Nuclear Regulatory Commission
Office of the Chief Information Officer
Computer Security Standard

Office Instruction:	**CSO-STD-0001**
Office Instruction Title:	**Strong Password Standard**
Revision Number:	**2.0**
Effective Date:	**November 30, 2018**
Primary Contacts:	**Jonathan Feibus**
Responsible Organization:	**OCIO/CSO**
Summary of Changes:	CSO-STD-0001, “Strong Password Standard,” provides the minimum security requirements that must be met for the creation and maintenance of passwords.
Training:	As requested

Approvals			
Primary Office Owner	Office of the Chief Information Officer (OCIO) / Computer Security Organization (CSO)	**Signature**	**Date**
SWG Chair	Bill Bauer	/RA/	1/4/2019
CISO	Jonathan Feibus	/RA/	1/7/2019

TABLE OF CONTENTS

Computer Security Standard
CSO-STD-0001

Strong Password Standard

---

1 PURPOSE

CSO-STD-0001, “Strong Password Standard,” provides the minimum security requirements that must be met for creation and maintenance of passwords. This standard addresses passwords used to protect Nuclear Regulatory Commission (NRC) sensitive information and information systems.

The information in this standard is intended to be used by all accounts within NRC systems and whenever passwords are used.

2 GENERAL REQUIREMENTS

This document applies to all use of passwords to protect access to NRC sensitive electronic information and information systems. Electronic information sensitivity is based upon the potential impact of compromise if the confidentiality, integrity, or availability of information is compromised. A system’s sensitivity is determined based upon the highest level of sensitivity that resides within the system.

Passwords are commonly used to access systems and information. They are also used to access credentials that grant or deny access to systems and information. These credentials can be digital certificates.

However, digital identity is the unique representation of a user engaged in an online access to a system or a resource. Digital authentication is the process of establishing the validity of one or more authenticators (e.g., a password) used to claim the digital identity of such user. Further information on other types of digital authentication, in addition to the use of passwords, can be found in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63B, “Digital Identity Guidelines: Authentication and Lifecycle Management.”

Passwords for shared/group accounts should be changed immediately and must be changed within 72 hours after an individual with knowledge of the shared/group account password changes roles, where such password access is not required, or leaves the NRC. The shared/group accounts are only permitted for use subject to the conditions specified in CSO-STD-2006, “User Access Management Standard,” and CSO-STD-0020, “Organization-Defined Values for System Security and Privacy Controls.”

3 SPECIFIC REQUIREMENTS

Passwords must be of sufficient strength to minimize the probability of compromise. In all cases, passwords should be composed in a manner that enables the user to reconstruct the

password from memory, so that the password does not need to be written down. If the password is written down, the written password must be protected at the same level as the information and information systems being protected by the password.

All passwords must meet the following requirements:

- Passwords must be case-sensitive.
- Electronically stored and transmitted passwords must be protected using cryptographic algorithms/ciphers in accordance with CSO-STD-2009, "Cryptographic Control Standard."
- Passwords must NOT be a word in any dictionary, names of places or things, or other easily identifiable constructs, spelled forwards or backwards, and must not be based on a single word (e.g., "Pa$$wOrd").
- Passwords must NOT be a word in any language, slang, dialect, jargon, etc.
- Passwords must NOT be based on personal information (e.g., family names, pet names).
- Passwords must NOT be predictable or easily deduced based upon preferences of the user and must not be easily associated with the user, such as names, car registration or tag numbers, and telephone numbers.

3.1 Methods for Creating Strong Passwords

One way to create a strong password or memorized secret is to use a passphrase. A passphrase is a type of password composed of several words, which can be a part of a sentence, a sentence, or multiple sentences. Passphrases can include special characters and numbers. Additional details on passwords or memorized secrets strength can be found in NIST SP 800-63B, Appendix A, "Strength of Memorized Secrets."

3.1.1 Password Strength

Strong passwords help mitigate guessing and cracking. Password strength is measured by how predictable a password is based on the character set used and password length, known as password entropy. Password entropy calculates how difficult a given password would be to guess or crack using brute force. For establishing a password complexity policy, it must require characters from at least two or three of the following four groups be present in every password:

1. Lowercase letters
2. Uppercase letters
3. Digits
4. Symbols

The password strength is directly proportional to password length and complexity, which is named as keyspace. Keyspace is the total number of possible values that a key, such as a password or a personal identification number (PIN), can have. For example, a four-digit PIN could have any of 10 different values (i.e., 0 through 9) for each of its four characters—the keyspace would be 10^4, or 10,000 (i.e., 0000 – 9999). An eight-character password using a character set of 95 has a keyspace of 95^8, approximately $7 * 10^{15}$ which allows 7 quadrillion

possible passwords. As the keyspace increases, the time required to perform an exhaustive brute force attack on a password also increases.

