



CITY OF HAMILTON
CORPORATE SERVICES DEPARTMENT
Information Technology Division

TO:	Chair and Members Audit, Finance and Administration Committee
COMMITTEE DATE:	May 20, 2021
SUBJECT/REPORT NO:	Information Security Policy Report (FCS21039) (City Wide)
WARD(S) AFFECTED:	City Wide
PREPARED BY:	Emilia Jasnic (905) 546-2424 Ext. 5704
SUBMITTED BY:	Maria McChesney Director, Information Technology Corporate Services
SIGNATURE:	

RECOMMENDATION

That the Information Security Policy, attached as Appendix “A” to Report # FCS21039 be approved.

EXECUTIVE SUMMARY

The City is responsible to protect confidentiality, integrity and availability of information systems and data in order to provision and manage city services. Staff are obligated to protect personal information under the Municipal Freedom of Information & Protection of Privacy Act (MFIPPA) and the Personal Health Information Protection Act (PHIPA). The Information Security Policy, attached as Appendix A, establishes accountability, roles and responsibilities and direction to support staff through legislated requirements and guidelines. In addition, the Information Security Policy is required to ensure compliance to industry standards such as the Payment Card Industry Data Security Standard (PCI DSS).

The City is committed to protecting the security of information systems and data and the Information Security Policy, attached as Appendix A, establishes accountability, roles and responsibilities, and provides direction for information security management at the City of Hamilton modelled after *ISO/IEC 27001:2013 - Information Technology — Security Techniques — Information Security Management Systems — Requirements* (the “ISO Standard”).

OUR Vision: To be the best place to raise a child and age successfully.

OUR Mission: To provide high quality cost conscious public services that contribute to a healthy, safe and prosperous community, in a sustainable manner.

OUR Culture: Collective Ownership, Steadfast Integrity, Courageous Change, Sensational Service, Engaged Empowered Employees.

SUBJECT: Information Security Policy Report (FCS21039) (City Wide)
- Page 2 of 3

ISO/IEC 27000 Series Standards are dedicated to the Information Security. The ISO Standard is an Information Security Program Framework that provides requirements for establishing, implementing, maintaining and continually improving Information Security Management Systems. The Framework defines areas of focus in building an Information Security Program. This consists of policies, procedures, processes, and activities that organizations should implement in order to have a robust Information Security Program.

ISO/IEC 27002 Information Technology – Security techniques – Code of practice for information security controls provides guidance for implementing ISO/IEC 27001. The Information Technology (IT) Division of the Corporate Services Department is committed to implementing the City's Information Security Program by following the guidance from this Program Framework.

Once the Information Security Policy is approved, operational support documentation and processes will be developed, and training will be provided to all impacted city staff and elected officials.

FINANCIAL – STAFFING – LEGAL IMPLICATIONS

Financial: N/A

Staffing: The Information Technology (IT) Division of the Corporate Services Department will work on aligning Standard Operating Procedures to the Information Security Policy. The IT Security Team will develop role-based information security awareness training for all city staff and elected officials.

Legal: N/A

HISTORICAL BACKGROUND

In 2020, the Information Technology (IT) Division of the Corporate Services Department in partnership with the Clerk's Office, Legal, Risk Management, Procurement Divisions in the Corporate Services Department, the Privacy Officer from the Public Health Division of Healthy and Safe Communities Department and Corporate Communications of the City Manager's Office, formed the Information Privacy and Security Committee. The Information Privacy and Security Committee and its membership were endorsed by Senior Leadership Team (SLT) in October 2020.

The IT Security Team has reviewed and updated existing Information Security Policies and created a new comprehensive suite of Policies that together make up the Information Security Policy. The Information Security Policy will be the overarching Policy.

POLICY IMPLICATIONS AND LEGISLATED REQUIREMENTS

The Information Technology (IT) Division of the Corporate Services Department will work on aligning Standard Operating Procedures with the PHIPA. Policy – Section 12:

Security - 12 (1) A Health Information Custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the Custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. 2004, c. 3, Sched. A, s. 12 (1).

The City of Hamilton holds a Health Information Custodian status under PHIPA legislations for the purposes of Hamilton Paramedic Services and Long-Term Care homes and the Medical Officer of Health holds this status with respect to public health.

Payment Card Industry Data Security Standard (PCI DSS):
Requirement 12: Maintain a Policy that addresses information security for all personnel.

RELEVANT CONSULTATION

This Policy has been approved by the Information Privacy and Security Committee and Senior Leadership Team in March and April 2021.

ALIGNMENT TO THE 2016 – 2025 STRATEGIC PLAN

Built Environment and Infrastructure

Hamilton is supported by state-of-the-art infrastructure, transportation options, buildings and public spaces that create a dynamic City.

Our People and Performance

Hamiltonians have a high level of trust and confidence in their City government.

APPENDICES AND SCHEDULES ATTACHED

Appendix “A” to Report FCS21039 - Information Security Policy

EJ/sn