Elections Ontario

Cyber Security Policy

Office of the Chief Electoral Officer
Elections Ontario
July 2026

Document History

Revision Number	Revision Date	Effective Date	Description of Changes	Approved By
1.0		July 27, 2026	Original	Greg Essensa, CEO

TABLE OF CONTENTS

Section 1: Introduction

Elections Ontario (EO) is committed to protecting its digital information systems and infrastructure from unauthorized access, breaches, and cyberattacks. EO prioritizes digital security to safeguard the privacy and security of personal information, ensure the continued delivery of election services, and maintain the public trust of Ontarians.

EO maintains the integrity of its information technology (IT) environment by establishing security requirements that minimize vulnerability and strengthen resilience to constantly evolving cyber threats, including but not limited to malware, phishing, ransomware, nation-state attacks, and supply chain exploits.

The purpose of this Cyber Security policy is to prevent disruption and harm to EO's systems, networks and infrastructure, including digital products and information. This policy defines EO's mandatory requirements, approvals, and roles and responsibilities for managing cyber security risks.

Section 2: Principles

Elections Ontario protects information assets to fulfill its legislative mandate to ensure fair, secure, and transparent provincial elections and uphold electoral integrity for Ontarians.

EO adheres to related Government of Ontario policies, where practical and feasible, including the Government of Ontario Information and Technology Standards (GO-ITS).

Resilience and Risk Mitigation

EO is committed to ensuring that its digital information systems and infrastructure can anticipate, withstand, recover from, and adapt to cyber disruptions. EO emphasizes risk-informed decision making to maintain a secure and stable IT environment by proactively addressing known and potential threats.

Privacy and Data Protection

EO makes every reasonable effort to protect personal information appropriate to its sensitivity in order to maintain public trust and confidence. EO safeguards all components of an information technology environment against compromise to maintain the confidentiality, integrity, and availability of this information.

Responsive and Operational Readiness

EO will continually adapt its approach to address evolving cyber security risks and conditions. Given the unique nature of field activities, EO leadership may adopt EO-specific practices and procedures to protect information security and serve the public interest.

Section 3: Scope

This policy applies to all users of systems, workstations, networks, devices and data owned by Elections Ontario, including:

- All networks and infrastructure at EO's headquarters and field offices
- All employees (permanent and temporary), consultants, authorized users accessing EO's network and infrastructure, and election officials, including individuals retained by EO to manage the electoral process during general and by-elections (e.g. Returning Officer, Election Clerk, field employees, voting location employees, etc.), hereinafter referred to as EO personnel
- All components of an IT environment that store, process, or transmit information, whether managed directly by EO or by vendors and contractors on EO's behalf

This policy does not provide guidelines for implementing cyber security safeguards, including cyber threat monitoring. EO's Cyber Security team provides cyber security guidance, processes, and procedures.

This policy does not provide steps for managing privacy and security breaches or responding to cyber incidents. Refer to the following:

- The Privacy and Security Breach Management Protocol provides more information on the responsibilities of EO personnel and service providers in addressing breaches.
- *Cyber Security Incident Response Plan* provides classified guidance on incident response for authorized first responders.

This policy does not address the protection or retention of Personal Information (PI) in non-digital formats that are in EO's custody and control. Refer to the following:

- Elections Ontario's Privacy Policy provides more information on the collection, use, disclosure, retention, and safeguarding of personal information in all forms.
- Records Retention Schedule provides more information on the storage, retention, and disposal of EO records.

Section 4: Mandatory Requirements

Elections Ontario is committed to abiding by the following security standards:

4.1 Cyber Risk Assessment and ApprovalApproval

- EO will ensure risk is contained at the accepted and authorized level by deploying a cyber risk management process that continually assesses the security of information systems and infrastructure.

- EO's risk appetite and tolerance will be defined and approved by the Chief Electoral Officer. Any risks above tolerance will require formal approval to avoid, accept/mitigate, or transfer. Regular cyber security risk reporting will be delivered to EO leadership.

- EO will designate primary and alternate cyber security contacts who are responsible for communication with the Ministry of Public and Business Service Delivery and Procurement (MPBSDP). EO will provide notice of any change in designated contacts within 10 business days.

