Elections Ontario

Computer and Technology Acceptable Use Policy

Table of Contents

1. Explanatory Note

The Computer and Technology Acceptable Use Policy for Elections Ontario (EO) establishes the standards for the protection and security of EO information systems, technology infrastructure and non-computer resources that contain EO information assets. This policy is guided by overarching privacy and security protection principles reflected in legislative framework and industry standards that apply to government agencies in Ontario and is in conformity with the standards and expectations of Elections Ontario's data partners.

This policy is owned by the Director Technology Services who is responsible to regularly (e.g., annually) review and revise the policy (as required), monitor compliance, and oversee training (in consultation with EO training specialists) and enforcement activities where appropriate.

2. Purpose

EO requires IT systems and resources to be used for conducting the business of EO with reasonable allowances for personal use. EO requires that all employees will not use IT systems in an illegal, immoral, unethical or harmful manner. The purpose of this policy is to:

- Ensure information assets are protected from unauthorized access, loss, damage or disposal and to reduce the risk of damage to papers, media and information;
- Protect EO's interest in ensuring that computer and technology resources are used only for EO business and other approved purposes;
- Define the security requirements for computer and technology resources; and
- Ensure that the use of computer and technology resources do not result in unacceptable risks to EO.

3. Scope

This policy extends to all information systems and technology infrastructure managed by EO and to all non-EO computer resources that contain EO information assets. The scope of information technology resources includes, but is not limited to the following:

- Desktops
- Laptops
- PDAs (e.g. BlackBerry devices)
- Servers
- Tablets
- All storage media (e.g. CDs/DVDs, memory sticks, discs)

Also included in the scope of this document are information systems and resources that are used by, or on behalf of EO to create, enter, process, communicate, transport, disseminate, store or dispose of information (e.g., infrastructure and services provided by ITS).

This policy applies to all EO employees, contractors, sub-contractors, Returning Officers, other election officials, and to other users who have been authorized by any of the above to have access to EO information systems/assets (e.g., system users). For the purpose of this policy, such individuals are referred to collectively as "users" unless otherwise specified.

Given the close working relationship between EO and Ministry of Government Services (MGS) Information and Technology Services (ITS) group with regards to information technology, EO will strive to adhere to MGS policies as they relate to technology. However, given the unique nature of field activities (e.g., the urgency of ramp-up once an election has been called), EO leadership may choose to adopt different practices and procedures.

4. Definitions and Abbreviations

The following table defines applicable terminology used in this policy.

Term	Definition
Authentication	Authentication is the process by which an IT system validates the credential entered by the user. For example, an identity is deemed to be authenticated when a secret password is used in conjunction with a User Identification (User ID).
Authorization	Access to EO systems and information assets must be limited, except to users that have been specifically granted access on a need to know basis or the principle of "What must be generally forbidden unless expressly permitted". Authorization mechanisms must be used to allow, deny or limit a user's access or permissions to a resource.
Beyond Reasonable Repair	Refers to equipment requiring repair or upgrade with an unexpected cost close to the cost of total replacement.
Corporate Software	Software required by EO and used for the business purposes of EO.
Disposal	Refers to the reselling, recycling, donating or discarding of IT equipment.
EMS	The Elections Management System (EMS) solution at Elections Ontario (EO) is the mission critical system for the running and the management of an election event, as well as the day-to-day operations necessary for planning and executing events. EMS works as a "fully-integrated solution" meant to provide all functionality necessary for running and managing events.
ELMS	Elector List Management System. ELMS is an application that supports event delivery including elector list management in the field. ELMS is used at each RO during an electoral event to complete the following tasks: manage elector data; track certificates and ballots; managing geographic data; managing polls and voting locations; record results; and print reports.
Freeware	Software that is freely distributed where no license fee is required for use.
Highly Sensitive Information	Any information that can identify an individual (individual elector or employee) including: name, address, phone number, gender, date of birth, SIN, voting information and financial information (as it relates to elections finances). Highly sensitive data can also include confidential information such as financial information (e.g., employee salaries), planning information (e.g., budgets, Returning Office operational plans) or contracts or agreements of EO; as well as information relating to security configuration of any of EO's IT systems (e.g., audit logs, passwords, encryption keys, etc.). When this information is collected, accessed, used, disclosed, modified, destroyed, lost or stolen in an unauthorized manner, it has a high risk of causing harm to the organization (e.g., reputational) or to individuals (e.g., identify fraud).

