# CITY OF VANCOUVER
# INTERNAL AUDIT REPORT
# VPL Cybersecurity Audit

**Distribution:**

| | |
|---|---|
| Audit Committee | Christina de Castell – Chief Librarian |
| Auditor General | Kay Cahill – Director, Information Technology & Collections |
| External Auditor | Balwinder Rai – Director, Human Resources |
| | Janet Horne – Senior Manager, Information Technology |

## EXECUTIVE SUMMARY

January 21, 2022

The objective of the audit was to assess the overall state of the Vancouver Public Library's (VPL) cybersecurity program. Effective cybersecurity programs help organizations develop cyber resiliency by embedding layers of security measures and practices.

Opportunities exist to further mature the cybersecurity program at VPL. While technical security measures for protecting systems are in place and continually being enhanced, additional layers of security involving operational IT processes are needed to enhance overall cybersecurity and cyber resiliency. Key cybersecurity functions, such as security patching and updating processes, identified by the NIST Cybersecurity Framework are in place.

During the course of this audit, management had taken a proactive approach in addressing the findings identified. The more significant findings and recommendations are:

### F.1 Standardize and strengthen password requirements

Password rules for key VPL systems have different requirements for length, complexity and expiry. A common, minimum password standard, that balances security and usability, should be set for key systems to prevent risk of system breaches.

### F.2 Ensure timely user access removal for terminated employees

Access management is a core part of cybersecurity to authenticate and authorize users. This includes timely deactivation of user accounts for terminated employees to prevent unauthorized access to systems. Periodic review of user accounts should be performed and time limits should be set on accounts that remain active for knowledge transfer purposes.

### F.3 Formalize a cybersecurity incident response plan

The goal of cybersecurity incident response planning is to minimize service disruption and to facilitate a coordinated response. While plans exist for certain scenarios to enable response and recovery, a comprehensive cybersecurity incident response plan should be developed. Going forward, the plan should be tested and exercised regularly.

### F.4 Implement a cybersecurity awareness training program

All employees who use VPL technologies have a role in ensuring cybersecurity. A comprehensive cybersecurity awareness training program should be developed for all technology users. Targeted training for staff in IT and training to non-IT staff in specialized or enhanced positions should continue to be provided.


**Carmen Fuellbrandt, CPA, CMA, CIA, CRMA**
**Manager, Internal Audit**

**Jenny Lau, CIA, CISA**
**Senior Internal Auditor**

## A. BACKGROUND

Cybersecurity

Cybersecurity is the protection of information and technology assets against cyber threats. Examples of cyber threats include ransomware, malware, phishing, and denial of service attacks. Effective cybersecurity programs help organizations develop cyber resiliency by embedding layers of security measures and practices. Cyber resiliency enables improved capacity to recover and continue operations despite cyber incidents.

Information Technology Services

The Vancouver Public Library (VPL) manages its IT services with a dedicated Information Technology Services (IT) team. In 2020, the IT team was responsible for supporting information systems that enabled over 6.4 million[1] digital and physical items being borrowed across 21 VPL locations.

## B. SCOPE

The objective of the audit was to provide reasonable independent assurance on the state of the Vancouver Public Library's cybersecurity program. The scope of this audit focused on the cybersecurity policies and procedures as managed by the VPL. Our work included:

- Interviews with members of the IT team;
- Review of policy and procedure documents such as the Security and Integrity, and Acceptable Use Guidelines policies;
- Observation of processes through screen demos and walk-throughs of tools and dashboards; and
- Sample review of terminated employee user accounts.

The audit was not designed to detect fraud. Accordingly, there should be no such reliance.

## C. CONCLUSION

Opportunities exist to further mature the cybersecurity program at the Vancouver Public Library. While technical security measures for protecting systems are in place and continually being enhanced, additional layers of security involving operational IT processes are needed to enhance overall cybersecurity and cyber resiliency.

The findings and recommendations identified have been discussed with management and their responses were incorporated in this report. We thank the IT team for their assistance with this audit.

[1] Obtained from 2020 VPL Annual Report

## D. RISK ANALYSIS

The potential risks considered if controls were not in place included:

- Disruption to systems that support critical VPL services;
- Financial losses from data loss, cyberattack schemes or recovery efforts;
- Reputational harm from loss of confidence to the integrity of VPL systems; and
- Regulatory penalties from breach of personal or financial information.