- EO will complete a cyber security maturity assessment, as required, based on its risk appetite. In accordance with organizational risk considerations and governance requirements, EO's designated contact will submit a summary of the assessment to the Chief Information Security Officer of MPBSDP promptly following completion.

4.2 Security Awareness and Training

- EO will ensure measures are in place to build the knowledge and awareness of EO personnel to recognize cyber security concerns and respond accordingly.

- EO personnel must understand their responsibilities for information security under this policy and other relevant policies, standards, and procedures, including those set out under the:
    - Computer and Technology Acceptable Use Policy
    - EO Privacy Policy
    - Privacy and Security Breach Management Protocol

- EO will provide role-based security training, simulated testing, and tools only for EO personnel whose job functions require them to fulfill security responsibilities and the requirements of this policy.

4.3 Access and Security Controls

- EO will implement a documented approval process in accordance with the IT Access Control and User Access Management Policy to authorize EO personnel and devices that require access to EO information systems.

- EO will implement appropriate safeguards to secure digital information systems and infrastructure to a degree consistent with the requirements outlined here or as may be outlined in other EO policies (listed in section 7) and applicable legislation.

- EO will implement additional safeguards when a threat risk assessment, cyber risk treatment plan, vulnerability management report, privacy impact assessment or other assessments identify risks to system security.

4.4 Service Provider and Third-Party Security

- EO will include security clauses that meet the requirements of this policy and applicable standards in contracts with service providers who have access to or share custody of EO's digital information systems and infrastructure. These contract requirements must also state that they extend to any subcontractors on whom service providers rely on to deliver services to EO or electors.

- EO will conduct due diligence and ongoing review of all service providers with access to EO's digital information systems or data. High-risk suppliers, as defined through risk assessment, will be continuously monitored.

- EO will require service providers to give advance notice of any changes to service delivery, including changes to technical infrastructure, the location or jurisdiction in which information is handled, service reconfiguration, or the use of other external parties (e.g. new subcontractors to support the provision of services).

4.5 Availability and Reliability of Information Systems and Resources

- EO will employ its Business Continuity Plan to ensure a timely and orderly recovery from disruption, emergency or outage caused by a cyber incident and resume critical business functions and service delivery to intended levels of quality and availability.

- EO will ensure that all systems and applications supporting critical functions and services have operational, verified, and tested disaster recovery plans in place to restore normal operation in the event of a cyber incident. Plans will be reviewed and tested periodically.

- EO will create and store data backups for information that may be needed to verify or replace records that have been falsified, lost or destroyed before their scheduled disposal date, in accordance with the Secure Storage, Transfer, and Destruction of Personal Information Procedure and in compliance with applicable legislation.

4.6 Cyber Incident Monitoring and Reporting

- EO will monitor digital information systems and infrastructure to detect and prevent potential security breaches.

- EO will implement a cyber security incident plan in the event of a cyber-related security breach. This plan explicitly defines the roles and responsibilities of authorized first responders and escalation reporting procedures to relevant parties.

- EO will report critical cyber security incidents to MPBSDP's Chief Information Security Officer within 72 hours of confirmation, including all information required by regulation.

- In accordance with the cyber security requirements and standards of this policy, the Computer and Technology Acceptable Use Policy and EO Privacy Policy, any person who causes or contributes to security incidents may be held accountable when their actions contravene training received, job specifications, agreements, corporate direction, policies, or law.

Section 5: Roles & Responsibilities

5.1 Chief Electoral Officer (CEO)

The CEO is responsible for:

- Approving policies that govern Elections Ontario's commitment to maintaining secure and stable digital information systems and infrastructure
- Providing strategic direction for the development and implementation of business practices that ensure the consistent application of this policy
- Ensuring that the principles and requirements of this policy are practiced, met, and reported on
- Approving risk assessments and risk management strategies, where appropriate, with the advice of the Chief Information Officer, the Manager of Cyber Security, and EO's Executive Team

5.2 Deputy Chief Electoral Officer

The Deputy Chief Electoral Officer (DCEO) may act in place of the CEO if required. If acting for the CEO, the DCEO is accountable for the same responsibilities assigned to the CEO.

