Auditor General
MANITOBA

Report to the Legislative Assembly

Information Systems – Privileged Access

Independent Audit Report

Website Version

October 2022

This page is intentionally left blank.

Website Version

Auditor General
MANITOBA

October 2022

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

Dear Madam Speaker:

It is an honour to submit my report, titled *Information Systems – Privileged 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

Tyson Shtykalo, CPA, CA
Auditor General

Office: 204. 945.3790 | 500-330 Portage Avenue | Winnipeg, Manitoba R3C 0C4 | oag.mb.ca

Website Version

This page is intentionally left blank.

Website Version

Table of contents

Website Version

This page is intentionally left blank.

Website Version

Auditor General's comments

Information systems help the Province of Manitoba (the Province) deliver a range of services, including health care, online registrations, provincial program applications, and fee payments. These systems contain a considerable amount of personal, health, and corporate information, making them a target for cyber threat actors.

The Province relies on privileged users to administer these information systems. Privileged users can add and remove users, modify privileges, change system configurations and security settings, and alter data tables. An unauthorized individual with privileged access could potentially steal data or funds, disrupt operations, or cause system outages. As a result, government standards mandate additional controls be applied to protect privileged access.

In previous reports we've noted issues regarding poor controls and a lack of monitoring of privileged users' activities. Unfortunately, we continue to identify similar issues in this report. We found that the Province is not adequately controlling privileged access rights to prevent unauthorized access to information systems. I've included 5 recommendations in this report.

Given the sensitive nature of cyber security, more detailed findings and additional recommendations were presented to the Department of Labour, Consumer Protection and Government Services, and to Shared Health, in internal letters. It's imperative that action on these recommendations be taken immediately.

I would like to thank management and staff from the Department and from Shared Health for their cooperation and assistance during this audit. I would also like to thank my audit team for their dedication and hard work.

Original Signed by:
Tyson Shtykalo

Tyson Shtykalo, CPA, CA
Auditor General

Other audits with findings related to cybersecurity controls:

- Vital Statistics Agency, September 2020
- eChart Manitoba, October 2018
- WRHA's Management of Risks Associated with End-user Devices, July 2015

Website Version

This page is intentionally left blank.

Website Version

Report highlights

Why we did this audit

- The Province of Manitoba (the Province) relies on information systems that contain personal, health, and corporate information to deliver a variety of services.
- Adequate controls are needed to ensure only authorized users have privileged access to these systems, allowing them to modify users' privileges, change system configurations, and alter security settings.
- Without adequate controls, there is a greater risk that cyber threat actors could gain privileged access, resulting in data theft, operational disruptions, system outages, and financial losses.

Objective

To determine if the use of privileged access rights is restricted and controlled to prevent unauthorized access to information systems.

Conclusion

The Province is not adequately controlling privileged access rights to prevent unauthorized access to information systems.

Our report includes 5 RECOMMENDATIONS.

What we found

There are inadequate controls in place to ensure privileged access rights are assigned to authorized users.

- Processes to review privileged access rights are inadequate.
- Unnecessary privileged user access is not removed promptly.
- Approvals for granting privileged access rights are not always documented.

Identification and authentication controls need strengthening.

- The standards that govern identification and authentication are inadequate.
- Information systems are not configured to enforce quality passwords.

Monitoring of privileged users' activities is inadequate.

- Processes for logging and monitoring the activities of privileged users are missing or need improvement.
- Higher-risk activities are not always identified for monitoring.

Website Version

This page is intentionally left blank.

Website Version

Background

The Province of Manitoba (the Province) relies on **information systems** to deliver a wide-range of services, including health care, online registrations, provincial program applications, and fee payments. Information systems contain significant amounts of personal, health, and corporate information that should be well-protected to prevent unauthorized access and to ensure these systems are available when needed.

An **information system** refers to a collection of multiple components, including hardware and software, involved in the collection, processing, storage, and dissemination of information.

