Auditor General
MANITOBA

Report to the Legislative Assembly

Managing IT Security for Remote Access

Independent Assurance Report

WEBSITE VERSION

March 2024

This page is intentionally left blank.

Auditor General
MANITOBA

March 2024

Honourable Tom Lindsey
Speaker of the Legislative Assembly
Room 244, Legislative Building
450 Broadway
Winnipeg, Manitoba R3C 0V8

Dear Mr. Speaker:

It is an honour to submit my report, titled *Managing IT Security for Remote Access*, to be laid before Members of the Legislative Assembly in accordance with the provisions of Section 28 of *The Auditor General Act*.

Respectfully submitted,

Original Signed by:

Tyson Shtykalo, CPA, CA
Auditor General

Office: 204.945.3790 | 500-330 Portage Avenue | Winnipeg, Manitoba R3C 0C4 | oag.mb.ca

This page is intentionally left blank.

Table of contents

This page is intentionally left blank.

Auditor General's comments

The global COVID-19 pandemic transformed the traditional workplace structure. Employees in a variety of sectors learned to work remotely, or share time between home and the office. Technological advancements made this possible, providing new ways to access and share information, and collaborate remotely.

In response to this shift, the Province of Manitoba implemented a flexible work arrangements policy for its core public service employees in June 2021. The policy formalized expectations for those employees working remotely – whether full time or hybrid. The policy also recognized the need for strong IT security controls in the remote work environment due to added security threats, as information should remain safe regardless of location, remotely or in the office.

I am encouraged that Manitoba has introduced security measures to protect information and systems used by employees to work remotely, but there is room for some improvement. This audit found the Province uses encryption to protect data-in-transit but some settings could be strengthened. This audit also found not all employees have completed mandatory security awareness training. Addressing these findings ensures a more secure remote work environment.

This report includes 3 recommendations. A separate letter addressed to management was also provided to present findings that contain sensitive security information. I encourage the Department of Consumer Protection and Government Services and the Public Service Commission to act on our recommendations in this report and management letter to resolve the risks identified by this audit.

I would like to thank provincial government officials and staff we met during our audit for their cooperation and assistance. I would also like to thank my audit team for their efforts.

Original Signed by:

Tyson Shtykalo, CPA, CA
Auditor General

This page is intentionally left blank.

Report highlights

Why we did this audit

- In June 2021, the Province of Manitoba (the Province) introduced a flexible work policy resulting in the adoption of a hybrid work model, where core public employees can work remotely on specific days.
- Information systems and data must be adequately protected when staff work remotely.
- We wanted to determine if the Province has processes and controls that mitigate IT security risks in the remote work environment.

Conclusion

The Province is managing IT security risks associated with remote work, but some improvements are needed.

This audit includes 3 RECOMMENDATIONS.

What we found

Data security

Information is protected but encryption settings need improvement

- Data is encrypted in the remote work environment, but some encryption settings need to be amended to improve security.

Device authentication and patching

Devices are authenticated and securely patched

- Remote workers must use devices issued by the Province. Access to these devices is controlled through multi-factor authentication.
- An automated patch management process ensures that security-related updates are applied to all computers.

Vulnerability and incident management

Security vulnerabilities and incidents are identified and mitigated promptly

- The Province has a process for responding to and resolving security incidents and disruptions related to the technologies used by remote workers.
- Remote work technologies are regularly scanned to identify and resolve vulnerabilities.

Security awareness training

Many employees have not completed mandatory information security awareness training

- All Manitoba government employees are required to take the Manitoba Information Security Awareness training course within the first 2 months of employment.
- As of March 31, 2023, 31% of employees had not completed this training.

Policies and procedures

Security policies and procedures are outdated

- IT security policies and procedures related to remote work have not been updated in many years.

Background

Remote work has become increasingly popular and feasible due to advances in technology, high-speed internet connectivity, and the changing nature of many jobs that can be performed digitally. On June 28, 2021, the Manitoba Public Service Commission (PSC) took steps to increase opportunities for remote work arrangements by introducing the **flexible work arrangements** policy that allowed **core public service** employees to work from home or anywhere other than their offices.

