2023-2026

BUSINESS PLAN

Office of the Chief Information Officer

Newfoundland & Labrador

MESSAGE FROM THE MINISTER

As Minister responsible for the Office of the Chief Information Officer, I am pleased to present this business plan for the Office of the Chief Information Officer covering April 1, 2023 to March 31, 2026. The Office of the Chief Information Officer is a category two government entity and this plan was prepared in accordance with the applicable guidelines required for multi-year performance-based plans.

The goals and objectives identified in this plan will guide the Office of the Chief Information Officer in providing modern secure technology, day-to-day service, along with information management services, to enable and protect government departments, agencies, boards and commissions under its mandate.

In accordance with the **Transparency and Accountability Act**, the Office of the Chief Information Officer has identified the following areas (modernize, enable and protect) to guide its work over the next three fiscal years. The progress and achievements of this plan will be provided in each annual report. I look forward to working with the Office to advance these initiatives.

My signature is indicative to the accountability for the preparation of the plan and achievement of its goals and objectives.

Hon. Sarah Stoodley
Minister Responsible for the Office of the Chief Information Officer

Table of Contents

Introduction

Overview

The Office of the Chief Information Officer (OCIO) was established under the **Executive Council Act**. It is a category two entity under the **Transparency and Accountability Act** and is responsible for providing information technology (IT) support, developing information management (IM) and information protection (IP) policies and standards, and providing IT and IM/IP advisory/consulting services to government departments and other primary clients under its mandate.

The OCIO supports the business of government with over 10,000 computers, over 1,500 servers, over 800 software applications and services, a significant network infrastructure, and a comprehensive province-wide area network. This varied and complex environment requires security frameworks, preventative maintenance, disaster recovery plans, capacity planning, and software license monitoring and management.

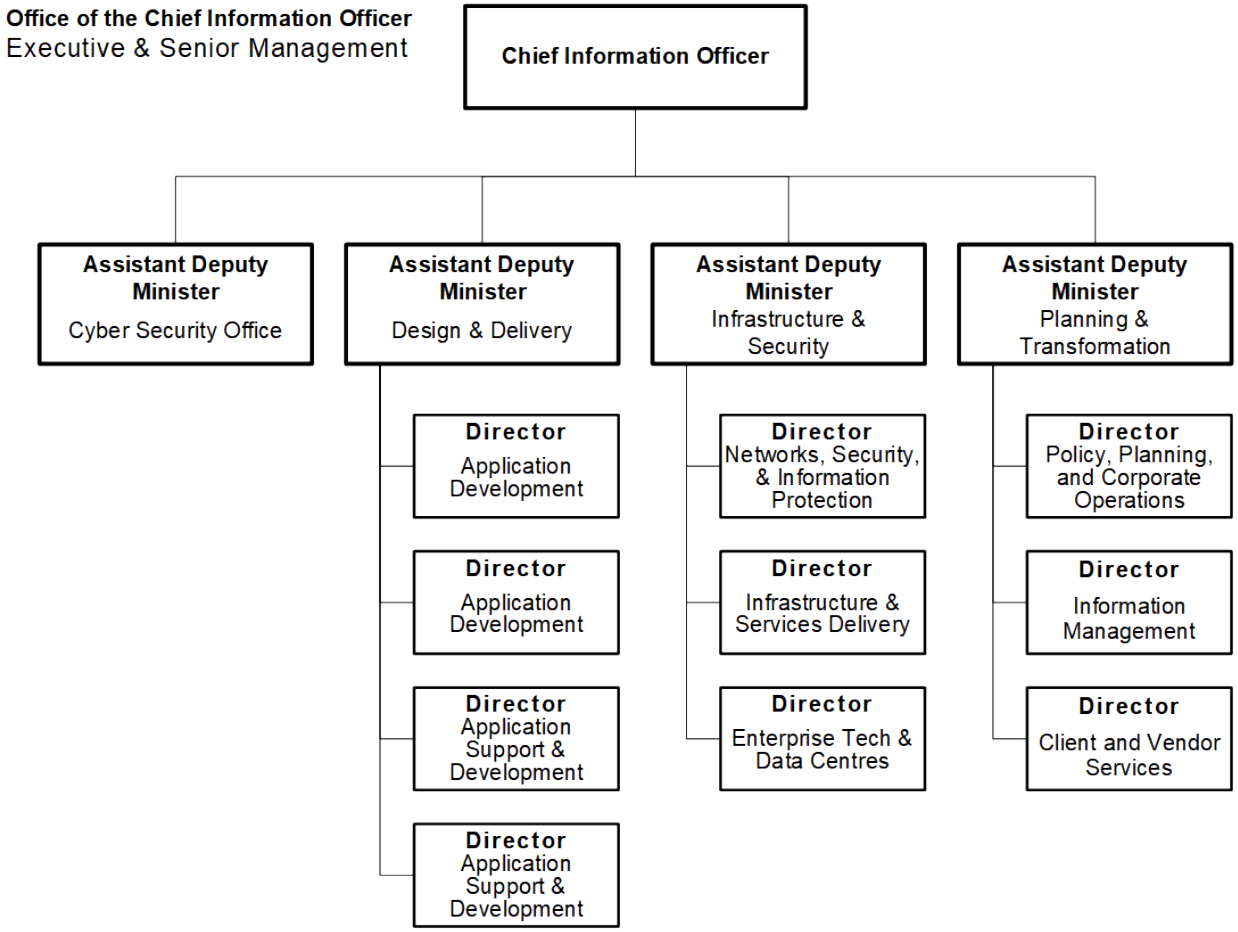
As of March 31, 2023, the OCIO had 294 employees. The majority of employees are located in offices throughout St. John's and Mount Pearl. There are 15 employees distributed among the OCIO's regional offices in Happy Valley-Goose Bay, Stephenville, Corner Brook, Grand Falls-Windsor, Gander, and Clarenville.