## E. POSITIVE OBSERVATIONS

The IT team is continually enhancing VPL's cybersecurity capabilities. Initiatives in 2021 included strengthening threat intelligence reporting, end-point device monitoring, and network security enhancements. Further enhancements are planned for 2022.

## F. AUDIT ISSUES, RECOMMENDATIONS AND MANAGEMENT RESPONSES

### F.1 Standardize and strengthen password requirements

Different password requirements across key systems

Password rules for key VPL systems have different requirements for length, complexity and expiry. A common, minimum password standard, that balances security and usability, should be set for key systems to prevent risk of system breaches. Leading practices for password management include:

- Password expiry;
- Minimum password length;
- Preventing use of commonly used or simple dictionary words (eg: password, test); and
- Multi-factor authentication methods.

**Recommendation:**

**F.1.1 The Director, Information Technology & Collections should review password requirements across key systems to ensure a common and minimum set of requirements are applied. Where possible, multi-factor authentication should be implemented. This should be completed by September 30, 2022.**

***Management Response:***

☑ Agree with the findings ☑ Agree with the recommendations

☐ Disagree with the findings ☐ Disagree with the recommendations

*Management Action Plan:*

Conduct an inventory of existing systems and password requirements. Establish minimum requirements and conduct a gap analysis to identify where changes are required. Implement minimum requirements for applicable systems, including migration of systems to SSO or other solutions where practical.

## F.2 Ensure timely user access removal for terminated employees

Manage user accounts for terminated employees

Access management is a core part of cybersecurity to identify, authenticate and authorize users. This includes timely deactivation of user accounts for terminated employees to prevent unauthorized access to systems. Terminated employees include those who are no longer VPL employees through retirement or staff departure.

However, user account deactivation to VPL systems is not timely for terminated employees. A periodic review of user accounts would also identify users who no longer require access. To perform this, timely information on employee terminations is required.

Set time limits on accounts used for knowledge transfer

In certain scenarios, user accounts may be requested to remain active for knowledge transfer purposes. While passwords are reset, a time limit should be implemented on how long user accounts remain accessible to reduce risk of inappropriate access.

**Recommendations:**

**F.2.1 The Director, Information Technology & Collections should update the user account management process to ensure timely deactivation of user accounts for terminated employees. This includes developing a process to periodically review user access to identify user accounts that are not required. This should be completed by June 30, 2022.**

***Management Response:***

☑ Agree with the findings ☑ Agree with the recommendations

☐ Disagree with the findings ☐ Disagree with the recommendations

*Management Action Plan:*

Update existing account deletion process to include steps developed in recommendation F2.2.2 to ensure timely notification from HR to IT when staff termination/departure requires an account to be deleted, including establishing parameters for account suspension (e.g. during leave). Acquire list of expired staff from HR and conduct a review to ensure that account deletion is fully up to date.

**F.2.2 The Director, Human Resources should develop a process to provide up-to-date information for terminated employees to enable a periodic review of user access by the IT team. This should be completed by June 30, 2022.**

***Management Response:***

☑ Agree with the findings ☑ Agree with the recommendations

☐ Disagree with the findings ☐ Disagree with the recommendations

*Management Action Plan:*

Communicate compliance requirements to HR staff. Develop process for proactive notification to IT when employees are terminated, depart the organization, or take leave longer than the time period identified in the response to F.2.1.

**F.2.3 The Director, Information Technology & Collections should develop and implement a policy for time limits on user accounts requested to remain active for knowledge transfer purposes. Access to such user accounts should be automatically disabled after the specified duration. This should be completed by June 30, 2022.**

***Management Response:***

☑ Agree with the findings ☑ Agree with the recommendations

☐ Disagree with the findings ☐ Disagree with the recommendations

*Management Action Plan:*

In consultation with the Directors' Group, establish role-based parameters for retaining accounts required for knowledge transfer and determine a time limit for retention of accounts that fall within these parameters, including a tracking process. Conduct a review to identify and delete existing accounts that fall outside this time period.