Per PSC's policy, remote work is a flexible work arrangement whereby an employee has approval to carry out some or all their work duties from an alternate location, typically the employee's primary residence, on a re-occurring or on-going basis. A remote work arrangement may be full-time or partial, split between the work headquarters and the alternate location.

A **flexible work arrangement** is an agreement between management and an employee to adjust the employee's location of work and/or hours on a re-occurring or on-going basis.

Source: Section 1.2.4 of Public Service Commission Policies

The **core public service** consists of the Clerk of the Executive Council, the other deputy ministers, and the employees in positions within the departments of government.

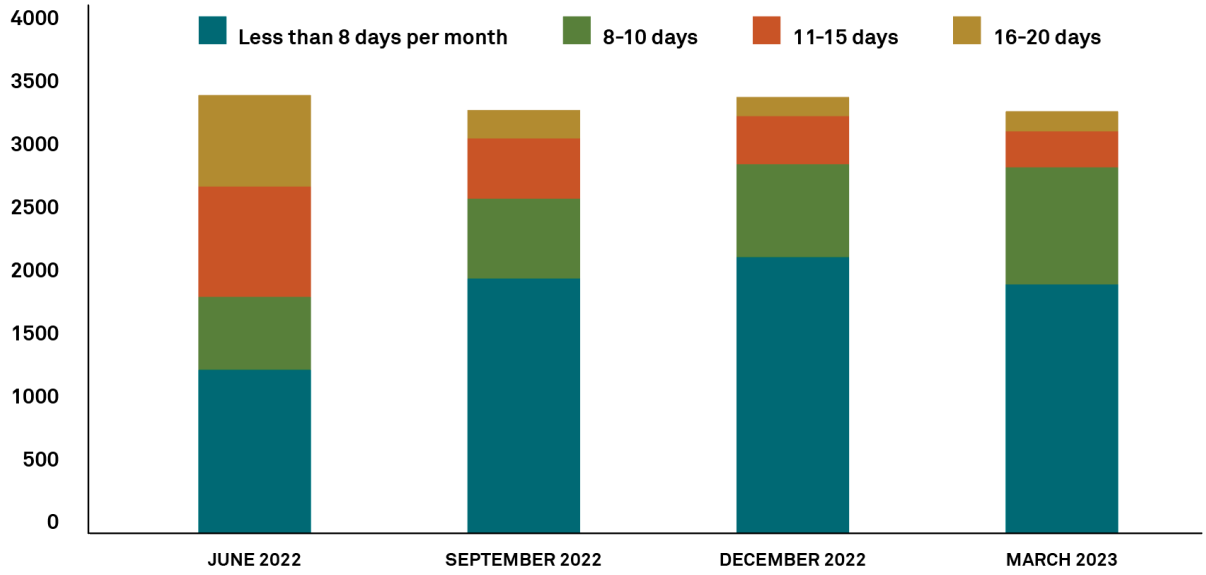
Source: Manitoba Public Service Act

This flexible work arrangement has become a tool to ensure continuity of essential government functions during the recent public health emergency. And while the COVID-19 pandemic is over, remote work continues to play a key role in the workplace. According to a Business Development Canada study completed in March 2021, 54% of employees surveyed said that access to remote work is a determining factor when applying or accepting a job. In a more recent poll by Angus Reid completed in April 2023, half of employees who were surveyed said that they would look for a new job if their employers wanted them back full time in their offices. As such, allowing remote work gives employers access to a bigger talent pool and capability to retain their current resources.

Prior to the pandemic, remote work was limited in the public sector due to technology limitations or reluctance to disrupt established norms. In Manitoba, there were less than 1,000 members of core public service employees working remotely. However, as the pandemic surged and public health emergencies and lockdowns were in place, the Province of Manitoba (the Province) had to quickly adapt to enable its core public service employees to work remotely and continue to provide services to its citizens. The pandemic compelled investment into remote technology because of necessity.

