ATTACHMENT 2


# *Corporate Services – Regional Clerk – Handling of Private Information Audit Report*

## *July 2022*

## TABLE OF CONTENTS

**Section** **Page No.**

# 1.0 Management Summary

Audit Services has completed a Handling of Private Information audit.

The audit was conducted in accordance with the *Institute of Internal Auditors International Standards for the Professional Practice of Internal Auditing.*

The scope of the audit included a review of internal controls related to the handling of private information at York Region. Audit Services reviewed the Region's policies and procedures, interviewed relevant personnel and reviewed documents as part of this audit.

Overall, the results of our detailed testing indicate that the Region's processes for the handling of private information operate in a manner to ensure compliance with relevant policies and legislation.

Opportunities for internal control improvements are detailed below and have been discussed with appropriate management. These improvements relate to policy updates, staff education and training, documentation practices, and client services.

There were key processes identified during the audit where controls were strong and working as designed to ensure adherence to the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and the Personal Health Information Protection Act (PHIPA). This includes pro-active privacy assessments when acquiring new systems, well-documented policies for handling private information, responding to Freedom of Information Requests, complying with consent best practices, and responding to privacy breaches.

Should the reader have any questions or require a more detailed understanding of the risk assessment and sampling decisions made during this audit, please contact the Director, Audit Services.

Audit Services would like to thank Regional Clerks staff for their co-operation and assistance provided during the audit.

# 2.0 Introduction

As part of the Regional Council Approved Audit Plan, the Audit Services Branch performed a Handling of Private Information audit. The Audit Plan is developed by Audit Services using a risk assessment methodology that helps to define the different risks associated with the various processes at the Region. It is one tool that Audit Services uses in assessing where best to allocate audit resources.

York Region employees must handle personal information in accordance with the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and the Personal Health Information Protection Act (PHIPA).

The administration of the Region's Access and Privacy policies and procedures is the responsibility of the Office of the Regional Clerk. Audit Services reviewed the policies, procedures, toolkits, and training administered by the Access and Privacy Office to ensure compliance with required laws and legislation for the handling of personal information.

# 3.0 Objectives, Scope and Methodology

The main objectives of this engagement were to:

- Determine that the collection and handling of private information complied with legislation and policies.
- Verify that the internal controls over the security of private information collected were adequate and working as intended.

The scope of the audit included a review of internal controls related to the handling of private information at York Region. Audit Services reviewed the Region's policies and procedures, interviewed relevant personnel and reviewed documents as part of this audit.

The audit objectives were accomplished through:

1. Review of relevant policies, procedures, and legislation.
2. Interviews with appropriate personnel.
3. Review of other related documentation.

# 4.0 Detailed Observations and Recommendations

## 4.1 Corporate Privacy Policy

**The existing Corporate Privacy Policy outlining definitions, descriptions, roles and responsibilities was last updated on June 21, 2012.**

The Region follows the recommendations of the Information and Privacy Commissioner of Ontario (IPC) for best practices regarding consent. The Privacy Policy includes a description and obligations regarding consent; however, there is no distinction between the definitions of actual consent, implied consent, and voluntary consent. Ideally, information should only be collected under actual consent; however, there are limited circumstances in which implied consent may be required.

Failing to understand the various levels of consent may result in the overcollection, or unnecessary internal sharing of personal information, increasing the risk of liability to the Region. Depending on the type of information collected or shared, this may have larger consequences or create exposure in the event of a breach.

### Recommendation

**4.1.1** Due to the changing nature of the workforce over the past ten years and the transition to a hybrid work environment, the Corporate Privacy Policy should be reviewed and updated to ensure continued compliance with legislation.

The updated Privacy policy should provide distinct definitions of implied consent, actual consent and voluntary consent to ensure staff are aware and fulfill their obligations related to consent.

Recommendation Owner: Regional Clerk
Target Completion Date: Complete.

### Management Response

Complete. The Corporate Privacy Policy was updated and approved by the Chief Administrative Officer in September 2022. The updated policy consolidates three separate policies relating to personal and personal health information and will make it easier for staff to understand their privacy obligations. It also incorporates an updated definition of consent that covers implied and express consent.

## 4.2 Responsible Use of Technology Policy

**At the time of this audit, the Responsible Use of Technology Policy was last updated on November 14, 2016.**

Regarding the use of personal devices, the policy states:

> "Authorized Users must use the website 'york.ca/eservices' to access the Enterprise Network and Technology Systems and Resources through Personal Devices. Configuring Personal Devices for access through any other method, including but not limited to connection to Wi-Fi (e.g., 'Staff' network), cloud services and email accounts (e.g., 'Regional Exchange account), is not permitted."

Since the time of this policy update, employees have moved to a virtual environment, and a future "York @ Work" hybrid environment, due to the onset of the COVID-19 Pandemic and may be unclear of their expectations and responsibilities regarding the use of personal devices to perform their job responsibilities remotely.

