that is known by only one person and is used to authenticate that person's identity.

Privileged Accounts: An account that allows special programs or elevated access to read and/or change sensitive systems and/or data. "Administrator", "Service", and "Root" accounts fall into this category.

Restricted data: Any confidential or personal data that are protected by law or policy and that require the highest level of access control and security protection, both in storage and in transit.

There are two sub-classifications of restricted data

Highly Restricted Data: Examples of highly restricted data are: a) an individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: social security number, driver's license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity, or financial account numbers; b) user name (e.g., NID) or email address, in combination with a password or security question and answer that would permit access to an online account; c) data concerning an individual that is considered "nonpublic personal information" within the meaning of Title V of the Gramm-Leach Bliley Act of 1999 (Public Law 106-102, 11 Statute 1338) (as amended) and its implementing regulations, and; d) data concerning an individual that is considered "protected health information" within the meaning of the Health Insurance Portability and Accountability Act of 1996 (as amended) and its implementing regulations, and the HITECH Act. Protection of such data may also be subject to additional operating regulations in accordance with vendor or partner agreements, such as the Payment Card Industry Data Security Standards.

Restricted Data: Restricted data include electronic information the unauthorized access, modification, or loss of which could adversely affect the university (e.g., cause financial loss or loss of confidence or public standing in the community), adversely affect a partner (e.g., a business or agency working with the university), or adversely affect the public.

SIRT: Acronym for Security Incident Response Team. The website <http://www.infosec.ucf.edu> contains additional information on the role of SIRT when responding to incidents.

Strong password: A password that is difficult to guess, is not in any dictionaries, contains upper and lower case letters, and consists of eight or more characters including numbers and specials characters.

Valid password: A personal password that will authenticate the identity of an individual when presented to a password system or an access password that will allow the requested access when presented to a password system.

RELATED DOCUMENTS:

- 1) 4-002.1 *Use of Information Technologies and Resources* policy
- 2) 4-007.1 *Security of Mobile Computing, Data Storage, and Communication Devices* policy
- 3) 4-008.1 *Data Classification and Protection* policy
- 4) NIST Special Publication 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management
 - a. <https://pages.nist.gov/800-63-3/sp800-63b.html>
- 5) Account Lockout Best Practices White Paper
 - a. <https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/account-lockout-threshold>
- 6) System Administration, Networking, and Security Institute (SANS) Password/Passphrase Policy:
 - a. http://www.sans.org/security-resources/policies/Password_Policy.pdf
- 7) CIS System Benchmarks
 - a. <http://benchmarks.cisecurity.org/>

CONTACTS:

Information Security Office

<https://infosec.ucf.edu>

infosec@ucf.edu

Identity and Access Management

<https://infosec.ucf.edu/identity-management>

iam@ucf.edu

Security Incident Response Team (SIRT)

<https://infosec.ucf.edu/incident-response/>

SIRT@ucf.edu

UCF Information Technology Support Center

(407) 823-5117

<https://it.ucf.edu/>

itsupport@ucf.edu

INITIATING OFFICE: Information Security Office

STANDARDS APPROVAL

(For use by the Information Security Office)

Standards Number: 501

Initiating Office: Information Security Office

Chief Information Security Officer: *Chris Vakhordjian*

Signature: _____ Date: _____

501 Password Standards 7