## F.3 Formalize a cybersecurity incident response plan

Response plans to minimize service disruption

Cybersecurity incident response plans contain the steps for responding to and handling incidents such as cyber threats or other unplanned events that impact systems. While plans exist for certain scenarios to enable response and recovery, a comprehensive cybersecurity incident response plan is not in place.

The goal of incident response planning is to minimize service disruption and to facilitate a coordinated response. An incident response plan should include:

- Processes and procedures to detect, respond, and recover from incidents;
- Roles and responsibilities of the response team;
- Communication plans to internal and external stakeholders;
- Schedule for regular testing and exercising of plans with IT and staff from other departments; and
- Integration with disaster recovery, business continuity plans, and the City's overall incident response plan.

**Recommendation:**

**F.3.1 The Director, Information Technology & Collections should formalize a cybersecurity incident response plan. Going forward, the plan should be tested and exercised regularly on a minimum annual basis. This should be completed by December 31, 2022.**

***Management Response:***

☑ Agree with the findings ☑ Agree with the recommendations

☐ Disagree with the findings ☐ Disagree with the recommendations

*Management Action Plan:*

Complete hiring of dedicated Emergency Planner role at VPL. In consultation with Emergency Planner, the City's Cybersecurity Team and external vendors where appropriate, develop a comprehensive technical response plan for the library. Note that there are dependencies related to the Emergency Planner position that may impact the completion deadline for this action plan.

## F.4 Implement a cybersecurity awareness program

Technology users play a role in cybersecurity

All employees who use VPL technologies have a role in ensuring cybersecurity. Improving the cybersecurity practices and digital hygiene of all users helps VPL reduce its risk of cybersecurity incidents. Different types of training such as PCI compliance and specific security training for directors are provided. However, a comprehensive cybersecurity awareness training program is currently not in place.

Implement a cybersecurity awareness training program

A comprehensive cybersecurity awareness training program includes mandatory awareness training for all employees who use technology. Awareness training should be provided on a regular and periodic basis, and include new employees who join VPL. Targeted training to staff in IT and training to non-IT staff in specialized or enhanced positions should continue to be provided.

**Recommendation:**

**F.4.1 The Director, Information Technology & Collections should implement a cybersecurity awareness training program for all VPL staff with system accounts. Awareness training should be mandatory and taken by employees on a regular and periodic basis going forward (e.g. annually). This should be completed by December 31, 2022.**

***Management Response:***

☑ Agree with the findings ☑ Agree with the recommendations

☐ Disagree with the findings ☐ Disagree with the recommendations

*Management Action Plan:*

Expand existing staff training through the development of additional internal tools and a vendor contract for training services, as appropriate. Identify cybersecurity awareness as part of VPL's core training suite to ensure regular attendance and tracking. Include an introduction to cybersecurity awareness in new staff orientation training.

## F.5 Limit use of USB storage keys

In response to the COVID-19 pandemic beginning March 2020, VPL implemented remote work for staff. At the time, VPL laptops were not available to all remote workers. To compensate for this, encrypted USB storage keys were issued to store information.

Risk of file storage on USB keys

Although storage keys are encrypted, there is a risk that encryption could be compromised depending on the type of USB device. In addition, restoring data in the event of data loss or corruption would not be possible as data stored on USB keys are not systematically backed-up.

Store files on network drives

Given the risks of USB storage keys, their use should be limited. Files containing key operational and sensitive information should be stored on network drives. Unless in exceptional circumstances when not used for storing sensitive information, USB keys may be employed. In

these cases, USB storage devices distributed should be inventoried and tracked to enable proper sanitization and secure disposal.

**Recommendations:**

**F.5.1 The Director, Information Technology & Collections should update VPL policies and implement measures to limit the use of USB storage keys. Sensitive data should be stored in network drives that are secured and backed-up on a regular basis. This should be completed by June 30, 2022.**

***Management Response:***

☑ Agree with the findings ☑ Agree with the recommendations

☐ Disagree with the findings ☐ Disagree with the recommendations

*Management Action Plan:*

Conduct investigation into use cases. Set up alternate, secure solutions for staff wherever feasible. Recall USB keys, replacing with alternate solution where required.