The number of days for remote work varies in each workweek, but remote workers significantly grew and have remained at around 3,500 employees for the period of June 2022 to March 2023. Refer to **FIGURE 1** below.

Figure 1 – Number of core public service employees working remotely – June 2022 to March 2023



Source: Public Service Commission

Remote work helped keep employees safe during the COVID-19 pandemic. However, it has increased IT security threats that can put systems and data at risk. According to the March 2020 Information Technology Laboratory bulletin of the US National Institute of Standards and Technology (NIST), "Telework and remote access technologies often need additional protection because their nature generally places them at higher exposure to external threats compared to technologies that are only accessed from inside the organization." Security threats or concerns about remote work during the audit period of June 2021 to June 2023 include:

1. Information that is stored and transmitted using remote devices is not protected from unauthorized access	Unauthorized access to sensitive information can result in data breaches. This can lead to the exposure of confidential data, including personal and financial information of Manitobans. Data breaches can be costly to resolve and could also damage the Province's reputation.
2. Devices used for remote work are not securely patched before granted access to the Province's network.	Remote workers could use devices infected with malware. When the devices connect to the Province's network, the malware could spread to other IT assets, such as computers, servers, and applications, if there is no mechanism to detect, quarantine, and clean those devices before they connect to the network.

3. Security vulnerabilities and incidents impacting remote workers are not identified and mitigated promptly.	Security issues and vulnerabilities left unaddressed may escalate into larger and more destructive incidents. For example, a single compromised remote worker's device could potentially be used as a point to launch attacks on other parts of the Province's network.
4. Employees do not receive regular training on and awareness of remote work risks and mitigation practices.	Without adequate training regarding the security risks of working remotely, employees are more likely to fall victim to phishing attacks, malware, and other cyber threats. Remote workers may also be more susceptible to tactics that manipulate them into revealing sensitive information or performing actions that compromise security—things that could be addressed by a proper employee training and security awareness program.

As a result of the security threats noted above, it is important to have IT security controls in the remote work environment (such as at home) to make sure information systems and data remain protected as effectively as they would be in the office.

In this audit, we examined the controls implemented to mitigate IT security risks of remote work arrangements. This includes an examination of IT security processes, policies and practices, inspection of information system and data protection measures, and assessment of security training and guidance provided to employees.

This page is intentionally left blank.

Roles and responsibilities

Digital and Technology Solutions

The General Manual of Administration establishes Digital and Technology Solutions (DTS, formerly known as Business Transformation and Technology or BTT) as the Province of Manitoba's central agency for information and communication technology (ICT) management. In terms of managing the IT security of remote work arrangements, DTS is responsible for:

- Setting province-wide IT policies and procedures that govern remote work arrangements.
- Deploying devices and technologies to aid in the remote work of government employees.
- Implementing controls to prevent and detect security incidents to remote devices and technologies.
- Supporting the Public Service Commission with developing a security awareness training program for government employees.

DTS is also responsible for leading the work to secure Manitoba government's data, systems, and electronic networks, while aligning IT security policies and practices with the Province's priorities and risk tolerances.

Public Service Commission

The Public Service Commission (PSC) is responsible for leading effective human resource and workforce relations management in the government and representing the public interest in the administration of *The Public Service Act* (the Act) and regulations.

The Act requires the Province of Manitoba (the Province) to develop and implement policies for flexible work arrangements. In response, the PSC created the flexible work arrangements policy in collaboration with Central Payroll, Insurance and Risk Management Branch, Accommodation Services Division, Digital and Technology Solutions, Legal Services Branch and Remote Advisory Panel. The flexible work arrangements policy applies to roughly 13,000 members of core public service and became effective on June 28, 2021.

In relation to managing remote work arrangements, PSC responsibilities include:

- Setting policies and procedures that govern remote work arrangements for the Province.
- Deploying the DTS-developed security awareness training program through PSC's training platform.
- Monitoring departmental compliance on completion of mandatory security awareness training.