Term	Definition
Identification	Identification is the process of identifying an individual and associating this individual with a credential or User ID.
Low Sensitivity Information	Information considered to be of low sensitivity includes: aggregate information about the electoral process (e.g., how many individuals voted for each party within a polling division or electoral district), EO business activities, non-confidential information (e.g., marketing information). Threat of loss, theft, or unauthorized access to this information poses low to no business risk to EO or to individuals.
Obsolete	Refers to any equipment that has been fully depreciated according to EO's accounting standards (over 4 years old) and / or equipment that is technologically outdated or non-functional for company business processes). It is the goal of the company to reassign IT assets wherever possible in order to achieve full return on investment (ROI) from the equipment and to minimize hardware expenditures.
Personal Information	Personally identifiable Identifying information collected by EO about any individual, such as name, home address, home phone number, personal email address, gender, date of birth, social insurance number, voting information, and financial information (e.g., contributions to political parties) and . It also includes personally identifiable information about EO employees (e.g., confidential employee-related information such as information about employees' education, health or employment history) or confidential information (e.g., personal information identified in RFP responses), but does not include business contact information.
Personal Software	Software provided by the employee that is not prescribed or supported by EO.
Privacy/Security Breach	An event that contravenes EO's Privacy Policy and the EO Code of Conduct, and compromises the confidentiality, integrity, or availability of personal information or any other highly sensitive information for which EO is directly responsible. Security breaches may also be or lead to privacy breaches where personally identifiable information is inappropriately accessed, collected, used, disclosed or modified.
PREO	Permanent Register of Electors for Ontario is an up-to-date database of eligible Ontario voters. PREO contains the elector's name, address, date of birth and gender. It is maintained for electoral purposes only.
Service Provider	Companies or individuals (third parties) that perform services on EO's behalf and for EO's purposes and not their own.
Shareware	Software that is commonly distributed for use but requires a registration or license fee be paid to the developer or distributor of the product.
Test of Beta Software	Software currently under development that is available for use for test purposes.

5. Responsibilities

This policy requires all system users to ensure all computer resources that contain EO information assets (e.g., confidential business information and identifiable personal information) are protected from unauthorized access, loss, damage or disposal, during and outside working hours. The following table summarizes the roles and respective responsibilities of all EO users. All EO users are responsible for understanding the elements of this policy and understand that monitoring will occur to measure compliance.

5.1. Key Roles

Role	Responsibilities
Chief Privacy Officer	The Chief Privacy Officer is responsible for managing actual or potential privacy breaches. The Chief Privacy Officer will also provide support and/or direction to the Director of Technology Services on privacy best practices as they relate to acceptable use of personal information.
Director of Technology Services	The Director of Technology Services is responsible for overseeing the implementation of this policy, including monitoring compliance with the policy. The Director of Technology Services is also responsible for managing actual or potential IT security breaches and monitoring compliance with this policy and providing direction to users on appropriate use. Where an IT security breach has the potential to be a privacy breach, the Director of Technology Services will engage the Chief Privacy Officer.
Data Steward	Individual who is responsible for a data holding/system with respect to provision access requests, identifying and managing change requests, and supporting business processes.
Human Resources (HR)	HR will work with the Director of Technology Services and the Director of Communications to ensure employees are appropriate trained on this policy through EO's on-boarding process. HR will also support the Director of Technology Services and other Senior Leadership in effectively enforcing this policy.
ITS	The Government of Ontario Information & Technology Standards (GO-ITS) are the official publications concerning the standards, guidelines, technical reports and preferred practices adopted by the Information Technology Standards Council under delegated authority of the Management Board of Cabinet.
Users	All users are responsible for: • Complying with directives, policies, procedures and standards when using information and information systems, including this policy; • Attending privacy and security training with respect to acceptable use of information and information systems; • Using information and information systems in compliance with this policy; • Using EO issued hardware and software only as authorized under this policy; • Reporting all privacy and security incidents, in accordance with EO's Privacy and Security Breach Management Procedure, to the Chief Privacy Officer immediately upon discovery of an incident and/or possible incident. Users include all EO employees (Headquarter and RO/field employees), contractors, sub-contractors, Returning Officers, and other election officials.

