Newfoundland Labrador

Office of the Chief Information Officer

Standard

Remote Access and Administration

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:	2019-09-10
Date Last Reviewed:	2023-07-30
OCIO Reference:	DOC03461/2019
Version Number:	2.0

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 remote access requirements outlined in this document are mandatory for Employees to follow and dictate a consistent approach to establishing, securing and controlling remote access connections for supported Information Technology (IT) Assets.

In the context of this Standard, "Employee" includes 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.

2.0 Purpose

This Standard applies to any remotely initiated connection granting an Employee access to a Government of Newfoundland and Labrador (hereafter referred to as “Government”) IT Asset, owned, maintained or supported by the OCIO. The requirement is specific to remote access that enables remote administration or operating system interface visibility.

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)

Credential **–** A unique physical or electronic object (or identifier) issued to, or associated with, an individual, organization or device. I.e., Unique Identifier, Account, Username, ID. (Source: GoC - Guideline on Defining Authentication Requirements)

Firewall – A part of a computer system or network that is designed to block unauthorized access while permitting outward communication. (Source: NIST SP 800-152)

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.

Information Technology Assets – For the purpose of this Standard, "Information Technology Assets" include, but are not limited to; Government assigned employee IT assets, enterprise infrastructure and platform assets such as desktops, laptops, tablets, servers, networking, storage, and security devices.

Multi-Factor Authentication – using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See Authenticator (Source: NIST SP 800-53 Rev. 4)

Privilege (account) User – A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. Abbreviations and Synonyms: root user, super user. (Sources: NIST SP 800-171 Rev1 NIST SP 800-53 Rev4)

Remote Access – Access by users (or information systems) communicating external to an information system security perimeter. Network access is any access across a network connection in lieu of local access. (Source: NIST SP 800-53)

Role-Based Access Control – A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities. (Source: NIST SP 800-95)

Security Service – Mechanisms used to provide confidentiality, integrity authentication, source authentication and/or support non-repudiation of information. (Source: NIST SP 800-57 Part 1 Rev. 4)

Single-Factor Authentication – A characteristic of an authentication system or an authenticator that requires only one authentication factor (something you know, something you have, or something you are) for successful authentication. (Source: NIST SP 800-63-3)

User interface – The physical or logical means by which users interact with a system, device or process. (Source: NIST SP 800-152)

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

Abbreviation	Description
DNS	Domain Name System
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
PIN	Personal Identification Number

4.0 Requirements

This Standard establishes a consistent approach for initiating, securing and monitoring remote access connections for supported Information Technology (IT) Assets.

4.1 Remote Access General

a) Remotely initiated access to IT Assets owned, maintained or supported by the OCIO must originate from, or transverse through, the designated OCIO Security Service.

b) IT Assets owned, maintained or supported by the OCIO must be protected by a local or enterprise firewall to ensure remotely initiated access attempts can only be established via the designated OCIO Security Service.

c) Only credentials bound to an Employee are permissible. Shared or guest credentials are not allowed.

d) At minimum, Employees must validate their credential with the designated OCIO Security Service using Single-Factor Authentication.

e) Authenticated Employees must be placed into a profile or group allowing role-based access control to be applied, limiting remote access to just those IT assets required to execute their assigned duties and responsibilities.

f) At a minimum, log all remote access attempts, successful or otherwise, including the source and target Asset Domain Name System (DNS) name and/or IP address, Employee identifier, time and remote access method.

4.2 Remote Access for Privileged Account Users; Connecting to Employee Assets

a) Includes all requirements listed in Section 4.1.

b) Remote access attempts using privileged accounts must be monitored and a notification sent to the Employee's direct supervisor.

4.3 Remote Access for Privileged Account Users; Connecting to Enterprise Assets

a) Includes all requirements listed in Section 4.1, with the exclusion of 4.1 (d).

b) Replacing 4.1 (d): Employees must validate their credential with the designated OCIO Security Service using Multi-Factor Authentication.

5.0 Monitoring of the Network and IT Assets

The Network, its components and all Government IT assets are the property of the Employer and not the property of the Employee. The Employer can add, remove, update and/or block any content, technical or otherwise, and view all Government records (as well as any other records, which may be generated, stored on or handled by Government-issued assets), if that action is deemed necessary for the maintenance or security of the Network, or if inappropriate use is suspected. The Employer maintains the right to monitor the Network, its components and all Government IT assets for the purposes of maintenance, repair and management; to ensure continuity of service; to improve business processes and productivity; to meet its legal requirement to produce information; and to prevent misconduct and ensure compliance with the law. The Employer may forward IT assets and/or information to law enforcement agencies when deemed necessary.

Employees should be aware these assets, equipment and resources are monitored and will be searched where necessary for the maintenance or security of the Network and government's overall IT environment, or if inappropriate use is suspected, by those authorized to do so on behalf of the Employer or law enforcement agencies.

6.0 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 Infrastructure and Security Branch

- 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 Remote Access and Administration standard
- 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

7.0 Compliance and Enforcement

Compliance monitoring

Compliance monitoring of this Standard is the responsibility of the OCIO's Infrastructure and Security Branch.

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.

8.0 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/

Access to Information and Protection of Privacy Act, 2015
http://www.assembly.nl.ca/Legislation/sr/statutes/a01-2.htm

Rooms Act
https://assembly.nl.ca/legislation/sr/statutes/r15-1.htm

OCIO Website
https://www.gov.nl.ca/exec/ocio/

Version History

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

Date (yyyy-mm-dd)	Version
2019-09-09	1.0
2023-07-30	2.0