This page is intentionally left blank.

Objective, scope and approach, and audit criteria

Objective

Our objective was to determine if the Province of Manitoba (the Province) has processes and controls that mitigate IT security risks in the remote work environment.

Scope and approach

The audit included the inspection of documents, procedures, standards, reports, and other documentation relevant to the Province's processes to manage IT security risks in a remote work environment. We interviewed key process owners and stakeholders within Digital and Technology Solutions (DTS) and Public Service Commission (PSC) to understand the processes and activities in place to manage IT security when conducting work at a workplace other than the government's premises.

The audit examined practices and controls from June 2021 to June 2023. Since the flexible work policy only applies to members of the core public service of the Province, our population included those who are defined as core public service per *The Public Service Act* (the Act). We also included contractors used for resource augmentation within these departments as part of our population.

Members of the broader and allied public service were excluded from this audit. Per the Act these include:

- Broader public service – Chief Executive Officer and employees of:
  - Crown corporations
  - Shared Health Inc.
  - Regional health authorities
  - Universities
  - School districts
- Allied public service – staff for the Assembly offices and the constituency offices of members of the Assembly, the staff for the officers of the Legislature, and political staff.

This audit did not cover contractors who are not used for resource augmentation, such as those used for outsourced services (for example, Kyndryl, DXC).

Audit criteria

To determine whether the Province of Manitoba has processes and controls that mitigate IT security risks in the remote work environment, we used the following criteria:

Criteria	Sources
Criteria 1: Information that is stored and transmitted using remote devices should be protected from unauthorized access.	National Institute of Standards and Technology (NIST) Cybersecurity Framework • PR.DS Data Security • PR.PT Protective Technology
Criteria 2: Devices used for remote work should be authenticated and securely patched before granted access to the Province's network.	NIST Cybersecurity Framework • PR.AC Access Controls • PR.MA Maintenance • DE.CM Security Continuous Monitoring
Criteria 3: Security vulnerabilities and incidents impacting remote workers should be identified and mitigated promptly.	NIST Cybersecurity Framework • RS.MI Mitigation
Criteria 4: Employees should receive regular training in and awareness of remote work risks and mitigation practices.	NIST Cybersecurity Framework • ID.GV Governance • PR.AT Awareness and Training

The Province is managing IT security risks associated with remote work, but some improvements are needed

The COVID-19 pandemic drove the transition from traditional office-based work to remote work arrangements. While remote work capabilities already existed pre-pandemic, the worldwide mandate by governments for non-essential workers to stay home during lockdowns made remote work more common and accepted. Now that COVID-19 is no longer viewed as a public health emergency of international concern, the Province of Manitoba's flexible work arrangement policy ensures that employees who choose a **hybrid work arrangement** are supported. This work flexibility resulted in rapid deployment of security controls by Digital and Technology Solutions (DTS) to protect an extended perimeter due to diverse remote locations.

A **hybrid work arrangement** is a work model that supports a blend of in-office and remote working.

We concluded that the Province of Manitoba (the Province) has implemented controls to manage IT security risks related to a remote workforce, however, there are some improvements needed to strengthen these controls. We based this conclusion on the following findings:

- Information stored and transmitted using remote devices is protected but encryption settings need to be improved **(SECTION 1)**.
- Devices used for remote work are authenticated and securely patched **(SECTION 2)**.
- Security vulnerabilities and incidents impacting remote workers are identified and mitigated promptly **(SECTION 3)**.
- Mandatory security awareness training has not been completed by many employees **(SECTION 4)**.
- Security policies and procedures are outdated **(SECTION 5)**.

1 Information is protected but encryption settings need improvement

The Province uses encryption to protect data stored and transmitted by remote workers. According to the Center for Internet Security (CIS), encryption is a cryptographic operation that is used to enhance security and protect electronic data by transforming readable information (plaintext) into unintelligible information (ciphertext). CIS is a non-profit entity who develops, validates, and promotes timely best practice solutions that help people, businesses, and governments to protect themselves against cyber threats.