The password length must be selected in accordance with the level of protection required.

3.2 Administrative Passwords

Administrative passwords for all information technology (IT) systems must meet the following requirements:

- Passwords must be at least 20 characters in length.
- Passwords must contain at least 3 of following: 1 uppercase letter, 1 lowercase letter, 1 number, and 1 special character.
- New passwords must change at least 6 characters from the last password.
- The password lifetime must not exceed 180 days.
- The minimum password lifetime must not be less than 24 hours.
- Passwords must not be reused for 24 generations.

3.2.1 Backup Local Administrative Passwords

Backup local administrative accounts are used on rare occasions when regular system administrative accounts are not accessible. For example, a backup local administrative account on a network device may be created for local access when the enterprise directory server (e.g., Microsoft Active Directory) authentication service is not available for some reason. Another example is when a password is written down, placed in an opaque envelope and sealed, and then placed inside a locked safe for use in case of emergency when backup local administrative account access is required. This account type is not used regularly but only when the need arises. The backup local administrative password should be changed immediately or must be within 72 hours after the individual designated as the backup local administrator changes roles or leaves NRC. Backup local administrative passwords for all IT systems must meet the following requirements:

- Passwords must be at least 20 characters in length.
- Passwords must contain at least 3 of the following: 1 uppercase letter, 1 lowercase letter, 1 number, and 1 special character.
- New passwords must change at least 6 characters from the last password.
- The password lifetime must not exceed 1 year.
- The minimum password lifetime must not be less than 24 hours.
- Passwords must not be reused for 24 generations.

3.3 Application/Service Account Passwords

Application/service account passwords for all IT systems must meet the following requirements:

- Passwords must be at least 20 characters in length.

- Passwords must contain at least 3 of the following: 1 uppercase letter, 1 lowercase letter, 1 number, and 1 special character.
- New passwords must change at least 6 characters from the last password.
- Password lifetime must not exceed 1 year.
- Minimum password lifetime must not be less than 24 hours.
- Passwords should be changed immediately or must be within 72 hours after the individual (i.e., system administrator) with knowledge of the password changes roles, where such password access is not required, or leaves the NRC.
- Passwords must not be reused for 24 generations.

Application/service account passwords should be managed automatically by using an automated tool (e.g., via Microsoft Local Administrator Password Solution.)

3.4 Passwords Used to Protect Sensitive Unclassified Non-Safeguards Information and Systems or Controlled Unclassified Information

Passwords used for all mobile phones must meet the requirements listed below for **"mobile phones."**

Passwords used for all unclassified desktops, tablets, laptops, and other devices must meet the requirements listed below for **"all devices other than mobile phones."**

Passwords used to protect information and systems that currently process Sensitive Unclassified Non-Safeguards Information (SUNSI), or Controlled Unclassified Information (CUI) in the future, must meet the following requirements:

- Passwords for **mobile phones**:
  - Length must be at least – 8 characters
  - Must contain at least – 2 of the following: 1 uppercase letter, 1 lowercase letter, 1 number, and 1 special character
  - Must change at least – 3 characters from the last password
  - Lifetime must not exceed – 180 days
  - Minimum lifetime must not be less than – 24 hours
  - Must not be reused for – 10 generations
- Passwords for **all devices other than mobile phones**:
  - Length must be at least – 15 characters
  - Must contain at least – 2 of the following: 1 uppercase letters, 1 lowercase letters, 1 number, and 1 special character
  - Must change at least – 3 characters from the last password
  - Lifetime must not exceed – 180 days
  - Minimum lifetime must not be less than – 24 hours

- Must not be reused for – 10 generations

3.5 Passwords Used to Protect Safeguards Information and Systems

Passwords used to protect NRC electronic Safeguards Information (SGI) and information systems must meet the following requirements:

- Passwords must be at least 20 characters in length.
- Passwords must contain at least 3 of the following: 1 uppercase letter, 1 lowercase letter, 1number, and 1 special character.
- New passwords must change at least 6 characters from the last password.
- The password lifetime must not exceed 180 days.
- The minimum password lifetime must not be less than 24 hours.
- Passwords must not be reused for 24 generations.