Digital and Technology Solutions (DTS)—formerly Business Transformation and Technology—is the central agency with overall responsibility for information technology and business transformation strategy, policy, and service delivery for the Government of Manitoba. It is a branch of the Department of Labour, Consumer Protection and Government Services. DTS provides most government departments with support for their information systems. An exception is health-care information systems. These are maintained by Shared Health—the provincial health organization that coordinates the planning of patient-centred care across Manitoba and supports centralized administrative and business functions for Manitoba health organizations.

Information system users with privileged access have more privileges and authority than general users. Organizations require privileged users to perform activities such as adding users, removing users, modifying users' privileges, changing system configurations and security settings, and altering data tables. Privileged users are also known as system administrators or super-users. Information systems include business applications, **operating systems, databases,** and shared network infrastructure such as **firewalls**. It is common for information systems to have multiple privileged users. This ensures that organizations are not dependent on a single individual. To meet operational demands, DTS and Shared Health's privileged users include both government employees and vendor staff.

An **operating system** is a program that acts as an interface between the system hardware and the user. Examples are Microsoft Windows, macOS, and Linux.

A **database** is an organized collection of structured information, or data, typically stored electronically in a computer system.

A **firewall** is the part of a computer network that is designed to block unauthorized external access while permitting outbound communication from within the network.

Organizations may face significant impacts if **cyber threat actors** (CTAs) are able to obtain privileged access to information systems. These impacts could include data theft, operational disruptions, system outages,

Website Version

phishing, brute force, and **credential stuffing**. CTAs specifically target privileged users with the intention of taking control of one system as a starting point to spread to other systems across the organization.

Organizations use a variety of processes to manage privileged access, including **access provisioning, identification and authentication,** and **activities monitoring**.

Cyber threat actors are states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, or technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks.

Phishing is a technique where an attacker tricks a person through emails or text messages into revealing sensitive information or deploying malicious software on information system.

Brute force is an attack that involves repeated attempts to guess a user's password.

Credential stuffing is an attack wherein an attacker gains access to a list of credentials like passwords and tries to use them against multiple accounts to see if there's a match.

Access provisioning is the process that provides required access to users to perform their jobs and responsibilities.

Identification is the process used to establish and prove who an individual is. **Authentication** is the process of verifying the identity of a user requesting access.

Activities monitoring is regularly reviewing the activities performed by privileged users to detect suspicious behavior or security risks to information systems.

Website Version

Audit objective, scope and approach, and audit criteria

Audit objective

Our objective was to determine if the use of privileged access rights is restricted and controlled to prevent unauthorized access to information systems.

Scope and approach

This audit included the examination of documents, procedures, standards, reports, system settings and other information relevant to privileged users' management processes for information systems managed by the Digital and Technology Solutions (DTS) branch of the Department of Labour, Consumer Protection and Government Services, as well as by Shared Health.

We interviewed key process owners and stakeholders responsible for information systems to understand the controls used to restrict the use of privileged user access rights and prevent unauthorized access.

We tested varied sample sizes for assessing effectiveness of controls on the management of privileged access. We selected samples for testing from key systems holding sensitive personal, health, and corporate information and included individual, **service**, and **system accounts**.

This audit did not include testing to detect misuse of privileged access.

A **system account** is a default account that comes with the system.

A **service account** is used by an information system to run automated services and internal processes.

Audit criteria

We used the following criteria in performing this audit:

	Criteria	Sources
1.1	Controls should be in place to ensure privileged access rights are assigned to authorized users.	COSO Control 10 ISO 27002 Controls 7.1, 9.1, 9.2 CIS Control 6
1.2	Identification and authentication controls should be in place to ensure only authorized privileged users can access systems.	ISO 27002 Controls 9.4.2, 9.4.3 CIS Control 6
1.3	Monitoring of privileged users' activities should be performed to detect unauthorized activity.	ISO 27002 Control 12.4 CIS Control 6

Website Version

This page is intentionally left blank.

