Nuclear Regulatory Commission
Computer Security Office
Computer Security Standard

Office Instruction:	CSO-STD-0001
Office Instruction Title:	NRC Strong Password Standard
Revision Number:	1.3
Issuance Date:	Date of Last Signature
Effective Date:	June 1, 2015
Primary Contacts:	Kathy Lyons-Burke, SITSO
Responsible Organization:	CSO/PCT
Summary of Changes:	CSO-STD-0001, "NRC Strong Password Standard," provides minimum requirements for acceptable passwords.
Training:	Upon request
ADAMS Accession No.:	ML15090A302

Approvals				
Primary Office Owner	Policy, Compliance, and Training		**Signature**	**Date**
Standards Working Group Chair	Bill Dabbs		**/RA/**	**May 5, 2015**
Responsible SITSO	Kathy Lyons-Burke		**/RA/**	**May 4, 2015**
DAA for Non-Major IT Investments	Director, CSO	Tom Rich	**/RA/**	**May 4, 2015**
	Director, OIS	Jim Flanagan	**/RA/**	**May 5, 2015**

TABLE OF CONTENTS

Computer Security Standard

CSO-STD-0001

NRC Strong Password Standard

---

1 PURPOSE

The purpose of CSO-STD-0001, “NRC Strong Password Standard,” is to provide minimum requirements 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 types of users.

2 GENERAL REQUIREMENTS

This document applies to all use of passwords to protect access to NRC electronic sensitive 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. However, passwords are also used to access credentials that are used to grant or deny access to systems and information. These credentials can be digital certificates.

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 and does not require that the password 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 shall meet the following requirements:

- Passwords must be case-sensitive.
- Electronically stored and transmitted passwords must be encrypted.
- 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 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 include special characters and numbers. The following is an example of how a passphrase can be created, inspired by Security Tip (ST04-002) "Choosing and Protecting Passwords"[1] and the "Password Security, Protection, and Management" article[2] from the United States Computer Emergency Readiness Team (US-CERT):

1. Think of a sentence: "Strong passwords are more secure"
2. Remove space between words in the sentence: "Strongpasswordsaremoresecure"
3. Replace some words with shorthand and/or intentionally misspell at least one word: "StrongpasswordsRmorsecure"
4. Change the case of several letters to upper case or lower case: "strongPasswordsRmOrseCure"
5. Include numbers and special characters at the beginning of the sentence, within the sentence, and/or after the sentence: "5tr0ngP@ssword$RmOrseCure!"

Another method to create a strong password is to use the first letter of each word in a sentence. For example:

1. Think of a sentence: "Using long and complex passwords enhances security for the organization"
2. Begin creating the password by using the first letter of each word in the sentence and use numbers logically for some words: "Ulacpes4to"
3. Change the case of several letters in the sentence and add several special characters and numbers: "ULacp!s4to"

3.2 Administrative Passwords

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

- Passwords must be at least 15 characters in length.

[1] Uniform Resource Locator (URL): http://www.us-cert.gov/cas/tips/ST04-002.html

[2] URL: http://www.us-cert.gov/reading_room/PasswordMgmt2012.pdf

- Passwords must contain at least 2 upper case letters, 2 lower case letters, 2 numbers, and 2 special characters.
- New passwords must change at least 6 characters from the last password.
- The password lifetime must not exceed 90 days.
- 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 shall meet the following requirements:

- Passwords must be at least 15 characters in length.
- Passwords must contain at least 2 upper case letters, 2 lower case letters, 2 numbers, and 2 special characters.
- 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 must be changed whenever an individual (i.e., system administrator) with knowledge of the password leaves the NRC or is assigned to another position without the system administrator responsibilities for that system.
- Passwords must not be reused for 24 generations.

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

Please note that all unclassified desktop and laptop systems must meet the requirements for information and systems categorized with a sensitivity of high. However, tablets must meet the requirements for the information system with which the tablet is associated. If the tablet is not assigned to an information system, the tablet must meet the requirements associated with the systems accessed by and the information stored on the device.

Passwords used to protect information and systems that process Sensitive Unclassified Non-Safeguards Information (SUNSI) shall meet the following requirements:

- Passwords length must be at least:
  - Mobile phones: 8 characters
  - Not Mobile phones:
    - Systems/information with a security categorization of **high**: 12 characters
    - Systems/information with a security categorization of **moderate**: 10 characters
    - Systems/information with a security categorization of **low**: 8 characters

- Passwords must contain at least:
  - Mobile phones: 3 of the following: 1 upper case letter, 1 lower case letter, 1 number, and 1 special character
  - Not Mobile phones:
    - Systems/information with a security categorization of **high**: 2 upper case letters, 2 lower case letters, 1 number, and 1 special character
    - Systems/information with a security categorization of **moderate**: 2 upper case letters, 2 lower case letters, 1 number, and 1 special character
    - Systems/information with a security categorization of **low**: 1 upper case letter, 1 lower case letter, 1 number, and 1 special character
- New passwords must change at least:
  - Mobile phones: 3 characters from the last password
  - Not Mobile phones:
    - Systems/information with a security categorization of **high**: 4 characters from the last password
    - Systems/information with a security categorization of **moderate**: 3 characters from the last password
    - Systems/information with a security categorization of **low**: 2 characters from the last password
- The password lifetime must not exceed:
  - Mobile phones: 90 days
  - Not Mobile phones:
    - Systems/information with a security categorization of **high**: 90 days
    - Systems/information with a security categorization of **moderate**: 120 days
    - Systems/information with a security categorization of **low**: 180 days
- The password minimum lifetime must not be less than:
  - Mobile phones: 24 hours
  - Not Mobile phones:
    - Systems/information with a security categorization of **high**: 24 hours
    - Systems/information with a security categorization of **moderate**: 12 hours
    - Systems/information with a security categorization of **low**: 6 hours
- Passwords must not be reused for:
  - Mobile phones: 24 generations

- Not Mobile phones:
    - Systems/information with a security categorization of **high**: 24 generations
    - Systems/information with a security categorization of **moderate**: 15 generations
    - Systems/information with a security categorization of **low**: 10 generations

3.5 Passwords Used to Protect Safeguards Information and Systems

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

- Passwords must be at least 15 characters in length.
- Passwords must contain at least 2 upper case letters, 2 lower case letters, 2 numbers, and 2 special characters.
- New passwords must change at least 6 characters from the last password.
- The password lifetime must not exceed 90 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, shall meet the following requirements:

- Passwords must be at least 15 characters in length.
- Passwords must contain at least 2 upper case letters, 2 lower case letters, 2 numbers, and 2 special characters.
- New passwords must change at least 6 characters from the last password.
- The password lifetime must not exceed 90 days.
- The minimum password lifetime must not be less than 24 hours.
- Passwords must not be reused for 24 generations.

3.7 Personal Identity Verification Personal Identification Numbers

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

APPENDIX A. ACRONYMS

CSO	Computer Security Office
DAA	Designated Approving Authority
IT	Information Technology
NRC	Nuclear Regulatory Commission
PCT	Policy, Compliance, and Training
PIN	Personal Identification Number
PIV	Personal Identity Verification
SGI	Safeguards Information
SITSO	Senior Information Technology Security Officer
ST	Security Tip
STD	Standard
SUNSI	Sensitive Unclassified Non-Safeguards Information
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Readiness Team

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.
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.
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
02-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
30-Apr-15	1.3	Modified to address passwords for application and service accounts.	Distribution at ISSO forum and posting on CSO web page	Upon request