Further information about the OCIO, can be found at: www.gov.nl.ca/ocio/office.

Organizational Structure Chart

The OCIO is structured into four branches as follows:

1. Cyber Security Office;
2. Design and Delivery;
3. Infrastructure and Security; and
4. Planning and Transformation.



The Cyber Security Office is pivotal in leading cyber security initiatives within government departments and public bodies in the Province of Newfoundland and Labrador. The Office is committed to protecting government assets, along with the integrity and confidentiality of data throughout the province, and works collaboratively to fulfill its mandate.

The Office's initiatives emphasize delivering innovative cyber programming and guidance for awareness aligned with the Government's objectives and priorities.

The Office aims to prevent and address cyber security attacks proactively with standards, best practices, guidelines, and directives (including cyber training, phishing campaigns, social engineering, monitoring, audit and compliance).

The Office provides business continuity and disaster recovery capability guidance including incident response planning services and incident response support.

The Planning and Transformation Branch is responsible for information management, corporate services, client services, and vendor services. Information Management Division administers the **Management of Information Act** which includes developing IM directives, standards, procedures, and guidelines; and providing IM advisory services and guidance to government departments and other public bodies.

The Corporate Services Division is responsible for: the OCIO's business operations; financial management (budget preparation and monitoring); vendor contract management; human resource planning; IT procurement oversight; cabinet support; facilities management; and, occupational health and safety.

The Client and Vendor Services Division is responsible for: client engagement and alignment of OCIO's strategic direction with the needs of client departments, agencies, boards, and commissions to enable better program and service delivery to citizens and businesses; vendor engagement to enable local IT industry partnerships; and, stakeholder engagement for planning, monitoring, and reporting.