Website Version

Province not adequately controlling privileged access rights to prevent unauthorized access to information systems

The Department of Labour, Consumer Protection and Government Services, and Shared Health, have implemented policies and procedures to manage privileged access and to protect their information systems. However, we concluded there are inadequate privileged access controls in place to prevent and detect unauthorized access to information systems. We based this conclusion on the following findings:

- There are inadequate controls to ensure privileged access rights are assigned to authorized users **(SECTION 1)**.
- Identification and authentication controls need strengthening **(SECTION 2)**.
- Monitoring of privileged users' activities is inadequate **(SECTION 3)**.

Given the sensitive nature of the security findings, our detailed findings and recommendations were presented to the Department of Labour, Consumer Protection and Government Services, and to Shared Health, in internal letters. If this information is disclosed publicly, cyber threat actors could misuse it to compromise systems operated by these entities.

1 Inadequate controls to ensure privileged access rights are assigned to authorized users

Controls must be in place to ensure information system access rights are assigned only to appropriate authorized users. These controls help preserve the confidentially, integrity, and availability of the systems.

As part of their recruitment processes, the Department of Labour, Consumer Protection and Government Services, and Shared Health (the entities), require staff to pass security checks. To prevent unauthorized access it's important that users' access to assets is approved, and approval documentation is retained for future reference. Periodic access rights reviews should be completed to ensure access rights align with job responsibilities. Access that is not needed should be withdrawn promptly.

We found that the controls implemented by the entities to ensure privileged users are authorized and that they have the appropriate access rights, are inadequate. We based this conclusion on the following findings:

Website Version

- Shared Health does not always document approvals for granting privileged access rights **(SECTION 1.1)**.
- Unnecessary privileged user access is not removed promptly **(SECTION 1.2)**.
- There are inadequate processes to review privileged access rights **(SECTION 1.3)**.

1.1 Shared Health does not always document approvals for granting privileged access rights

Shared Health's *Information and Communication Technology (ICT) Administrative Accounts Standard* requires that privileged accounts only be created when an approval request has been submitted to the service desk.

We found no documented approvals for assigning privileged access rights to some users sampled at Shared Health. We confirmed with entity officials that these users require this access to perform their job duties. Without documented approvals there is a risk of granting individuals inappropriate access to information systems and data.

Additionally, for several of the applications we selected for testing, we found Shared Health did not identify officials who would approve access to those applications. In absence of a documented and approved list of individuals who are authorized to approve access there is a risk that inappropriate access to Shared Health systems may be granted. An approvers list is used by staff administering access to applications to validate that an access request approver has the authority to approve application access. Shared Health officials recognized the lack of formality and confirmed all access is authorized.

Recommendation 1

We recommend that Shared Health:

- Prepare a list of authorized officials who will approve access to applications.
- Grant access only after validating access approval from the authorized officials.
- Retain the access approval documents.

1.2 Unnecessary privileged user access not removed promptly

The entities' standards require access be removed promptly for terminated users. We reviewed a sample of privileged users who had left the entities. We found that access for most of those users was not promptly removed. These issues occurred across applications and infrastructure systems managed by the entities.

The processes the entities use rely on managers and supervisors to promptly submit requests to remove access. Inherently people forget things, so there is a risk managers and supervisors may not submit these

Website Version

requests. Entities can remove access promptly by integrating access removal processes with human resources processes and implementing automated workflows.

Recommendation 2

We recommend that the Department of Labour, Consumer Protection and Government Services, and Shared Health:

- Investigate and implement automated solutions to improve management of privileged access.
- Integrate access removal processes with human resources to remove users promptly.

1.3 Inadequate processes to review privileged access rights

The *Manitoba Access Control* and *Shared Health ICT Administrative Accounts* standards require that users must be reviewed on a periodic basis to ensure access privileges are appropriate and to confirm access has been deleted for individuals who have changed roles or left the entities.