**F.5.2 The Director, Information Technology & Collections should record USB storage keys in the IT asset inventory listing in circumstances where storage keys are required by users. Tracking would enable proper sanitization and secure disposal upon return of the storage key. This should be completed by June 30, 2022.**

***Management Response:***

☑ Agree with the findings ☑ Agree with the recommendations

☐ Disagree with the findings ☐ Disagree with the recommendations

*Management Action Plan:*

IT maintain an inventory of all encrypted USB keys that are issued to staff.

## F.6 Review and enhance backup processes

Different backup procedures for backup media

Backup processes are essential to ensuring recovery from security incidents or other events that cause data loss or damage. To safeguard the integrity of backups, consistent security requirements should be applied. However, backup processes for two systems had different procedures involving backup media.

Review backup processes

In addition to security requirements, backup processes rely on other elements to ensure effectiveness. Backup processes should be reviewed periodically to consider the following:

- Backup frequencies and retention periods that align to both business needs and to incident response retention and recovery times;

- Up-to-date documentation on data restoration procedures; and
- Regular and periodic testing schedules of backup restoration procedures.

**Recommendation:**

**F.6.1 The Director, Information Technology & Collections should review backup processes for the following:**

- **Backup offsite storage locations and encryption requirements of backup media;**
- **Alignment with incident response or operational requirements for backup retention and recovery times; and**
- **Backup recovery testing schedules.**

**This should be completed by December 31, 2022.**

***Management Response:***

☑ Agree with the findings ☑ Agree with the recommendations

☐ Disagree with the findings ☐ Disagree with the recommendations

*Management Action Plan:*

Create documentation for existing backup cycles. Implement any changes identified as a result of the action plan for F.3.1. Continue work with the City's IT team to test backing up VPL data to the City's remote data centre.

## F.7 Continue to build resiliency into cybersecurity functions

Knowledgeable staff is important to an effective cybersecurity function. At the same time, the risk due to loss of knowledge from staff turnover could impact the resiliency of cybersecurity functions.

To minimize resource related risks, considerations for longer-term resiliency of key cybersecurity functions should be evaluated. Depending on the criticality of the process, different approaches could be implemented. Different approaches include:

- Cross-training to facilitate knowledge transfer;
- Documentation of key processes; and
- Retaining the support of external services firms to provide continuity of knowledge and subject matter expertise where needed.

**Recommendation:**

**F.7.1 The Director, Collections & Technology should continue to identify methods to develop resiliency into cybersecurity functions to minimize the risk of knowledge loss due to resource changes. This should be completed by December 31, 2022.**

***Management Response:***

☑ Agree with the findings ☑ Agree with the recommendations

☐ Disagree with the findings ☐ Disagree with the recommendations

*Management Action Plan:*

Proceed with planned staffing analysis and workforce planning exercise for IT, with the support of an external consultant. Identify backup positions for cybersecurity functions, and implement training and knowledge transfer for incumbents. Explore automation and/or outsourcing of some cybersecurity functions.

## F.8 Review physical security of server and server equipment

Part of cybersecurity is the protection of server and server equipment from physical and environmental threats. Potential threats could result in theft, tampering or damage to equipment affecting system confidentiality, availability and integrity.

While physical and environmental controls are in place to protect VPL server equipment, a review of these controls should be performed on a periodic basis. As it has been a number of years since the design and review of the physical server and equipment storage locations, a review should be performed to consider the following:

- Physical safeguards that protect equipment from unauthorized access or unintentional damage;
- Environmental controls to prevent fire or water damage; and
- Review of access rights to ensure only authorized staff have access on an as needed basis.

**Recommendation:**

**F.8.1 The Director, Information Technology & Collections should review physical and environmental controls in place for server equipment to identify updates where required. This should be completed by December 31, 2022.**

***Management Response:***

☑ Agree with the findings

☑ Agree with the recommendations

☐ Disagree with the findings

☐ Disagree with the recommendations

*Management Action Plan:*

Review controls and implement updates as feasible in the current space by December 31 2022. As part of the planned rebuild of the VPL data centre, engage with a consultant to review the current server room and ensure that best practices for modern server room design are implemented as part of the data centre redevelopment. The redevelopment is part of the 2023-2026 IT Capital Plan.