

Electronic Data Security Policy

1.0 Policy Statement

City of Mount Pearl employees are expected to support and uphold the security of sensitive electronic data. This policy applies to all sensitive electronic data in the custody and/or control of the City of Mount Pearl and its employees and volunteers. This policy conforms with the *Access to Information and Protection Act, 2015* (ATTIPA) and with City's privacy regulations.

2.0 Purpose

To establish a policy that outlines the responsibilities of all City of Mount Pearl employees in supporting and upholding the security of the City's sensitive electronic data.

3.0 Definitions

Computing resource: All devices (including, but not limited to, personal computers, laptops, USB keys, and Smart phones) that are used to access, process, or store City's data.

Electronic Data: Includes all data that belongs to or is used by the City of Mount Pearl that is processed, stored, transmitted and/or copied to or from computing resources.

Sensitive Electronic Data: Electronic data that has been designated as private or confidential by law or by the City of Mount Pearl. Sensitive Electronic Data includes, but is not limited to, data protected by the *Protection of Privacy Policy* and the *Access to Information Policy*. To the extent there is any uncertainty as to whether any data constitutes Sensitive Electronic Data, the data in question shall be treated as such until a determination is made by the City.

4.0 Procedures

All employees have responsibility to protect Sensitive Electronic Data from unauthorized disclosure, modification and destruction. All employee users shall adhere to this policy and related Information Technology policies and procedures.

Standards for approved security software and configurations shall be set by the Manager of Information Technology, and periodically revised in response to best practices technologies.

Emerging security threats and incidents may require immediate response. When such circumstances arise, the Manager of Information Technology has the authority to revoke an existing standard and/or introduce a new one.

Access

Sensitive data access shall be limited in accordance with the principle of the least privilege. Authorized employees needing access to a subset of data shall not be granted access to all records, for instance, nor shall they be provided write access if creating or modifying records is beyond the scope of their authorized duties. Application of this principle can limit damage resulting from user error and unauthorized access.

Change of Authorized User Status

When an authorized employee user who has been granted access changes responsibilities or leaves employment, their access rights shall be re-evaluated by the Information Technology Division any access to data outside of the scope of the new responsibility or status shall be revoked as soon as possible but not later than five working days.

Operating Systems

All computing resources purchased with the City's funds shall run a currently supported operating system for which security patches are actively released and applied.

Antivirus

All desktops and laptops purchased by the City shall run approved anti-virus software.


Backups

Data that is critical to the operation of the City of Mount Pearl should be backed up to prevent accidental loss. Backup copies of Sensitive Electronic Data shall be protected to the same standards set out in this policy.

Use of Non – City of Mount Pearl – Owned Equipment

Sensitive Electronic Data must not be stored on equipment not owned by the City, unless authorized by the Director of Corporate Services. If such data must be stored on equipment not owned by the City, the authorized employee user is responsible for ensuring the equipment meets the same security requirements in this policy.

5.0 Approvals



Steve Kent, Chief Administrative Officer
August 30, 2018

Date