We found that privileged users' access rights were not reviewed for most of the systems we selected for testing. In a few cases where the reviews were performed they were not done in a timely fashion.

We also examined certain privileged users to determine if their privileged access was required. We found several users had access that was not required and had not been removed. Performing regular reviews of privileged users and their access rights ensures access remains appropriate and unnecessary access is removed promptly.

Recommendation 3

We recommend that the Department of Labour, Consumer Protection and Government Services, and Shared Health:

- Regularly review all privileged users to verify their access rights align with their job responsibilities and to ensure unauthorized privileges do not exist.
- Remove unnecessary access promptly after the review.
- Retain the access rights review documents.

Website Version

2 Identification and authentication controls need strengthening

Identification and authentication controls are fundamental to restricting access to data and to information systems. These controls help ensure that users are who they say they are, and that they have appropriate access to systems and data.

We found weaknesses in identification and authentication controls which are used by the entities to ensure only authorized privileged users can access systems.

2.1 Identification and authentication controls need improvement

We tested a sample of information systems and found that identification and authentication controls for privileged users need to be strengthened. For example, improvements are needed to the standards that govern identification and authentication, and information systems have not been configured to enforce quality passwords as required by the Manitoba and Shared Health password standards.

Compliance with strong standards helps prevent unauthorized access to information systems. Good identification and authentication standards include multifactor authentication, minimum number of failed login attempts, inactive session terminations, minimum password length, password complexity (uppercase, lowercase, numeric, special characters), limited password life, and password history (number of previous passwords the system remembers).

Given the sensitive nature of the security findings, our detailed findings and recommendations were presented to the entities in internal letters.

Recommendation 4

We recommend that the Department of Labour, Consumer Protection and Government Services, and Shared Health, implement the identification and authentication standard and control recommendations presented in our letters to management.

Website Version

3 Inadequate monitoring of privileged users' activities

Monitoring privileged users' activities is important as it supports timely detection of malicious or accidental misuse of privileged access. Prompt detection of malicious or inappropriate activity contributes to timely response to these events and can reduce impacts such as data theft and system outages. Examples of privileged users' activities that entities may log and monitor are inappropriate systems or data changes, changes to privileged user groups, and business transactions being input with privileged IDs.

We found that the Department of Labour, Consumer Protection and Government Services and Shared Health don't adequately log and monitor privileged access to detect unauthorized activity.

3.1 Lack of privileged users' activities logging and monitoring

The *Manitoba Access Control Standard* requires that additional controls be applied to users with privileged access. These controls include applying additional audit logging and reviewing the use of privileged access.

Shared Health's *Information and Communication Technology Security* policy on logging and monitoring requires management to monitor information systems to detect security violations through an automated audit trail of security-related events.

There may be significant impacts if privileged access is misused. As a result, it's important that all privileged users' activities be logged, and activities that may indicate a security-related event be investigated. Security-related events could be inappropriate or abnormal activities. Logs are also valuable for investigation of illegal activities and may be required for compliance with legislation.

For most of the systems we tested, we found there were either no processes in place for logging and monitoring privileged users' activities, or the processes needed improvements. For example, we noted cases where the entities had not determined which privileged user activities to monitor. Determining which activities to monitor would help the entities focus their monitoring activities on the most relevant events, such as those that present the highest risk of systems being compromised. We also noted activities of some privileged user IDs were not logged and monitored.

We noted that the use of manual procedures to monitor activities is inherently time consuming and prone to errors because of the volume of events that are logged. This can lead to delays in detecting security events or events going undetected. Automated log management tools help aggregate and prioritize monitoring of the risky events.

Website Version

Recommendation 5

We recommend that the Department of Labour, Consumer Protection and Government Services, and Shared Health:

- Log all privileged user activities.
- Determine and regularly review risky activities.
- Where not already implemented, investigate methods to automate privilege user monitoring, including alerts of activity that should be reviewed.

