Policy Number: IT- 6012

Department: Information Technology

Division: Corporate Services

Adoption Date: April 13, 2026

Authority: CR 210/2007

Scheduled for Review: Oct 1, 2030

Information & Digital Protection Policy

1. Policy Statement:

1.1 Information, in any way it is produced, kept, transported, or used, is a valuable asset of the Corporation of the City of Windsor ("Corporation") and must be protected.

1.2 Information assets include all categories of electronic information, records, files, databases, applications, software, equipment and technology infrastructure

1.3 The Senior Manager, Cyber Security & Risk shall ensure rules governing information security are developed, implemented, and enforced.

1.4 The Chief Administrative Officer provides executive oversight to ensure alignment with corporate objectives and compliance obligations.

The purpose of this Information & Digital Protection Policy ("Policy") is to:

1.5 Establish clear responsibility and authority for protecting information assets,

1.6 Protect the confidentiality, integrity, and availability of information assets,

1.7 Ensure operational continuity,

1.8 Minimize damage to information assets and technology systems from security incidents,

1.9 Effectively manage the risk of security exposure within technology systems,

1.10 Alert users in their responsibility for protecting information assets,

1.11 Ensure that this Policy, along with the Corporation's Acceptable Use Policy and related security standards, combine to create a comprehensive framework for protecting information assets and technology systems.

2. Scope:

This Policy applies to:

2.1 All employees of the Corporation, elected officials, contractors, consultants, volunteers, vendors, and all other individuals or third parties who access, either

from internal or external locations, any corporate-owned information assets, network facilities, and technology systems, or any outsourced data or applications managed on behalf of the Corporation (collectively referred to as "users").

2.2 Technology systems for which the Corporation has administrative responsibility, including on-premises infrastructure, cloud-hosted services, and outsourced applications. This encompasses all electronic information created, processed, or used in support of the Corporation's activities and services, regardless of the form or format. Controls over access to information are provided by a combination of adequate security applied to the physical infrastructure, computer and network systems, remote access capabilities, cloud environments, and applications.

3. Definitions:

N/A

4. Responsibilities:

The following is a description of the organizational structure charged with the responsibility for administering this Policy:

4.1 Chief Administrative Officer (CAO)

The CAO provides executive oversight for information security and ensures that this Policy aligns with corporate objectives and compliance obligations.

4.2 Senior Manager, Cyber Security & Risk

The Senior Manager, Cyber Security & Risk is accountable for developing, implementing, and enforcing the Policy, standards, and practices of the City's information security program. This role leads the City's information security program, ensures appropriate monitoring and reporting, and coordinates responses to security incidents. The Senior Manager, Cyber Security & Risk is responsible for ensuring the Policy is reviewed at least once every term of Council.

4.3 IT Cyber Security & Risk Division

The Cyber Security & Risk Division, under the Senior Manager, is responsible for ensuring the Corporation's overall cybersecurity resilience and defense. This includes:

- Monitoring and managing cyber threats, vulnerabilities, and emerging risks,
- Leading and coordinating incident response and recovery efforts,
- Conducting risk assessments, audits, and compliance reviews in partnership with Information Owners,
- Maintaining security records and reporting on the City's risk posture to senior leadership,

- Providing user training and awareness programs related to cybersecurity,
- Developing, implementing, and maintaining technical and procedural security controls,
- Advising on security requirements for new technology projects, cloud services, and vendor contracts,
- Ensuring alignment with applicable laws, regulations, and corporate policies,
- Driving continuous improvement in cybersecurity practices to strengthen organizational resilience.
- Responsible for labeling, handling, storage, and destruction procedures.

4.4 Information Owner

The Information Owner is the manager of the service area, department, or division that creates, manages, or updates the information and whose business function the information asset supports. Information Owners are responsible for:

- Approving and managing user access rights to the information asset,
- Classifying information according to corporate standards,
- Ensuring contingency and recovery plans are in place,
- Information Asset lifecycle management, which includes creating, storage, archiving and secure disposal.
- Working in partnership with the Cyber Security & Risk Division to safeguard information assets.

4.5 Information Technology (IT) Department

The Information Technology Department supports the Cyber Security & Risk Division by maintaining secure technology infrastructure, enforcing access controls, and assisting Information Owners with protecting and recovering information assets.

4.6 Users

- All employees, elected officials, contractors, consultants, volunteers, and third-party service providers with access to Corporation's systems are responsible for complying with this Policy and safeguarding information assets.
- Responsible for reporting suspicious activity.

5. Policy:

N/A

6. Additional Legislative Authority:

6.1 Referenced or Governing Policies, Regulations, and Legislation

6.1.1. The Corporation of the City of Windsor - Acceptable Use Policy

6.1.2. *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), R.S.O. 1990, c. M.56, as amended.

6.1.3. Personal Health Information Protection Act (PHIPA), 2004, S.O. 2004, c. 3, Sch. A, as amended.

6.1.4. *Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c. 5, as amended.

6.1.5. *Criminal Code*, R.S.C. 1985, c. C-46, as amended.

7. Records and Attachments:

N/A