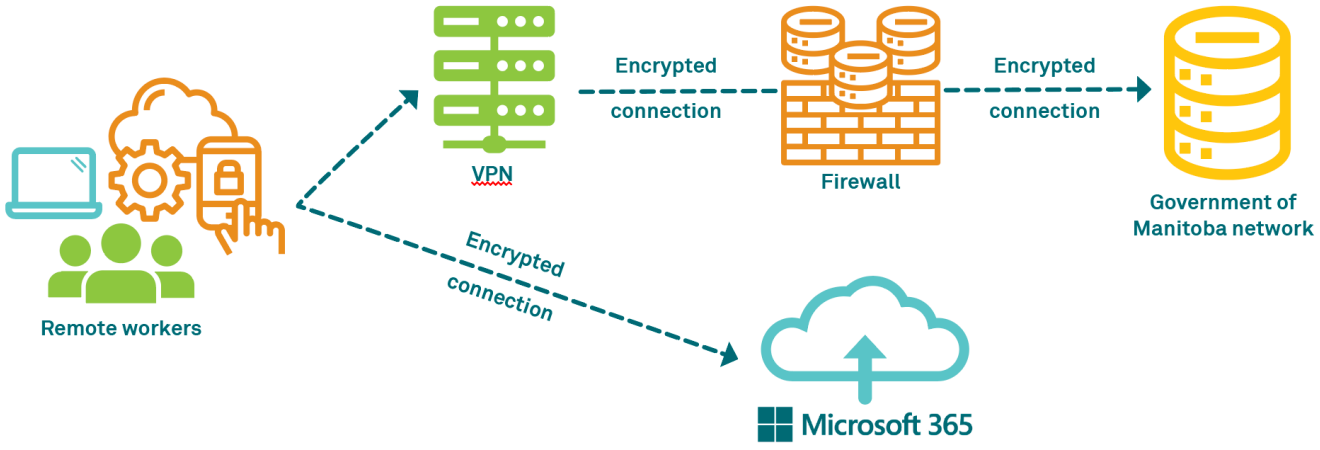
Workstations, including laptops and desktops, are encrypted to prevent unauthorized data disclosure. Secure file transfer with email is available for sending sensitive information in an encrypted format. The data transmitted between the Province's network and a remote worker's computer on their home network is also protected through a virtual private network (VPN). As defined by Canadian Centre for Cyber Security, a VPN is a secure connection between 2 points. It acts as a tunnel that can be used to send and receive secure data on an existing physical network.

Cloud computing is a model that enables on-demand network access to computing resources such as networks, servers, storage, application, and services, that can be rapidly provisioned with minimal management effort or service provider interaction.

Source: NIST Special Publication 800-145

Microsoft Office 365 (including its collaboration tool Microsoft Teams) was deployed by DTS to support remote workers' productivity. This is a subscription-based business software service hosted by Microsoft in the **cloud**. Users are not required to connect to the VPN to use Microsoft Office 365 applications. However, users still need to have a user account with the Province to access these cloud resources. The non-use of VPN for Microsoft Office 365 does not imply less secured connections. Microsoft provides an encrypted connection between the user and the desired Microsoft Office 365 application.

Figure 2 – This diagram shows connections to Microsoft 365 are sent directly to that service. All other traffic traverses the VPN.



While encryption is a good method to secure connections, we noted some encryption settings and configurations that could be improved to optimize the security of these connections.

We identified instances where weak encryption could be used for data-in-transit with remote workers. In these instances, the encryption did not meet the Manitoba Information and Communication Technologies Standards (ICT Standards). The ICT Standards establish best practices for securing data and systems and contain security recommendations and requirements to prevent data compromise using strong encryption.

If a cyber attacker were to intercept a communication with weak encryption, they could use techniques to decrypt and read the data, which could expose sensitive and confidential data to unauthorized access.

