Newfoundland Labrador

Office of the Chief Information Officer

Standard

Password Management

Governance

Authority:	Treasury Board
Audience:	All staff, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons entrusted to access or use the Government Network and/or IT assets on behalf of the OCIO.
Compliance Level:	Mandatory
Issuing Public Body:	Office of the Chief Information Officer Infrastructure & Security Branch Information Protection Division
Original Issue Date:	2011-01-05
Date Last Reviewed:	2023-07-30
OCIO Reference:	DOC02393/2011
Version Number:	5.0

Notice:

The Office of the Chief Information Officer (OCIO) is mindful of creating and delivering accessible materials, in line with the Government of Newfoundland and Labrador's Accessible Communications Policy. New materials created by OCIO align with policy requirements and modifications to existing materials will occur as part of the standard review cycle.

This document is available in alternate format. Please contact OCIO@gov.nl.ca.

Forward questions and/or comments related to this document to OCIOInfoProtection@gov.nl.ca.

Table of Contents

1.0 Overview

The password requirements outlined in this document are mandatory for Employees to follow and dictate uniform ways of issuing, securing and maintaining passwords. This Standard is issued in support of the Password Management Directive, released by the OCIO's Information Protection Division of the Infrastructure and Security Branch.

2.0 Purpose

This Standard applies to any password used to access Government of Newfoundland and Labrador (hereafter referred to as “Government”) electronic information assets developed, owned, maintained or supported by the OCIO, including but not limited to mobile devices, computers, applications, etc. Passwords, Passphrases and other secrets that are not used for authentication to Government electronic information assets are excluded from the scope of this Standard.

The requirements in this Standard are mandatory for all Government departments and public bodies supported by the OCIO to follow.

3.0 Definitions and Acronyms

A complete listing of terms are located on the OCIO website - Information Management and Protection (IM&P) Glossary of Terms.

Authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system (Source: NIST SP 800-63-3; IR-7298 Rev. 3).

Electronic Information Asset – Information within a Government of Newfoundland and Labrador application or information system and/or device that has value to the organization.

Encryption – The process of changing plaintext into cipher text for the purpose of security or privacy (Source: NIST SP 800-21 Rev. 2; CNSSI-4009-2015).

Enterprise Architecture (EA) Division – This division is responsible for the development and implementation of enterprise architecture. EA provides support, guidance, and expertise to IT programs and projects from ideation to closure, performs research, identifies business and information technology trends and best practices, and recommends appropriate solutions, methodologies, and strategies for achieving organizational goals.

Employee – For the purpose of this Standard, “Employee” includes staff, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons of departments and public bodies, supported by the OCIO, that are entrusted to access Government electronic information assets.

Information Protection (IP) – Information Protection is an area of practice focused on the protection of information from inappropriate access or use, using a variety of means as required; including, but not limited to, policy and standards; physical and electronic security measures; and compliance monitoring and reporting. Information Protection represents the point at which the management of information converges with security policy and measures. In the Government of Newfoundland and Labrador, public bodies are required to protect information as part of their accountability under Section 6 of the Management of Information Act SNL2005 c.M-1.01.

Information Protection and Security (IP&S) Program – The comprehensive, organized collection of documented policies, directives, standards, guidelines and processes that are used to continuously deliver information protection and security across the OCIO (Source: Deloitte).This program is managed by the I&S Branch and is focused on governance, policy and standards; planning and strategy; education and awareness; information risk management; monitoring and compliance; and executive incident response.

Information Protection and Security (IP&S) Policy Framework – Outlines the roles, responsibilities and processes for Information Security policies, directives, standards and guidelines within the OCIO. It also provides the overall model and the supporting method and responsibilities for making the OCIO policies, directives, standards and guidelines a vital element in the overall IP&S Program. The framework depends upon communication and coordination between the various stakeholders to ensure that overall risk is well managed.

Non-production environments – Any environment outside of production, including any or all of development, testing, staging or training environments.

Passphrase – Is a type of Password that is generally longer but less complex (Source: NIST SP 800-63-3; NIST IR-7298 Rev. 3).

Password – A secret, typically a character string (i.e., letters, numbers and other symbols) or a Passphrase that a claimant uses to authenticate its identity (Source: NIST SP 800-63-3; NIST IR-7298 Rev. 3).

Privileged Account Users – Individuals who have access to set “access rights” for users on a given system. Also referred to as system or network administrative accounts (Source: NIST SP 800-12)

The table below includes common abbreviations used by OCIO as well as acronyms found within this document.