Website Version

Additional information about the audit

This independent assurance report was prepared by the Office of the Auditor General of Manitoba on Information Systems – Privileged Access. 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 the use of privileged access rights is restricted and controlled to prevent unauthorized access to information systems.

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.

In conducting the audit work, we have complied with the independence and other ethical requirements of the Rules of Professional Conduct of Chartered Professional Accountants of Manitoba and the Code of Values, Ethics and Professional Conduct of the Office of the Auditor General of Manitoba. Both the Rules of Professional Conduct and the Code are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior.

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

1. Confirmation of management's responsibility for the subject under audit.
2. Acknowledgement of the suitability of the criteria used in the audit.
3. 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 from January 2018 to March 2022. This is the period to which the audit conclusion applies. However, to gain a more complete understanding of the subject matter of the audit, we also examined certain matters the preceding and subsequent to this audit coverage period.

Date of the audit report

We obtained sufficient and appropriate audit evidence on which to base our conclusion on August 12, 2022, in Winnipeg, Manitoba.

Website Version

This page is intentionally left blank.

Website Version

Summary of recommendations and responses of officials

RECOMMENDATION 1

We recommend that Shared Health:

- Prepare a list of authorized officials who will approve access to the applications.
- Grant access only after validating access approval from the authorized officials.
- Retain the access approval documents.

Response of Shared Health:

Shared Health has good practices in place for requesting access, both regular and privileged, to our managed systems and applications. The exceptions to our good practices identified through the audit are acknowledged and we will explore opportunities to bring these exceptions into compliance with our good practices.

RECOMMENDATION 2

We recommend that the Department of Labour, Consumer Protection and Government Services, and Shared Health:

- Investigate and implement automated solutions to improve management of privileged access.
- Integrate access removal processes with human resources to remove users promptly.

Responses of officials:

Department of Labour, Consumer Protection and Government Services:
Department of Labour, Consumer Protection and Government Services agrees privileged user access should be promptly removed when access is no longer required. Management has undertaken immediate action to audit existing privileged user access and is working a plan to address unnecessary access. To mitigate future and ongoing risk, a combination of process improvement and tools will be accessed as part of the Cyber Security Risk Reduction Program. Investigation will include assessing the level of integration required with human resources processes but understand additional measures are required over and above the integration as there are situations when privileged access changes are required without a corresponding human resources event (process).

Website Version

Shared Health:
Shared Health believes that timely removal of access is an important part of our Identity & Access Management (IAM) practices.

The exceptions to our current practices have been noted and we will explore opportunities to address them, including improving our documentation of the rationale for maintaining access after a person's support role changes (e.g., maintain access to support legacy and/or specialized technology).

Additional funding may be required to acquire the resources, both people and technology, to fully operationalize the requirements of this recommendation.

RECOMMENDATION 3

We recommend that the Department of Labour, Consumer Protection and Government Services, and Shared Health:

- Regularly review the privileged users of all information systems to verify their access rights align with job responsibilities and to ensure unauthorized privileges do not exist.
- Remove unnecessary access promptly after the review.
- Retain the access rights review documents.

Responses of officials:

Department of Labour, Consumer Protection and Government Services:
Department of Labour, Consumer Protection and Government Services' updated ICT Risk and Security process will include regular audits to verify access is required and promptly take action when deemed necessary. We will, however, require Departments to verify access levels required for their staff and in situations where systems/applications are managed or owned by Departments.

We will also collaborate with Shared Health in the future to align security practices when warranted.

Shared Health:
Shared Health believes that regular review of access rights is an important part of our Identity & Access Management (IAM) practices. We accept the feedback on our practices provided by the audit findings and improvement opportunity defined in the recommendation. We will explore opportunities to mature our practice of reviewing privilege access rights, including the proper documentation of the reviews.

Website Version

Additional funding may be required to acquire the resources, both people and technology, to fully operationalize the requirements of this recommendation.