5.2. Monitoring

System monitoring is performed for the purpose of systems analysis, planning and performance, and is considered to be an on-going and regular technology management activity unaffected by the scope of this policy.

If during the course of systems monitoring, potentially illegal or unacceptable use of EO resources is identified, the result of the systems monitoring may be used in further investigation and may result in disciplinary actions.

Personal monitoring of a particular individual's usage will take place if there is reasonable belief that EO resources are being used inappropriately. Personal monitoring is designed to determine whether there is evidence of inappropriate use, and if so, whether disciplinary action and/or legal action is appropriate.

Authorization: All personal monitoring must be approved by the user's Director or equivalent prior to monitoring and evidence gathering.

Complaints or concerns of Internet misuse must be reported to the Director of Technology Services.

5.3. Identification and Authentication

To provide for the accountability of the computer system utilization and to satisfy the requirement for authentication, the following must be invoked:

a) Unique user identifiers (e.g., User IDs) must be used to identify all individuals. Shared and/or Generic IDs may not be used;

   This unique user identifier will provide:

   i) Proof of identity;
   ii) Access to authorized networks, systems and information assets;
   iii) The basis for non-repudiation and proof of action;
   iv) Individual accountability of actions; and
   v) A record of action that can be used for audit and accounting purposes.

b) An authentication mechanism (e.g., password) must be used in conjunction with the user identifier (see below for an explanation on the various authentication methods);

   Authentication mechanisms (e.g., passwords, pin) must:

   i) Be used to authenticate a user identity;
   ii) Be kept secret; and
   iii) Be changed on a regular basis.

   Authentication mechanisms (e.g., password, pin) must not:

   iv) Be vulnerable to guessing or dictionary search attacks;
   v) Be derived or guessed from information easily obtained about the user; and
   vi) Be so obscure that the user will need to record it for reference.

c) Identification and authentication credentials are classified as *confidential* and must be treated accordingly with approved encryption;

d) Any applications requiring system level connections that require passwords to be stored on computers (e.g., ELMS) should be stored in encrypted format;

e) User management processes must keep track of all current user identities;

f) Unsuccessful authentication attempts must be limited and must be logged;

g) Encryption keys used for EO confidential information (e.g., highly sensitive business information and/or identifiable personal information) must be stored centrally with the Director of Technology Services.

See section 5.3.2 for password management guidelines.

5.3.1. Password Management

Passwords are a common way to verify the identity of a user and to prevent intruders from impersonating legitimate users. The protection of passwords depends on the efforts of users to maintain them in strict confidence. Password owners are responsible for any access to EO systems gained through the use of their passwords.

Passwords must:

- Be chosen so that they are easy enough to remember but not easily guessed by someone else;
- Contain at least 8 characters; and
- Contain at least one digit and a least one capital letter.
- Example: Good2Bback

Passwords must not:

- Include easily identifiable personal information about the owner (e.g., names of family members, pets, birthdays, anniversaries, or hobbies);
- Be any words, phrases, or acronyms that are part of the broadly recognized EO culture;
- Be the same as all or part of a user's login id, actual last or given names, or a commonly known nickname; and
- Be shared with anyone (including system administrators and management) or written down on paper near the vicinity of the system.

A User who suspects his/her password has been breached must change it immediately and report the incident to his/her manager or the IT Service Desk.

5.4. Authorization

To provide authorization, the following must be in place:

a) Each individual must have a unique User ID and be authenticated as per the policy;

b) Systems must restrict access and execution of system resources to authorized individuals;

c) Changes in user permissions that are initiated automatically by the information system and those initiated by the Data Steward must be managed appropriately;

d) Authorization may not be required for users that need to access public or unclassified data;

e) The Data Steward will grant authorization for data or system access based on the role of the user, the type of access required, and the classification of the data;

f) Data Stewards are responsible for determining the access rights or permissions users must have to access EO's information assets. The responsibility for managing or administering access rights can be formally delegated to the selected members of Technology Services team; and

g) Access rights are monitored at least annually by the Data Steward in conjunction with the appropriate business owner.