The Design and Delivery Branch is responsible for the Project Management Office (PMO), project delivery, application development and support, the MyGovNL program, and the enterprise application team that supports government's administrative solutions

(finance and human resources). The PMO manages the framework and methodology for project delivery, portfolio management, and reporting. The PMO works very closely with the project delivery division which is responsible for ensuring projects are delivered to our stakeholders and support the adoption of the technology they deliver. The application development team is responsible for most of the software development activities, which includes developing new solutions and supporting and enhancing existing applications. The MyGovNL team is responsible for the entirety of the MyGovNL program, which includes development, support, integration, and service roadmap. The enterprise application team supports all the enterprise applications used across government in the areas of finance, budgeting, and human resources, as well as database technologies. The branch works in collaboration with Digital Government and Service NL to define the overall digital government strategy.

The Infrastructure and Security Branch provides: day-to-day, front-line support to ensure OCIO clients have what they need to deliver government programs and services; back-end technology support and maintenance; cyber security services to ensure the integrity and availability of government's assets including computers, mobile devices, networking, storage, data backup, server infrastructure, enterprise data centre, enterprise infrastructure applications and related technologies; and information protection program and related advisory services to government.

Budget

The 2023-2024 budget for the OCIO is $49,787,700.

Branch	# of Employees	Budget
Operations and Security	116	$27,275,900
Application & Information Management Services	114	$10,152,700
Corporate Services and Projects	64	$12,359,100
	294	$49,787,700

Note: the above budget is prior to OCIO reorganization

Mandate

The OCIO operates as an entity within the Executive Council and is governed by the **Executive Council Act** and is responsible for:

- Information technology and information management coordination, planning, budgeting, and policy development;
- Customer support daily to line departments;
- Cyber security protection to GNL technology assets;
- Developing and operating computer systems and infrastructure for government departments, agencies, boards and commissions that are directly supported by the administrative support services of departments;
- Expenditures and procurement of information technology goods and services;
- Administering the **Management of Information Act;**
- Managing information technology related agreements and contracts;
- Providing consultative services, particularly in the area of information management; and
- Working collaboratively with the private information technology sector to maximize business opportunities while meeting the information technology and information management needs of government.

Lines of Business

In delivering its mandate, the OCIO's organizational structure is aligned with its lines of business to clients:

- Cyber Security Office;
- Design and Delivery;
- Infrastructure and Security; and
- Planning and Transformation.

Vision

To enable the business of government, by establishing an inclusive, modern workforce providing industry class daily support, modern technology, and information management services to the public service and citizens of Newfoundland and Labrador.

Business Issues

The business direction, goals, and objectives in this plan were prepared in consideration of the strategic directions of government and the departments that the OCIO supports. The OCIO identified the following three areas to guide its business plan over the next three fiscal years.

Issue One: Modernize

Information technology is constantly evolving and creating new opportunities for innovation. As announced in Budget 2023-2024 Modernizing Government's Information Technology Assets, the OCIO will undertake a three-year journey to modernize government's information technology assets, associated policies, and staff skills to spur innovation, operational improvements, and connectivity with the province's citizen and business stakeholders securely.

Goal

By March 31, 2026, the OCIO will have modernized its workforce, its processes (e.g., operational and service delivery frameworks), and government's foundational technologies.

Indicators

Goal progress will be measured by completion of:

- Cyber security, solution delivery, cloud computing, disaster recovery, and government data framework modernization;
- IM policy modernization;

- Cyber security policy modernization;
- Operational controls and tier one service modernization;
- Collaboration technology modernization;
- Enterprise resource planning and case management enhancements;
- Government Wi-Fi and mobile workforce expansion;
- Legacy technology replacement;
- Employee training, skills, apprenticeship, and wellness program implementation; and
- Organizational structure and process modernization.

Objective 2023-2024

By March 31, 2024, the OCIO will have implemented the first year of a three-year modernization plan.

Indicators

Objective progress will be measured by completion of:

- Cyber security, solution delivery, and cloud programming framework modernization;
- IM policy modernization;
- Operational controls and tier one service modernization;
- Government Wi-Fi and WAN expansion;
- Collaboration technology delivery;
- Enterprise resource planning enhancements;
- Process modernization; and
- Employee training, skills, and wellness program implementation.