RECOMMENDATION 4

We recommend that the Department of Labour, Consumer Protection and Government Services, and Shared Health implement the identification and authentication standard and control recommendations presented in our letters to management.

Responses of officials:

Department of Labour, Consumer Protection and Government Services:
Department of Labour, Consumer Protection and Government Services agrees with the recommendations in principle but notes that a blanket approach isn't always an appropriate approach. Technology constraints, information/system/application contents and system/application architecture are considerations that influence the necessary controls. The OAG recommendations will be considered as part of the controls and policies additions/changes within the Cyber Security Risk Reduction Program.

We will also collaborate with Shared Health in the future to align security practices when warranted.

Shared Health:
Shared Health acknowledges the findings and recommendations contained in the letter to management. Work is currently underway to address some of the recommendations and Shared Health will explore opportunities to address recommendation requirements that may require additional resources.

This audit's scope focused on the privileged access management practices and controls of the former Manitoba eHealth environment, which was one of several information technology (IT) programs supporting the provincial health care system. The initiation of the audit in 2019 coincided with the establishment of Shared Health Digital Health – the IT service provider for Shared Health in April 2019 through the amalgamation of multiple regional IT programs with separate practices, infrastructures, people, etc. While the recommendations are focused on a former regional IT program, responses to the recommendations must consider the standardization of a provincial IT program requiring additional funding and resources to implement and maintain.

Website Version

RECOMMENDATION 5

We recommend that the Department of Labour, Consumer Protection and Government Services, and Shared Health:

- Log all privileged user activities.
- Determine and regularly review risky activities.
- Where not already implemented, investigate methods to automate privilege user monitoring, including alerts of activity that should be reviewed.

Responses of officials:

Department of Labour, Consumer Protection and Government Services:
Department of Labour, Consumer Protection and Government Services agrees with the recommendations in principle but notes that a blanket approach isn't always an appropriate approach. Technology constraints, Information/system/application contents and system/application architecture are considerations that influence the necessary controls. The OAG recommendations will be considered as part of the controls and policies additions/changes within the ICT Risk and Security Management Program.

We will also collaborate with Shared Health in the future to align security practices when warranted.

Shared Health:
Shared Health agrees that monitoring of privileged access is an important cybersecurity control, and we will evaluate the extent that some of our new security control capabilities will address this recommendation.

This audit's scope focused on the privileged access management practices and controls of the former Manitoba eHealth environment, which was one of several information technology (IT) programs supporting the provincial health care system. The initiation of the audit in 2019 coincided with the establishment of Shared Health Digital Health – the IT service provider for Shared Health in April 2019 through the amalgamation of multiple regional IT programs with separate practices, infrastructures, people, etc. While the recommendations are focused on a former regional IT program, responses to the recommendations must consider the standardization of a provincial IT program requiring additional funding and resources to implement and maintain.

Website Version

Our Vision

Valued for positively influencing public sector performance through impactful audit work and reports.

Our Mission

To focus our attention on areas of strategic importance to the Legislative Assembly, and to provide Members of the Legislative Assembly with reliable and efficient audits.

Our mission includes easy-to-understand audit reports that include discussions of good practices within audited entities, and recommendations that, when implemented, will have a significant impact on the performance of government.

Our Values | Accountability | Integrity | Trust | Collaboration | Innovation | Growth

Auditor General
Tyson Shtykalo

Executive Director - IT and Innovation
Wade Bo-Maguire

Principal - IT Audit
Ganesh Sharma

Communications Manager
Frank Landry

Admin Support
Jomay Amora-Dueck
Tara MacKay

Graphic Design
Waterloo Design House

Website Version

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 Fax: 204-945-2169
contact@oag.mb.ca | www.oag.mb.ca

Facebook.com/AuditorGenMB
Twitter.com/AuditorGenMB
Linkedin.com/company/manitoba-auditor-general