Hamilton

Information Security Policy

POLICY STATEMENT	The main goals of information security are to preserve: 1. *Confidentiality:* ensuring that information is accessible only to those who are authorized to have access. 2. *Integrity:* safeguarding the accuracy and completeness of information and processing methods. 3. *Availability:* ensuring that authorized users have access to information when needed. This document follows the guidelines given in *ISO/IEC 27002*, the international standard on *Security techniques, Code of practice for information security controls* and it provides Information Technology (IT) security policy direction to all Authorized Users through the following: 1. IT security solutions that are based on risk management principles for selecting, verifying, maintaining, monitoring and adjusting safeguards from the inception of any program, application, system or digital service; 2. A Management Framework that will ensure accountability, responsibility and support for the protection of digital information, information systems, process control systems, information services and process control assets; 3. Processes that will permit the management of IT Security to support maintenance of system security profiles that include the confidentiality, integrity and availability of IT and Process Control Systems for all users and partners; 4. Development, implementation and maintenance of appropriate controls, guidelines and procedures to address the confidentiality, integrity and availability of digital information, process control and information systems and information services; 5. Direction and guidance to system developers, analysts, external IT contractors and verification authorities for their tasks so that stipulated IT security requirements are met on an on-going basis; 6. Development of programs and resources to support the implementation and maintenance of a balanced security program.
PURPOSE	The purpose of this Policy is to provide management direction and support for information security at the City of Hamilton in accordance with business requirements and relevant laws and regulations. To define the Policies and Procedures for any individual or

	organization that connects to the City of Hamilton's information technology and process control systems or services. Establishing the roles and responsibilities for ensuring the principles in this Policy are implemented and maintained.
SCOPE	This Policy applies to all City of Hamilton employees, staff of elected officials, and all other organizations and individuals who are authorized by the City to use IT Resources.
DEFINITIONS **Authorized Users**	The following terms referenced in this Policy are defined as: **Authorized Users:** includes all persons who are authorized by City of Hamilton to access and use the City's Process Control and IT Resources for legitimate business purposes. **IT Resources** includes all: • Computer software, hardware and equipment owned or issued by the City, including desktops, laptops, tablets, notebooks, servers, process control devices or smart phones (such as iPhone or Android devices); • Telephones (including IP, cellular or traditional phones), and other audio/voice devices and networks, including voicemail; • Video conferencing systems and equipment; • Scanners, printers and fax machines and peripheral devices and removable media associated with the computer (such as USB drives, CDs, DVDs, etc.); • Transmission methods and services employed by the City's computer hardware and equipment, including wired, wireless and cellular networks, whether accessed from within the City's premises or elsewhere; • Internet and e-mail systems; • Data, information and other work products such as computer programs, databases, spreadsheets, etc., created and/or maintained in using these IT resources; and • City related data and information that is accessed, stored, created, processed, transmitted or filed in an electronic device. **Availability:** Information is available to authorized persons as agreed. **Integrity:** Ensuring information has not been altered accidentally or deliberately, and it is accurate and complete. **Information Security:** Maintaining confidentiality, integrity and availability of information, process control facilities and data processing facilities.

	ISO/IEC 27000 Series Standards: Defined Standards by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC) to manage information security. **Malware:** A generic term for several different types of malicious code. **Threat:** Potential cause of an unwanted incident, which may result in harm to the business. **Vulnerability:** The weakness of an asset that can be exploited by one or more threats. **Risk:** A combination of the likelihood of an event and its consequence. **Storage media:** Devices or other media that store data, application and user information. **Non-public Information:** means information that is exempt or is potentially exempt from disclosure under the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56 or the *Personal Health Information Protection Act, 2004, S.O. 2004*, c. 3, Schedule A, or that is otherwise deemed confidential. (Refer to Policy IT-04 “Data Classification” for further information about the classification and use of City data.) **Confidential Information** includes, but is not limited to, Cardholder Data as defined in the *Payment Card Industry Data Security Standard*, Personal Health Information as defined in the *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3, Sched. A or Personal Information as defined in the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56.
TERMS & CONDITIONS	The Director of Information Technology Division is responsible for maintaining IT Security Policies, Standards and Practices that will put this Information Technology Security Policy into practice and provide direction for those charged with security program implementation and management. In compliance with ISO/IEC 27002, the City’s information security procedures will include, but not be limited to the following security standards and objectives: 1. **Computer and Technology Acceptable Use Policy** This Policy defines the requirements regarding the use of information and the City’s IT Resources. These requirements are intended to help protect the

confidentiality, integrity and availability of the City's systems and data.

2. **Mobile Devices Policy**
This Policy defines the guidelines to ensure the security of mobile devices.

3. **Remote Work Security Policy**
This Policy defines the requirements to ensure the security teleworking.

4. **Human Resources Security Policy**
This Policy defines the requirements to ensure that employees and contingent workers understand their responsibilities and are suitable for the roles for which they are hired and to protect the City of Hamilton information as part of the process of changing or terminating employment.

5. **Information Asset Management Policy**
This Policy provides the guidelines to ensure proper record maintenance and asset tagging of all IT equipment; to classify and define protection requirements for the City's data; to ensure that information receives an appropriate level of protection in accordance with its importance to the City of Hamilton.