Due to the sensitive nature of these security settings, our detailed findings and recommendations were presented to DTS in an internal letter.

Recommendation 1

We recommend DTS review and update encryption settings to meet provincial standards as presented in our letter to management.

2 Devices authenticated and securely patched

Access to a virtual private network (VPN) is not the sole layer of security in place to access the Province of Manitoba's network resources. Aside from the requirement of having a network account, a remote worker needs to have a managed device, a VPN, and a **token** for multi-factor authentication. A managed device includes computers formatted and issued by the Province of Manitoba (the Province). The Province also takes care of patches of these computers.

A patch management process is in place to apply security related updates to these managed devices. A patch is a modification or update made to correct functional and security deficiencies. We found managed devices used for remote work are automatically updated with the latest patches once they connect to the internet, either through hardwire connection or VPN. Errors during patch deployment are monitored. The error messages are reviewed, and patches are re-sent when necessary.

A **token** is something that a user possesses and controls and is used to authenticate the user's identity. For example, it could be a device that is in the possession of the user that generates one-time passwords that are displayed and manually entered. Even though it is referred to as a "device", this authenticator can be either a distinct physical device or a software application running on a general-purpose device such as a smartphone.

Source: Definition - NIST Federal Information Processing Standards 201-3; Example – NIST Special Publication 800-63B

3 Security vulnerabilities and incidents are identified and mitigated promptly

There is a Service Desk function that handles the Province of Manitoba's incident management process to respond and resolve security incidents and disruptions affecting its IT environment including the technologies used by remote workers. Service Desk personnel use an incident management system that records and tracks incidents reported by employees, whether working remotely or not.

Likewise, a vulnerability management process is in place. This process is governed by Digital and Technology Solutions' (DTS) Vulnerability Management Standard which mandates regular vulnerability scan cycles for the Province of Manitoba's IT environment including remote servers, workstations, and network devices. The process aims to identify vulnerabilities on devices that are likely to be used by attackers to exploit to gain access to a device and use it as a starting point for further network compromise. A vulnerability is a weakness that could allow an attacker to compromise an information system. DTS monitors security sources for vulnerability announcements and threats that correspond to hardware and software used commonly in the government.

We found vulnerabilities are evaluated to identify their impact and determine the necessary remediation action. There are 3 primary methods of remediation that can be applied to an affected system during the audit period of June 2021 to June 2023—the installation of a software patch, the adjustment of a configuration setting or the removal of the affected software.

4 Mandatory information security awareness training not completed by many employees

Business Email Compromise is a type of cybercrime where the scammer uses email to trick someone into sending money or divulging confidential company info.

Source: Microsoft Security

The Province of Manitoba (the Province), through the Public Service Commission (PSC), requires all its employees to take the Manitoba Information Security Awareness (ISA) training course. The course teaches users about **Business Email Compromise** (BEC) attacks, which include phishing and social engineering tactics, as well as flash drive threats. For remote work, the training covers topics such as avoiding the use of public networks, using the Province's VPN, and encrypting sensitive data. Every government employee is required to complete this mandatory core training, which is essential in demonstrating the skills and knowledge expected of such employees. Completion of this training is expected within the first 2 months of employment.

PSC monitors the completion of this training and provides non-compliance reporting to the departments on a quarterly basis through a digital dashboard. These statistics are reviewed by deputy ministers and are included in departments' balanced scorecard reporting. Likewise, departments can also generate

their own reports showing which staff completed the mandatory training. Both the PSC and the departmental reports are used to ensure that everyone has taken this training.

PSC's monitoring found 3,843 employees (31%) had not completed the required Manitoba ISA training as of March 31, 2023. We selected a sample of 67 employees who are working remotely to determine if they have completed this mandatory training. We noted 5 employees had not completed the Manitoba ISA training, all of whom were hired more than 12 months ago.

Four of these 5 employees are at the Director or Executive Director levels. Employees at this level are expected to set the tone and culture for an organization, including its approach to cybersecurity. By participating in information security training, they demonstrate a commitment to security and serve as role models for other employees.