### Recommendation

**4.2.1** The policy should be reviewed and updated as appropriate to clarify staff expectations and responsibilities regarding the use of personal devices to perform their work.

Recommendation Owner: Director, IT Services
Target Completion Date: Complete

### Management Response

Due to the changing methods and circumstances where personal technology may be used, the updated Acceptable Use and Management of Technology policy permits use of personal technology "only through designated methods approved by the IT Services Branch". These designated methods are listed in the 'Supporting Procedures' document referenced at the end of the policy, with hyperlinks to detailed instructions on MyPortal. This allows for individual methods to be updated as required.

## 4.3 Personal Information Bank

**The Personal Information Bank does not identify the servers in which the data is stored.**

The Personal Information Bank is maintained by the Region as a repository to compile and track the location of all existing personal information held by the Region. Internal practice is to update the bank every three years. As part of our review of the Personal Information Bank, we noted that it does not identify the servers in which the data is stored.

As the Region moves towards a remote environment, there will be an increase in the amount of personal information stored digitally. Maintaining an accurate location of personal information is critical to information protection, as well as ensuring an appropriate and timely response in the event of a cyber breach.

## Recommendation

**4.3.1** Management should also consider including server information when updating the Personal Information Bank to easily identify the location and access rights to specific personal information. This would create a more complete repository of information, as well as assist the Region in a quick response in the event of a cyber breach.

Recommendation Owner: Regional Clerk
Target Completion Date: Q2 2023

## Management Response

Agreed. The Region maintains a record of its Personal Information Banks (PIBs) as required under the *Municipal Freedom of Information and Protection of Privacy Act.* The PIBs are updated every three years in coordination with departmental staff. The next update is anticipated to be completed by the end of Q2 2023 and, as part of the process, staff will collect server addresses for electronic repositories of personal and personal health information.

### 4.4 Privacy Review During the CRIT Process

**Privacy review during the Cyber Risk Information Tool (CRIT) process does not include a formal list of key inquiries for each acquisition.**

The CRIT process at York Region is a comprehensive review to address and mitigate cyber risks prior to acquisition, including input from the Regional Clerk regarding privacy concerns.

Our review determined that input from the Regional Clerk is based on experience of the person attending the meeting and does not include a formal list of key inquiries to be documented. This increases the risk that critical areas may not be addressed and documented during the assessment depending upon the experience of the personnel in attendance.

Advice provided during the CRIT process is subject to Freedom of Information (FOI) requests. Applying a consistent and comprehensive approach to document privacy considerations discussed during the CRIT process increases the level of transparency and support for the due diligence performed by the Region.

## Recommendation

**4.4.1** Management should implement a list of formal inquiries that must be documented for each acquisition through the CRIT process to provide a consistent standard to the privacy assessment for all acquisitions.

Recommendation Owner: Regional Clerk
Target Completion Date: Q3 2023

### Management Response

Agreed. Although, staff do address privacy risks through the CRIT process, a consistent approach is useful. Staff will develop a standard list of inquiries based on the seven principles of Privacy by Design. Privacy by Design, a standard developed by the Information and Privacy Commissioner, was incorporated into the updated Corporate Privacy Policy.

## 4.5 Freedom of Information Request (FOI) Form

**When attempting to access the FOI Request form on the external York.ca website, we were notified that "This site can not be reached. Beta.york.ca's server IP address could not be found."**

The York.ca website states "A formal request must be submitted in writing either by letter or on the Access Request Form, to the Regional Clerk's Office and be accompanied by a prescribed fee of $5 (cheque or money order made payable to York Region); however, we were unable to access the form using this process as part of our review

### Recommendation

**4.5.1** Management should update the external website to ensure that the FOI Request Form is available for download to the public.

Recommendation Owner: Regional Clerk
Target Completion Date: Complete

**4.5.2** Management should consider expanding the use of online payment capabilities for FOI requests to reduce the opportunities for fraud and / or theft.

Recommendation Owner: Regional Clerk
Target Completion Date: Complete

### Management Response

Complete. The link to the Access Request Form was broken following the Region's migration to a new web platform and was rectified shortly after being flagged. Online FOI payments launched on October 18, 2022

## 4.6 Employee Privacy Awareness and Training

**The Mandatory Employee Training Course "Corporate Privacy Policy" (Course Code: IM0040) is a one-time training course for new employees, with no requirement for refresher courses to provide updated information and reinforcement of acceptable practices**

Through discussion with staff, we noted that there is an absence of awareness around internal sharing of information among employees. Employees may share information internally for various business purposes, unaware they are creating a duplicate copy of personal information that is not captured in the personal information bank or may be exposed through a less secure environment.