5.4.1. Granting Authorization

Authorization granted is based on:

a) Unique user identification or role assigned to the user;

b) Functions of the user or role;

c) Rules that govern user or role-based access;

d) Classification of the information asset;

e) Application of override requests and rules; and

f) Direction from the Data Steward of the information asset.

5.5. Disposal of Information Assets

Note: This section should be read in conjunction with EO's Personal Information Use and Retention Procedure.

Stringent security measures are enforced to control the disposal of all EO information assets. These include but are not limited to the following:

5.5.1. Determination of Obsolescence

a) Identifying and classifying IT assets as obsolete is the responsibility of Technology Services.

b) Equipment lifecycles are to be determined by Technology Services operating procedures, which will be aligned to ITS standards as appropriate, and with the consideration of the equipment depreciation schedule as per EO accounting standards.

5.5.2. Disposal Considerations

Once the equipment is determined to be obsolete and the decision has been made to dispose it off, Technology Services, in partnership with ITS, will determine the method of the disposal based on the following considerations:

a) The equipment may be used as a trade-in against cost of replacement item.

b) Equipment determined as "Non-functional and beyond reasonable repair" may be dismantled for recovery of useable parts.

5.5.3. Pre-disposal Procedures

a) Once equipment is determined to be obsolete or disposable, Technology Services will delete all files, company-licensed programs, and applications using a pre-approved disk-sanitizer. This sanitizer must completely over-write all disk sectors of the machine with zero-filled blocks.

b) It is the responsibility of the user to ensure that all sensitive data written on hard drives, CD-ROMs, tapes, discs etc. is archived with Technology Services before being deleted, as appropriate.

c) Technology Services will remove any company tags and/ or identifying labels.

5.5.4. Disposal Procedures

Technology Services will decide on the appropriate method of disposal, including, in accordance with environmental laws, and in coordination with ITS policies/procedures, as appropriate. Technology Services will arrange for the equipment to be appropriately sanitized.

5.5.5. Disposal or Re-Use of Electronic Data Storage Devices

a) Surplus computers and associated hard drives must have all sensitive data and licensed software removed and overwritten, to an approved standard (e.g., Military level disc format standard), or by physical destruction of the equipment prior to disposal or making these devices available for re-use;

b) Assets disposed of are identified by a tag number and this list is held by Technology Services for future reference.

c) Software stored on discs, tapes, CD-ROMs, USB keys and any other external electronic media is destroyed prior to disposal or re-use;

d) Defective hard drives must be sent to Technology Services for proper processing; and

e) Hardware may be returned to the vendor if all data on the hard drive is removed or overwritten. The hardware may not be returned to the vendor if it is inoperable, or if EO approved data wiping software or overwriting software is unable to wipe the data completely.

5.5.6. Return of Rental, Lease, Loaned and Evaluation Computers

a) EO rents and/or leases computers on the basis of either not returning the hard drives to the vendor or under the condition that the hard drive is wiped, as per standards set by ITS. If inoperable, the hard drive is destroyed by EO. When using loaned and evaluation computers, EO should use removable and encrypted storage media wherever possible.

b) EO should make best efforts to replace the hard drives with comparable and compatible blank devices; and

c) EO must ensure that outside organizations agree with these conditions before accepting the loaned computers.

5.5.7. Disposal of Data Stored on Non-EO Data Storage Devices

a) If services are contracted to a service provider and EO Information assets are stored on non-EO electronic data storage devices (internal and external hard drives, discs, tapes, CD-ROMs, USB keys, and any other electronic media that stores data), then the contract must contain provisions for the confidentiality and security of data.

b) These contracts must also include provisions acceptable to EO for disposition of EO data upon contract completion or termination.

c) A certificate of physical destruction must be provided to EO.

5.5.8. Wrongful Disclosure of Information

All wrongful disclosures of information (e.g., unauthorized/inappropriate disclosures that result in an actual or potential breach) must be brought to the attention of the CPO, who will determine what further action needs to be taken, in accordance with the EO Privacy and Security Breach Management Procedure, and in consultation with the Director of Technology Services.