Abbreviation	Description
AES	Advanced Encryption Standard
EA	Enterprise Architecture
Government	Government of Newfoundland and Labrador
IM	Information Management
IM&P	Information Management and Protection
IP	Information Protection
IP&S	Information Protection and Security
I&S	Infrastructure and Security
IT	Information Technology
MOIA	Management of Information Act
OCIO	Office of the Chief Information Officer
SHA	Secure Hash Algorithm

4.0 Requirements

4.1 Password Issuance, Security and Maintenance – System

a) The minimum password length must be of at least eight (8) characters with at least two from a mixture of uppercase and lowercase letters, numbers and/or special characters.

b) Passwords must be changed periodically at intervals of 90 days or less.

c) Temporary and/or initial passwords must not be used more than once.

d) Temporary or initial passwords must be set to expire automatically after a maximum of 24 hours.

e) Users must be forced to change temporary and/or initial passwords immediately upon first time use of that password.

f) Passwords in clear-text must not be embedded inside application code or automated scripts.

g) Passwords must not be delivered or communicated in clear-text (e.g., email). Acceptable methods for delivering and/or communicating passwords include:

   i. In person (i.e., face to face);

   ii. Telephone (i.e., the telephone number has been verified as belonging to the authorized user and user identity is confirmed prior to providing the password);

   iii. Voicemail, if the mailbox is dedicated to the authorized recipient (i.e., not a group voicemail) and the number has been verified as belonging to that authorized user;

   iv. Call-back model (i.e., inform the user to contact OCIO for the password; OCIO can verify user identity before distribution of the password to that user (e.g., ask the user to provide details of why they are contacting the OCIO); and

   v. Via secure mail (i.e., tamper-proof envelopes, certified mail, etc.).

h) Passwords must be encrypted with AES or hashed with SHA of minimum 256 bits or equivalent when transmitted over an unsecured channel.

i) Passwords stored electronically (e.g., in configuration files or automated scripts) must be encrypted with AES or hashed with SHA of minimum size 256 bits or equivalent.

4.2 Password Issuance, Security and Maintenance – User

a) Users must change initial password within 24 hours of issuance.

b) Passwords must not contain, or be the reverse of, usernames, user IDs or their variations.

c) Passwords must not contain an individual's personal information (e.g., names, telephone numbers, dates of birth, names of family members, pets, addresses, etc.).

d) Use of "Remember Password" functions or unapproved utilities to store passwords electronically (i.e., key-ring applications) is not allowed.

4.3 Administrative Passwords

a) Passwords for privileged user accounts (e.g., supervisor, root, and administrator) must be unique and not used for other accounts.

b) All administrative passwords within an electronic information asset must be changed if system compromise is suspected or confirmed.

c) When an administrative user's account has been revoked, the password for that account must be changed and the account disabled.

d) Passwords used in production environments must be different from those used in the non-production environments. Passwords must be changed whenever electronic information assets are moved from non-production to production environments.

e) Prior to placing an electronic information asset into a production environment, all vendor supplied default passwords must be changed.

5.0 Roles and Responsibilities

It is the responsibility of all Employees granted access to, or assigned management of, Government electronic information assets to know their responsibilities as set out in this Standard and other IP&S policies, directives, standards and guidelines, and to conduct their activities accordingly. In addition, the following specific responsibilities apply:

OCIO Corporate Services and Projects Branch (Enterprise Architecture Division)

- Development, implementation and maintenance of this Standard
- Oversight and issuance of Exemptions related to this Standard
- Education and awareness of this Standard across Government
- Education and awareness of any related standards and guidelines across Government

OCIO Infrastructure and Security Branch (Information Protection Division)

- Development, implementation and maintenance of the Password Management Directive
- Education and awareness of any related directives across Government
- Oversight of the IP&S Policy Framework

Employees

- Understanding of responsibilities as outlined in this Standard
- Protection of passwords from unauthorized access, use or disclosure
- Adherence to this Standard and any related directives and guidelines

OCIO Security Council

- Review and approval of this Standard

Deputy Ministers (or Equivalent)

- Enforce this Standard across their Department or Public Body

6.0 Compliance and Enforcement

Compliance monitoring

Compliance monitoring of this Standard is the responsibility of the OCIO's Corporate Services and Projects Branch (EA Division).

Enforcement of this Standard is the responsibility of the Deputy Minister or equivalent of each department or public body, as per the Management of Information Act, and the Information Management and Protection Policy as approved by Treasury Board, under which it is issued. Where necessary, enforcement will be undertaken by the OCIO in accordance with requirements to secure the Government Network and electronic information assets.

Mandatory compliance

Adherence to this Standard is mandatory.

Penalty for failure to comply

Willful non-compliance with this Standard, including contravention through negligence, may result in disciplinary action, up to and including termination of employment, contract or access, in accordance with the Government's human resources policies.

7.0 Supporting Materials and Version History

Supporting Materials

Below is a listing of supporting materials hyperlinked to the published location.

Management of Information Act
https://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm

Human Resource Policies
https://www.gov.nl.ca/exec/tbs/working-with-us/alpha-policies/

Information Management and Protection Policy
https://www.gov.nl.ca/exec/ocio/im/policy-instruments/im-ip-policy/

Version History

The following table highlights the version history of this document including date issued and version number.

Date (yyyy-mm-dd)	Version
2011-01-05	1.0
2013-11-01	2.0
2018-03-16	3.0
2018-10-25	3.1
2019-08-23	4.0
2023-07-30	5.0