Our review also noted that the Region has legacy systems that were put in place prior to the implementation of the CRIT process which address appropriate access rights prior to system implementation. Managers may not be trained to periodically re-evaluate access rights on more vulnerable systems implemented prior to the CRIT process.

## Recommendation

**4.6.1** Due to the high-risk nature of handling of private information, Management should consider requiring a refresher course for employees on an annual basis reflecting the latest roles, responsibilities and best practices outlined in the Policy.

Recommendation Owner: Regional Clerk
Target Completion Date: Q4 2023

**4.6.2** As noted in Observation 4.1, the Corporate Privacy Policy requires update; accordingly, existing employees may not receive training on the new policy under the current training regimen.

Recommendation Owner: Regional Clerk
Target Completion Date: Q4 2023

**4.6.3** Management should consider implementing increased awareness materials into the training program regarding the risks and implications of the internal sharing of personal and sensitive information. Training materials should encourage employees to remove sensitive information to meet the minimum requirements when sharing information internally.

Recommendation Owner: Regional Clerk
Target Completion Date: Q4 2023

**4.6.4** To address the concerns of legacy access provided to systems implemented before the CRIT process, training materials for management should include a recommendation that Managers periodically review access rights to the systems in which they are responsible for.

Recommendation Owner: Regional Clerk
Target Completion Date: Q4 2023

## Management Response

The Region's required privacy training module will be updated to reflect the new Corporate Privacy Policy. While the module still reflects valid key privacy messages, it could benefit from specific messaging related to the new hybrid work environment. This is expected to be completed by the end of 2023.

Annual refresher training is being developed in partnership with the Privacy, IT Security, and Information Management functions to ensure the training is effective and relevant. Staff will consider including reminders to managers to periodically review access to systems containing personal information.

Additional materials have also been developed to support the protection of personal information such as a Privacy Breach Placemat to guide staff in the event of a breach. Access and Privacy staff also participate in the Data Sharing Working Group, which is developing processes and guidelines for the appropriate internal handling and sharing of personal information.

## 4.7 Privacy Information Audits

**The Region does not pro-actively audit the Region's internal processes to ensure compliance with policy and legislation, nor performs privacy compliance audits on third parties.**

The Cyber Risk Information Tool (CRIT) and Cyber Risk Exposure Tool (CRET) processes implemented by the Region are preventative controls to protect the personal information collected and maintained both internally and by third parties. However, there is no subsequent follow-up to ensure adherence with Region policies and legislative requirements, including the appropriate disposal of personal information by third parties.

Without pro-active audits, there is a risk that third-party vendors are not disposing of personal information in accordance with the Region's retention policies and in an appropriate manner to reduce the risks associated with handling personal information that is no longer required.

### Recommendation

**4.7.1** Management should consider pro-actively auditing our internal processes and those of third-party vendors handling the Region's private information.

Recommendation Owner: Regional Clerk
Target Completion Date: Complete

### Management Response

The Region uses standard terms when negotiating contracts with third parties that set out clear requirements around their handling of personal information on the Region's behalf. This includes confidentiality provisions, notification requirements in the event of a breach and an undertaking to delete all personal information at the end their engagement. Similarly, through the CRIT process, the Region's business units are provided with guidelines and requirements for new or substantially modified systems containing personal information.

Proactively auditing the numerous internal and third-party systems is a significant undertaking. The Region has submitted a business case for an additional Access and Privacy Officer in the 2023 Budget and, if supported, this may provide some additional capacity for such work. Management will consider proactive audits as part of a broader risk-based work planning exercise.

## 4.8 Client Feedback

**The Region does not pro-actively solicit client feedback regarding the level of understanding of consent when providing personal information to the Region.**

We verified that the Region includes Collection Notices in all forms used to collect personal information; however, the Region does not receive feedback from client users on their level of understanding.

Soliciting client feedback could assist in pro-actively addressing concerns and increase trust, confidence, and transparency with the public.

### Recommendation

**4.8.1** Management should consider periodically obtaining feedback from clients to ensure an adequate level of understanding of consent is being provided regarding the personal information the Region is collecting.

Recommendation Owner: Regional Clerk
Target Completion Date: Complete

### Management Response

The Region strives to ensure that its Collection Notices are written in plain language so clients can make informed decisions around consent. Each Collection Notice also identifies a program expert who can be contacted if clients have questions about what personal information is being collected and how it will be used.

Management will work with client service groups to consider the feasibility of gathering consent feedback as part of broader service satisfaction surveys.

End of observations.

Management has received a copy of this report and included a response as indicated in their signatures below.

**Original signed**

**Dino Basso**
**Commissioner, Corporate Services**

**Original signed**

**Christopher Raynor**
**Regional Clerk**

**Original signed**

**Richard Leest**
**Director, IT Services**

**Original signed**

**Michelle Morris**
**Director Audit Services**

eDocs# 14428345