5.3 Chief Information Officer (CIO)

The CIO is responsible for:

- Developing EO's cyber security strategy, including measures of effectiveness
- Providing direction on EO's cyber security policies and procedures
- Assessing compliance with this policy and standards
- Approving risk assessments and risk management strategies, where appropriate

5.4 Chief Privacy Officer (CPO)

The CPO is responsible for:

- Advising and supporting business operations and projects in understanding their privacy obligations in accordance with the EO Privacy Policy, and the policies and guidelines that flow from them
- Providing support and/or direction on privacy best practices as they relate to managing actual or potential privacy and security breaches, including the process, guidelines and tools required to assess whether a Privacy Impact Assessment is needed, and what it should address

5.5 Directors

Directors are responsible for:

- Providing resources to maintain a level of cyber security control consistent with this policy
- Identifying and implementing all processes, procedures and controls relative to cyber security standards defined by the business and this policy
- Fostering the participation of cyber security and technical staff in protecting digital assets, and in identifying, selecting and implementing appropriate and cost-effective security controls and procedures
- Managing breaches of this policy, and implementing mitigation measures to contain risks associated with noncompliance with this policy
- Implementing cyber-related business continuity and disaster recovery plans

5.6 Manager, Cyber Security

The Manager of Cyber Security is responsible for:

- Developing and implementing EO's cyber security program, which includes:
  - Providing incident response coordination and expertise
  - Monitoring networks for anomalies
  - Monitoring external sources for indications of data breaches, defacements, etc.
  - Maintaining ongoing contact with relevant parties
  - Providing timely notification of current threats and vulnerabilities
  - Providing awareness materials and training resources
- Assessing compliance with applicable cyber security policies and legislative cyber security requirements
- Overseeing the implementation of cyber security risk assessments and risk management activities
- Overseeing the monitoring and assessment of implemented security controls
- Advising on cyber security portions of proposals and other contracting documentation related to the procurement of products and services

- Escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures
- Disseminating threat information to appropriate parties
- Participating in the review and development of EO policies and procedures that have cyber security implications

5.7 EO Personnel

All EO personnel, including individuals retained by EO to manage the electoral process during general and by-elections (e.g. Returning Officer, Election Clerk, field employees, voting location employees, etc.) are responsible for:

- Understanding the baseline security controls necessary to protect EO's digital information systems and infrastructure being handled
- Protecting digital information systems and infrastructure to prevent unauthorized access, interruption or modification, theft or damage
- Following cyber security requirements and standards of this policy and other relevant EO policies and procedures, including: Computer and Technology Acceptable Use Policy, EO Privacy Policy, and IT Access Control and User Access Management Policy
- Reporting suspected cyber security incidents or weaknesses in accordance with the Privacy and Security Breach Management Protocol

Section 6: Glossary

The following 21 definitions are referred to throughout this policy:

Asset:

Anything that has value to the organization and requires protection. This includes information assets (e.g., data, records, and documents), digital assets (e.g., digital content, databases, cloud resources, and digital identities), and IT assets (e.g., hardware, software, applications, networks, and information systems), as well as supporting services and infrastructure.

Breach:

An information, security, or privacy event that compromises or discloses the confidentiality, integrity or availability of information or information systems.

Critical Cyber Incident:

An incident that affects (a) the security, continuity, confidentiality, integrity, or availability of Election Ontario's digital information (or the infrastructure that houses or transmits such information), and (b) meets at least one of the following criteria:

1. Causes a significant adverse impact on EO's delivery of public services.
2. Poses a risk to public safety.
3. Requires or results in significant recovery efforts for digital information or related infrastructure, or activation of cybersecurity incident response plans.
4. Poses a significant risk of harm to EO's reputation or public confidence.

Cyber Incident:

Any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete, or render unavailable EO's information assets, systems, workstations, networks, devices and/or any data owned by EO. A cyber security incident may compromise, or attempt to compromise, the confidentiality, integrity and availability of information owned by EO. These incidents can include cyberattacks, cyber threats, unauthorized access, denial of service, malicious code, and suspected or actual privacy or security breaches.

