Office of the Chief Information Officer

Directive

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:	2011-02-02
Date Last Reviewed:	2023-07-30
OCIO Reference:	DOC02392/2011
Version Number:	4.0

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

Passwords are a common way to provide identification and authentication based on a secret known only by the user. A password helps authenticate a user when accessing an electronic information asset. Password selection, strength, usage and management are primary methods used to control electronic access and, where practical, should align with industry standards and best practices. Adherence to appropriate Password Management processes will help maintain the confidentiality, integrity and availability of Government of Newfoundland and Labrador (hereafter referred to as "Government") information and reduce the risk of inappropriate access to and use of electronic information assets.

2.0 Purpose

This Directive will state expectations and establish rules for managing and protecting passwords used in accessing Government electronic information assets.

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).

Availability – The property of being accessible and useable upon demand by an authorized entity (source ISO/IEC 27000:2018); Ability of a component or service to perform its required function at a stated instant or over a stated period of time. It is usually expressed as the availability ratio, i.e., the proportion of time that the service is actually available for use by the customers within the agreed service hours (Source: ITIL).

Confidentiality – The property that information is not made available or disclosed to unauthorized individuals, entities, or processes (Source: ISO/IEC 27000:2018); Upholding required restrictions against unauthorized access or disclosure of information (e.g., personal information, Cabinet confidences, trade secrets).

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

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 Directive, "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) 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.

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 IP Division, of the Infrastructure and Security 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.

Integrity – The property of safeguarding the accuracy and completeness of assets (Source: ISO/IEC 27000:2018).

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 Passphrase 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
Government	Government of Newfoundland and Labrador
IM&P	Information Management and Protection
IP	Information Protection
IP&S	Information Protection & Security
I&S	Infrastructure & Security
OCIO	Office of the Chief Information Officer
SLT	Senior Leadership Team

4.0 Statements

1. Where possible, user identity shall be verified before issuance or reset of any password.
2. Passwords must be communicated in a secure manner.
3. Passwords must be delivered or communicated directly to the intended recipient.
4. Where possible, Employees shall change temporary and/or initial passwords immediately upon first time use of that password.
5. Passwords, including administrative passwords, must be treated as confidential and protected from unauthorized access, use or disclosure.
6. Passwords must not be written down in any form (e.g., taped to desk walls or terminals, stored in list finders, desk drawers, etc.).
7. Employees must not share or otherwise disclose their passwords.
8. Any password suspected of compromise must be changed immediately.
9. Passwords must not be circumvented without valid reasons and approval.
10. Government-approved mobile devices (e.g., BlackBerry, iPhones, etc.) must be protected by a password.
11. Where possible, passwords shall not be stored within the electronic information asset in an unprotected form.
12. Passwords must be created, issued, used and maintained in accordance with related Password Management standards and/or guidelines.

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 Directive and other IP&S policies, directives, standards and guidelines, and to conduct their activities accordingly. In addition, the following specific responsibilities apply:

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

- Development, implementation and maintenance of this Directive
- Education and awareness of this Directive across Government
- Issuance of Exemptions related to this Directive
- Oversight of the IP&S Policy Framework

OCIO Corporate Services and Projects Branch (Enterprise Architecture Division)

- Development, implementation and maintenance of any related standards and guidelines
- Education and awareness of any related standards and guidelines across Government

All Government Employees

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

OCIO Security Council

- Review and recommendation for approval of this Directive to the Senior Leadership Team (SLT)

OCIO Senior Leadership Team

- Approval of this Directive

Deputy Ministers (or Equivalent)

- Enforce this Directive across their Department or Public Body

6.0 Compliance and Enforcement

Mandatory compliance

Adherence to this Directive is mandatory for all Government Employees.

Enforcement

Enforcement of this Directive 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.

Penalty for failure to comply

Willful non-compliance with this Directive, including contravention through negligence, may result in disciplinary action by the Employer, 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

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

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

Version History

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

Date (yyyy-mm-dd)	Version
2011-02-02	1.0
2013-11-01	2.0
2018-10-25	2.1
2019-08-23	3.0
2023-07-30	4.0