Newfoundland
Labrador

Office of the Chief Information Officer

Guideline

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:	Recommended
Issuing Public Body:	Office of the Chief Information Officer Infrastructure & Security Branch Information Protection Division
Original Issue Date:	2010-09-20
Date Last Reviewed:	2023-07-30
OCIO Reference:	DOC02394/2011
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

This Guideline is issued in support of the OCIO’s IP&S Password Management Directive and the OCIO’s Password Management Standard.

2.0 Purpose

The statements in this Guideline are meant to provide ‘recommended approaches’ for managing passwords. While these statements are not currently mandatory, Employees are strongly encouraged to follow them to ensure adequate protection and security of passwords.

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.

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.

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.

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.

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

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

Abbreviation	Description
EA	Enterprise Architecture
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
OCIO	Office of the Chief Information Officer

4.0 Recommended Approach

4.1 Password Construction

- Passwords should contain mixes of uppercase, lowercase, numbers and punctuation:
    - Alphabets – A...Z, a...z
    - Digits – 0 to 9
    - Special characters – (e.g., !; £; $;); (; %; &; *; #; @; ?; {; }; [;]; =; +; >; <; “)
- Passwords should not include any words which are vulnerable to dictionary attacks (i.e., consist of words included in dictionaries).
- Each password should be significantly different from previously used passwords.
- Tips for creating strong passwords:
    - String several words together
    - Shift a word up, down, left, or right one row on the keyboard
    - Free of consecutive identical, all-numeric, or all-alphabetic characters
    - Transpose characters in a word by a certain number of letters up or down the alphabet
    - Transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word
    - Combine punctuation or numbers with a regular word
    - Create acronyms from words in a song, poem, or another known sequence of words
    - Deliberately misspell a word
    - Combine several preferences like hours of sleep desired and favorite colors

Sample Password Constructs

Original Phrase	Constructed Passwords
“to be or not to be”	2.be.0r.nOt@to0.bEE
“Dressed to the nines”	Dressed*2*the*9z
“bank” and “camera”	B@nkC@mera
“mail” and “phone”	m4!lf0N3

Note: Do not use these sample passwords as your password.

4.2 Password Issuance, Security and Maintenance

- Passwords should be used in combination with other authentication methods (i.e., multi-factor authentication) where stronger authentication and identity verification is required.

- Passwords should be entered with caution to prevent viewing by others nearby.

- Change test user password immediately upon completion of the test effort.

- Immediately report known or suspected compromises of passwords to an immediate supervisor, manager, or the OCIO Service Desk at (709-729-4357) or servicedesk@gov.nl.ca.

- Some passwords may not have expiry enforced through an automated password facility. In such cases, manual processes and procedures should be implemented to ensure periodic password changes.

- Passwords for service accounts (i.e., system and application accounts) should be of at least 15 alphanumeric characters and randomly generated.

- Passwords should be eligible for reuse every 5 passwords.

4.3 Administrative Passwords

- Precautions should be taken by system administrators to prevent loss and/or compromise of administrative passwords by secure backup and storage of the passwords.

- The minimum password length should be of at least 15 characters with a mixture of letters, numbers and special characters unless 2-factor authentication is implemented.

5.0 Roles and Responsibilities

It is the responsibility of all Government Employees granted access to, or assigned management of, Government electronic information assets to know their responsibilities as set out in this Guideline 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 Guideline
- Oversight and issuance of Exemptions related to this Guideline
- Education and awareness of this Guideline across Government

OCIO Infrastructure and Security (I&S) Branch (Information Protection Division)

- Development, implementation and maintenance of 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 Guideline
- Protection of passwords from unauthorized access, use or disclosure
- Adherence to this Guideline and any related directives and standards

OCIO Security Council

- Review and approval of this Guideline

Deputy Ministers (or Equivalent)

- Enforce this Guideline across their Department or Public Body

6.0 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
2010-09-20	1.0
2013-01-29	2.0
2015-01-13	2-year Review completed (No updates required)
2018-03-16	3.0
2018-10-25	3.1 (Updated TBM Number and Branch Names)
2019-08-23	4.0 (Updated as part of 3-Year review cycle)
2023-07-30	5.0