Cyber Risk:

The potential exposure to loss or harm stemming from EO's digital information or information systems. The possibility of damage or harm and the likelihood that damage or harm will be realized.

Cyber Security:

The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically,

cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.

Cyber Threat:

A circumstance, event, actor, or activity with the potential to exploit a vulnerability and adversely affect the confidentiality, integrity, or availability of information assets or information systems.

Digital Information Systems:

The technology environment used to collect, process, store, transmit, or manage digital information, including but not limited to applications, databases, hardware, networks, operating systems, servers, storage, and supporting infrastructure.

EO Personnel:

EO personnel include all employees (permanent and temporary), election officials, consultants, and authorized users accessing EO's network and infrastructure. This includes individuals retained by EO to manage the electoral process during general and by-elections (e.g. Returning Officer, Election Clerk, field employees, voting location employees, etc.).

Malware:

Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, ransomware, spyware, and adware.

Personal Information (PI):

Personally identifiable information about any individual, such as name, home address, home/cell phone number, personal email address, date of birth, social insurance number, voting-related information that identifies an individual, and financial information. It also includes personally identifiable information about EO personnel or service providers (e.g. about employees' education, health or employment history). PI can include any identifying number, symbol or other particular assigned to the individual. PI does not include business contact information. EO refers to the definition of PI set out in Ontario's Freedom of Information and Protection of Privacy Act, Section 2(1).

Phishing:

An attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking or spoofing a specific, usually well-known brand, usually for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.

Ransomware:

A type of malware that denies a user's access to a system or data until a sum of money is paid.

Risk Tolerance:

The amount and type of risk that EO is willing to accept in pursuit of its objectives. Risk tolerance guides decision-making and must comply with applicable legislative and regulatory requirements.

Safeguard:

A protective and precautionary measure or control intended to prevent a threat agent from causing harm and injury.

Security Control:

A management, operational, or technical safeguard implemented to protect information assets and information systems and maintain their confidentiality, integrity, and availability. Security controls can be applied by using a variety of security solutions that can include security products, security policies, security practices, and security procedures.

Sensitive Information:

Information that, if released without authorization, would cause harm (personal or enterprise injury, embarrassment, unfair economic advantage, etc.).

Service Provider/Vendor:

Companies or individuals (third parties) that provide products or services to EO and may have access to EO information, systems, networks, infrastructure, or personal information while performing those services.

Unauthorized:

Without the approval, authority, or permission of the designated EO personnel or their delegate.

Users:

All EO employees, contractors, subcontractors, temporary agency workers, ROs and other election officials (including field staff and poll officials), consultants and service providers, as well as other users who have been authorized to have access to EO information systems and applications.

Vulnerability:

A flaw or weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Section 7: Additional References

The following table identifies those Elections Ontario policies and procedures and industry best practices that expand upon Elections Ontario's Cyber Security Policy.

Document Name	Author(s)
1. Cross-Sector Cyber Security Readiness Goals Toolkit	Government of Canada
2. Enhancing Digital Security and Trust Act, 2024	Government of Ontario
3. Corporate Policy on Cyber Security and Cyber Risk Management	Government of Ontario
4. Elections Ontario Privacy Policy	Elections Ontario
5. IT Access Control and User Access Management Policy	Elections Ontario
6. Computer and Technology Acceptable Use Policy	Elections Ontario
7. Secure Storage, Transfer, and Destruction of Personal Information Procedure	Elections Ontario
8. Cyber Security Incident Response Plan	Elections Ontario
9. Privacy and Security Breach Management Protocol	Elections Ontario
10. Business Continuity Plan	Elections Ontario
11. Emergency Management Plan	Elections Ontario
12. Records Retention Schedule	Elections Ontario

Section 8: Approval

The following table shows the authorization, amendment, and review dates for this policy.

Cyber Security Policy	
Authorization	Greg Essensa Chief Electoral Officer Date: July 27, 2026
Effective date	July 27, 2026
Date last amended	July 2026
Date of next review (Once per election cycle)	July 2028
Contact officer	ceo@elections.on.ca