Objective 2024-2025

By March 31, 2025, the OCIO will have implemented the second phase of the modernization plan.

Objective 2025-2026

By March 31, 2026, the OCIO will have implemented the operational sustainment phase of the modernization plan.

Issue Two: Enable

The OCIO will enable government's departmental visions and goals through enhanced operational support, modern technology, and partner advisory services.

Goal

By March 31, 2026, the OCIO will have:

- Expanded evidence-based decision-making technologies for government departments;
- Implemented more online services to improve citizen and business interactions with government;
- Enhanced departmental partnerships to maximize the potential and value of government's technology investment; and
- Enhanced service to departments.

Indicators

Goal progress will be measured by completion of:

- MyGovNL technology modernization and service expansion;
- Government data collection, standardization, access, and usability improvements;
- Digital credential verification initiative advancement;
- Modern technology implemented for line departments, including departmental technology innovation process;
- Customer service process enhancement; and
- End user modern technology training program implementation.

Objective 2023-2024

By March 31, 2024, the OCIO will have expanded online services for citizens of the province and improved services for government departments.

Indicators

- Enhanced customer service processes for government departments;
- Deployed modernized collaborative technologies to the public service;
- Planned enterprise resource planning modernization for government departments;
- Implemented required technology for line departments; and
- Expanded accessibility.

Objective 2024-2025

By March 31, 2025, the OCIO will have:

- Continued online service expansion; and
- Continued implementing modern functionality with associated training to line departments.

Objective 2025-2026

By March 31, 2026, the OCIO will have:

- Continued online service expansion;
- Continued implementing modern functionality with associated training to line departments; and
- Enabled modern mobile technology.

Issue Three: Protect

Cyber security threats against government assets are evolving and increasing. Citizens and businesses trust government to provide services and keep their assets safe from unauthorized access and usage. The OCIO will continue to evolve its cyber security

programming to protect the Government of Newfoundland and Labrador against dynamic security threats to sustain asset availability, integrity, and confidentiality.

Goal

By March 31, 2026, the OCIO will have:

- Implemented the Cyber Security Office;
- Fostered cyber security resources and culture within government's public service;
- Modernized the cyber security framework including partnerships with subject matter experts; and
- Proactively strengthened (secured) government's cyber security posture in response to evolving technology and constant security risks.

Indicators

Goal progress will be measured by progress towards:

- Educating the public service with cyber awareness training;
- Updating cyber protection technology, processes, and skills; and
- Collaborating with partners for advisory services.

Objective 2023-2024

By March 31, 2024, the OCIO will have:

- Established the Cyber Security Office implementation plan;
- Strengthened cyber security resourcing;
- Delivered cyber security training;
- Refreshed the cyber security awareness program;
- Modernized the cyber security framework;
- Updated cyber technology;
- Required partnerships; and
- Strengthened foundational technologies.

Objective 2024-2025

By March 31, 2025, the OCIO will have continuous awareness of the cyber threat landscape and adjusted required operational frameworks, procedures, and continued to expand cyber security education and awareness across government.

Objective 2025-2026

By March 31, 2026, the OCIO will have continued to evolve government's cyber security program and provided additional cyber security education and awareness to public service.

Annex A – Strategic Directions

Government's strategic directions are generally communicated through platform documents, throne and budget speeches, policy documents, and other communications. The **Transparency and Accountability Act** requires departments and public bodies consider these strategic directions in the preparation of their performance-based plans.

The OCIO will advance government's information management / information technology strategic direction through its 2023-2026 Business Plan.

The following is the OCIO's strategic direction for 2023-2024.

Strategic Direction:

Modernizing and protect to enable government departments, agencies, boards, and commissions under its mandate.

Outcome:

Further enable and protect the business of government.