PSC is responsible for notifying departments about staff who have not completed the training. The departments are responsible for enforcing completion of the Manitoba ISA training to all their staff, whether they are remote workers or not, by sending them reminders. Other than the reminder, there is no strong adverse consequence given to anyone who has not completed the mandatory Manitoba ISA training within the expected completion time.

The Manitoba ISA training is crucial for educating employees about potential threats, safe practices, and the importance of maintaining security procedures. The completion of this training ensures that all employees, especially those working remotely:

- Are equipped with necessary knowledge of how to suitably use the government's network.
- Could recognize and respond to threats accordingly.
- Reduce cyber-attacks caused by human errors.

Human error is a major threat to cybersecurity. In 2022, a World Economic Forum report found that 95% of cybersecurity issues could be traced back to human error. Remote workers who have not undergone security training are more likely to fall victim to phishing emails and other social engineering tactics. This can result in compromised credentials, malware infections, and data breaches.

Recommendation 2

We recommend that PSC work with departments to develop escalation procedures that ensure employees complete mandatory training, including the Manitoba Information Security Awareness training. The escalation procedures should consider consequences, such as disabling system access, if training is not completed in a reasonable timeframe.

5 Security policies and procedures are outdated

The adoption of flexible work arrangements introduced new threats to the security landscape of the Province of Manitoba (the Province) as well as a rapid increase in the use of information technology assets related to remote work. It is essential to review and update policies and procedures to address the threats and technology related to remote work. For example, the Province has an increased use of mobile phones and tablets to perform work-related activities, but mobile devices are not explicitly included as an information and communication technology asset in the Manitoba Password Standard. As such, when compared to the Standard, mobile devices appear non-compliant.

We noted the following policies, procedures, and guideline documents are outdated:

Documentation	Last updated
Standards of Best Practice for Information Security Management	January 2003
Manitoba Electronic Media Disposal Standards and Procedures	November 2005
Data Classification Guide	December 2012
Information and Communication Technology Policy	July 2013
Guideline for securing information and Communication Technology assets while travelling	June 2014
Manitoba Password Standard	June 2015
Manitoba Baseline Security Controls	June 2016
Vulnerability Management Standard	November 2016

Information technology security policies, procedures and guidelines help the Province adapt to changing circumstances and provide direction to staff on evolving security practices. These documents are essential to establish and maintain a strong information security posture. Updating these policies and procedures would address current security threats and will also encourage a culture of continuous improvement.

Outdated policies could lead to confusion among employees about proper security practices, potentially resulting in unintentional security breaches. Lastly, if training programs are based on outdated documentation, it could also misinform employees, rendering training efforts ineffective.

During our fieldwork, we noted that a Standard Operating Procedure was approved in May 2023 which requires Digital and Technology Solutions (DTS) leadership and policy analysts to review these documents annually. We were informed by DTS management that this was implemented to ensure the policies are reviewed and updated.

Other audits with findings related to outdated policies and procedures:

- *Information Systems – Privileged Access*, October 2022
- *Aging Information Systems*, February 2022
- *Vital Statistics Agency*, September 2020

Recommendation 3

We recommend DTS:

a. Annually review and update outdated policies, procedures, and guidelines to reflect current best practices and regulatory requirements, in accordance with the standard operating procedure.
b. Provide training and awareness to educate employees about the updated documents and security measures.

This page is intentionally left blank.

Additional information about the audit

This independent assurance report was prepared by the Office of the Auditor General of Manitoba on the management of IT security in a remote work environment. Our responsibility was to provide objective information, advice, and assurance to assist the Legislature in its scrutiny of the government's management of resources and programs, and to conclude on whether Digital and Technology Solutions (DTS) and the Public Service Commission (PSC) comply in all significant respects with the applicable criteria.

All work in this audit was performed to a reasonable level of assurance in accordance with the Canadian Standard for Assurance Engagements (CSAE) 3001—Direct Engagements set out by the Chartered Professional Accountants of Canada (CPA Canada) in the CPA Canada Handbook—Assurance.