3.6 Passwords Used to Protect Classified Information and Systems

Passwords used to protect classified information and systems, including Restricted Data, must meet the requirements defined in:

- NIST SP 800-53 (as amended), “Security and Privacy Controls for Federal Information Systems and Organizations”
- Committee on National Security Systems Instruction (CNSSI) Number 1253, “Security Categorization and Control Selection for National Security Systems”

3.7 Personal Identity Verification Personal Identification Numbers

PINs used for Personal Identity Verification (PIV) cards must be at least 8 digits in length.

3.8 Password Information Management

System owners must ensure all default password information is changed upon software/firmware installation.

System owners must ensure that initial use password and user authentication information (e.g., PINs), issued by a system administrator, are one-time values that must be changed upon the user’s first login and are distributed to the user via a secure method as documented in the respective System Security Plan (SSP). The method must ensure confidentiality and integrity of the password from all parties other than the password creator and the user. At no time will the user id and password be contained within the same communication.

System owners must ensure that passwords and other authentication information are not transmitted using electronic mail or other form of electronic communication (except via telephone for unclassified, non-SGI systems), unless using encryption methods in accordance with CSO-STD-2009.

Password information must not be stored, transmitted, or incorporated in a readable form in any automatic login scripts, software developed either in-house or out-sourced, hardcopy, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover or use them.

3.8.1 Password Auditing

Only the Office of Inspector General (OIG), Computer Security Organization (CSO), system owners, and Information System Security Officers (ISSOs) have the authority to audit passwords. Password auditing will only be performed to determine vulnerabilities to a system due to weak passwords and must not be performed to enable a user to access another user's account.

When automated password auditing tools are used, passwords must not be revealed to anyone; only the time it took to break the password may be displayed.

APPENDIX A. ACRONYMS

CNSS	Committee on National Security Systems
CSO	Computer Security Organization
CUI	Controlled Unclassified Information
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OIG	Office of Inspector General
PIN	Personal Identification Number
PIV	Personal Identity Verification
SGI	Safeguards Information
SP	Special Publication
SSP	System Security Plan
SUNSI	Sensitive Unclassified Non-Safeguards Information

APPENDIX B. GLOSSARY

Application/Service Account	An information system account used by application or service, which operates in the background of a computer (e.g., server, workstation). Services are commonly referred to as daemons in Linux and Unix operating systems. Application/service accounts are not used directly by human users. In other words, a human user cannot use an application/service account to log in to a computer and work with the computer interactively.
Backup Local Administrative Account	An account created to provide access to a system or a device locally when centralized system resources are not accessible.
Initial Use Password	A password that has been provided to the user by a system administrator or other system authority to access the system for the first time.
Keyspace	The total number of possible values that a key, such as a password or a PIN, can have.
Memorized Secrets	A memorized secret, commonly known as a password, is a secret value (text and/or numeric) intended to be chosen or memorized by the user.
Mobile Phone	A device that is typically hand-held and is also referred to as a cell phone that can receive and make telephone calls without use of any wires while moving over a broad geographic area.
Password Entropy	A measure of how unpredictable a password is, which depends upon character set used and length.
Tablet	A device that is typically hand-held that can access the internet via a wireless local area network connection or cellular data network. A tablet is differentiated from a mobile phone because a tablet does not have the ability to receive and make telephone calls using a cellular carrier without using a data capability (e.g., Voice over Internet Protocol).

CSO-STD-0001 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
16-Nov-09	1.0	Initial issuance	Distribution at ISSO forum and posting on CSO web page	Upon request
26-Aug-10	1.1	Added administrative password strength based upon OIG wireless audit findings.	Distribution at ISSO forum and posting on CSO web page	Upon request
2-Aug-12	1.2	Modified to address mobile phone passwords, tablet passwords, PIV PINs, and to provide information on passphrases. Added new approvals table.	Distribution at ISSO forum and posting on CSO web page	Upon request
31-Mar-15	1.3	Modified to address passwords for application and service accounts.	Distribution at ISSO forum and posting on CSO web page	Upon request
14-Nov-18	2.0	Updated with latest requirements.	Post to OCIO/CSO web page	Upon request
7-Jan-19	2.0	Errata changes for document identifier and organizational changes.	Post to OCIO/CSO web page	N/A