6. **Access Management Policy**
This Policy defines a standard to limit access to information and information processing facilities according to the business and security requirements, to ensure authorized user access, to prevent unauthorized access to systems and services and to make Authorized Users accountable to safeguard their authentication information.

7. **Cryptography Policy**
This Policy defines the information security controls that are required to implement and manage cryptographic solutions according to the business and security requirements.

8. **Physical and Environmental Security Policy**
This Policy defines the requirements for the physical security of the City of Hamilton's information technology systems and to ensure that physical security of all City of Hamilton's information processing facilities is built and maintained.

9. **Operations Security Policy**
This Policy defines the requirements for implementing

	correct and secure operations of information processing facilities, protection from malware, protection against the loss of data, appropriate recording of events that generate evidence and vulnerability management. 10. **Network and Communications Security Policy** This policy defines the requirements to ensure the protection of information in networks and to maintain the security of information transferred within the City of Hamilton and with any external entities. 11. **System Acquisition, Development and Maintenance Policy** The procedures in this section outline the security requirements for the procurement of information and process control systems, software development and maintenance, and use of test data. 12. **Technology Service Provider Policy** This Policy defines the guidelines to ensure that access to City of Hamilton facilities, systems and information assets by Technology Service Providers is appropriately controlled so that confidentiality, integrity, availability and accountability of information and assets remain intact. 13. **Information Security Incident Management Policy** To implement an information security incident management process to identify and resolve information security incidents related to the City of Hamilton quickly and effectively, while minimizing their impact and reducing the risk of similar information security incidents from occurring. 14. **Information Security Aspects of Business Continuity Management Policy** This Policy defines the requirements and recommendations to embed the information security continuity into business continuity plans to ensure availability of all information systems and assets supporting the City of Hamilton business functions. 15. **Security Compliance Policy** This section identifies and documents information security obligations including business records, intellectual property, and privacy. This security procedure describes the legal and contractual commitments, security reviews and audits requirements.
RESPONSIBILITIES (if applicable)	Within the City of Hamilton, Security is everyone’s responsibility. The City of Hamilton, as a contracting authority, is legally responsible for ensuring contractors and

	partners are acting in accordance with these policies while executing work in the City of Hamilton’s name. This policy will be reviewed on a regular basis and updated as needed by the IT Security Manager. Reviews will consider: • Its effectiveness, as demonstrated by the nature, number and impact of security incidents. • The cost and impact of controls on business efficiency. • The effects of changes in risk; technology; available controls; regulatory and legal requirements; and industry best practice. The City Manager and the Senior Management Team will be required to approve significant changes to the policy. The Director of Information Technology Division is responsible for establishing, monitoring and ensuring compliance with Information Technology Security Policies and Standards. The Information Technology Division has the authority to implement the Information Technology Security Policy, oversees threat and vulnerability assessments and advises on safeguards and other elements of risk management throughout the life cycle of process control and information systems. The Clerk’s Division and Privacy Officers ensure that input is provided for privacy assessments, as part of risk management. All City of Hamilton Authorized Users are required to complete the training provided by the IT Division Security Awareness Program and notify management of actual or suspected policy breaches. These notifications should be sent to the Service Desk so that appropriate IT Security resources can be engaged. The Information Technology Division will designate auditors to undertake broad-based IT security audits on a periodic basis to ensure an objective third party view on the success of the security program. Manager, IT Security is responsible for ensuring the conduct of IT security reviews and reporting to the Information Technology Leadership Team about the findings of the IT security program.
COMPLIANCE	All requirements specific in Information Security Policies are mandatory. Any deviation from a mandatory requirement in Information Security Policy must be approved by the IT Security Team. All process control and information security exemption requests

	must be assessed by the IT Security Team and then reviewed by the Information Technology Leadership team for approval. All process control and information security exemptions requests and approvals must be logged by the IT Security Team. Information security exemptions may be requested and granted for any length of time. However, all approved exemptions must be reviewed by the IT Security Team at a minimum, every two years, to ensure that the level of risk has not increased or that new risks have not appeared.
RELATED	The following related documents are referenced in this Policy: 1. *ISO/IEC - 27002:2013 Security techniques, Code of practice for information security controls* 2. *Computer and Technology Acceptable Use Policy* 3. *Mobile Devices Security Policy* 4. *Remote Work Security Policy* 5. *Human Resources Security Policy* 6. *Information Asset Management Policy* 7. *Access Management Policy* 8. *Cryptography Policy* 9. *Physical and Environmental Security Policy* 10. *Operations Security Policy* 11. *Network and Communications Security Policy* 12. *System Acquisition, Development and Maintenance Policy* 13. *Technology Service Provider Policy* 14. *Information Security Incident Management Policy* 15. *Information Security Aspects of Business Continuity Management Policy* 16. *Security Compliance Policy*
HISTORY	The following stakeholders were consulted in the creation or revisions made to this Policy: Information Technology Leadership Team Information Privacy and Security Committee This policy is dated <<Insert Date here, if available>>