The Office applies Canadian Standard on Quality Control 1 and, accordingly, maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

We have complied with the independence and other ethical requirements of the Code of Professional Conduct of the Chartered Professional Accountants of Manitoba, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behaviour.

In accordance with our regular audit process, we obtained the following from management:

- Confirmation of management's responsibility for the subject under audit.
- Acknowledgement of the suitability of the criteria used in the audit.
- Confirmation that all known information that has been requested, or that could affect the findings or audit conclusion, has been provided.

Period covered by the audit

The audit covered the period between June 2021 and June 2023. This is the period to which the audit conclusion applies.

Date of the audit report

We obtained sufficient and appropriate audit evidence on which to base our conclusion on February 9, 2024, in Winnipeg, Manitoba.

This page is intentionally left blank.

Summary of recommendations and responses from officials

Recommendation 1

We recommend DTS review and update encryption settings to meet provincial standards as presented in our letter to management.

Response of officials:

The Department of Consumer Protection and Government Services (CPGS) agrees with the recommendation and will work to address the specific findings in the letter to management.

Recommendation 2

We recommend that PSC work with departments to develop escalation procedures that ensure employees complete mandatory training, including the Manitoba Information Security Awareness training. The escalation procedures should consider consequences, such as disabling system access, if training is not completed in a reasonable timeframe.

Response of officials:

The PSC agrees with the recommendation and will undertake a review of how to improve the completion of mandatory Information Security Awareness (ISA) course by public servants, including the escalation procedures. This will include leveraging tools and/or processes available as a result of new technology and functionality with the integration of the new SAP system and SuccessFactors modules.

Recommendation 3

We recommend DTS:

- Annually review and update outdated policies, procedures, and guidelines to reflect current best practices and regulatory requirements, in accordance with the standard operating procedure.
- Provide training and awareness to educate employees about the updated documents and security measures.

Response of officials:

a. Department of CPGS agrees with the recommendation and will continue to regularly review policies, procedures, guidelines, and standards to reflect best practices and the environment.

b. The Department of CPGS agrees with the recommendation and will implement processes to keep training and awareness tools up to date.

This page is intentionally left blank.

Vision
Government accountability and public administration excellence for Manitobans.

Mission
To provide independent information, advice and assurance on government operations and the management of public funds.

Values
Independence – We are independent from government and our work is objective and unbiased.
Integrity – We act with honesty and uphold high ethical standards.
Innovation – We promote innovation and creativity in what we do and how we do it.
Teamwork – We work as a team by sharing each other's knowledge and skills to reach our goals.

Auditor General
Tyson Shtykalo

Assistant Auditor General
Wade Bo-Maguire

Principal, IT Audit
Ian Montefrio

Senior IT Auditor
Tony Chu

Communications Manager
Frank Landry

Director, Infrastructure and Cybersecurity
Andrew Robertson

Admin Support
Jomay Amora-Dueck
Alex Dela Cruz
Tara MacKay
Wendy Rasmussen

Graphic Design
Waterloo Design House

The Office of the Auditor General of Manitoba acknowledges with respect that we conduct our work on the ancestral lands of Anishinaabeg, Anishininewuk, Dakota Oyate, Denesuline, and Nehethowuk Nations, and on the National Homeland of the Red River Métis. We respect the Treaties that were made on these territories, we acknowledge the harms and mistakes of the past, and we dedicate ourselves to move forward in partnership with Indigenous communities in a spirit of reconciliation and collaboration.

WEBSITE VERSION

Auditor General
MANITOBA

For more information, please contact our office at:

Office of the Auditor General
500-330 Portage Avenue
Winnipeg, Manitoba R3C 0C4
Phone: 204-945-3790
contact@oag.mb.ca | www.oag.mb.ca

@AuditorGenMB
@AuditorGenMB
@AuditorGenMB
company/manitoba-auditor-general