5.6. Clean Desk and Clear Screen

EO requires all users to keep a clean desk and clear screen (for unattended desktops) to protect information assets and reduce the risks of unauthorized access, loss of, and damage to information during and outside normal working hours.

a) All confidential documentation that exists in hard copy or on password protected and encrypted portable/removable media (e.g., laptops, USB keys, external hard drives, mobile phones) must be stored in locked drawers and cabinets when not in use and after office hours;

b) All confidential, critical business and/or personal information on EO employees and electors must be locked away when unattended and after working hours;

c) All employees are expected to maintain a “clean desk” whenever leaving the office at the end of the day;

d) Confidential information must be cleared from printers immediately;

e) Computer screens and all other displays must not face access doors or windows where they can be viewed by unauthorized persons;

f) Access to terminals, or other input device, is to be prevented when they are left unattended for any period of time in an unprotected area or where there is a risk of unauthorized access;

g) Screen savers with password logon will be used on all machines and configured to initiate within 15 minutes of user inactivity for machines not physically restricted from access.

h) Users with computers in high traffic areas (e.g., employees in cubicles) should use secure screens guards to avoid over the shoulder browsing of screen content.

i) Secure and private printers should be used when printing confidential or higher documents (e.g., payroll information, performance reviews).

j) Users must only store personal data (e.g., family photos) on ”Mysite”. If such data is found on EO network drives, the data may be deleted without notice.

k) Users are to keep their passwords and user-ID’s private, and shall log off the Internet and network if they will be away from their work area for a prolonged period of time.

5.7. Appropriate Use of Information Systems

It is the responsibility of EO users to utilize EO’s information and information systems/equipment in a responsible and professional manner. Compliance with this policy includes but is not limited to the following:

a) Users of EO provided information and information systems and/or equipment must use them to support the business of EO;

b) Personal use of EO information, information systems and/or equipment must not impact the operation of EO business. All personal programs, data, system access or equipment are subject to review to determine if they are having a negative effect on EO business;

c) Users must not distribute to any external parties any product or information asset without appropriate authorization;

d) Users are prohibited from violating any laws or participating in a crime or other unlawful or improper purpose;

e) Users must not cause intentional harm or disruption to a system;

f) Theft or copying of information classified as *confidential*, without authorization is prohibited;

g) Users must not utilize the information systems, equipment and/or networks of EO to gain unauthorized access to other systems or other organization's systems;

h) Users must not initiate actions that defeat or circumvent EO security measures;

i) Users are prohibited from creating or introducing computer-based material which is intended to be harmful to the operation of any computing system (e.g., viruses);

j) Users must not violate office decorum (e.g., inappropriate screen savers); and

k) Users must not access, display, download, create, distribute or store any software, graphics, images, text, music, video or other data (including email messages and attachments) which are offensive and conducive to a poisoned work environment, in accordance with EO's Mutual Respect in the Workplace Policy.

l) Users must ensure that EO devices and information is protected from access by unauthorized individuals (e.g., friends, family)

m) Users must report any suspected security incident(s) to their manager as soon as possible

5.8. Appropriate Use of the Internet

5.8.1. Access to the Internet

a) All access to the Internet must be made through an authorized and controlled and/or monitored (e.g., site activity loges) Internet access gateway. Any attempt to access the Internet by circumventing or defeating the authorized access methods will be deemed to be a serious breach of this policy; and

b) Users accessing the internet from EO laptops at home should not change the EO default settings within Internet Explorer (or any other browser).

5.8.2. Acceptable Business Use

a) Communicating with employees, the public and suppliers. Confidential or sensitive information must not be sent via the Internet unless a proper encryption is used;

b) Researching relevant business topics or obtaining useful business information; and

c) Maintaining business information on the EO website.

5.8.3. Acceptable Personal Use

a) Personal use of the Internet is only permitted where such use:

   i) does not interfere with work at EO;
   ii) is not for personal financial gain;
   iii) does not add to EO' costs; and
   iv) adheres strictly to this policy.

b) Any personal use that does not fulfill all these conditions is prohibited.

5.8.4. Prohibited Use of the Internet

Internet use is prohibited for any unauthorized, unlawful, or illegal purpose or activity that violates any federal, provincial or municipal law or regulation or that could give rise to a complaint or civil cause of action against the employee and/or EO.

This includes any activity that could constitute a criminal or quasi-criminal offence and/or result in civil liability including but not limited to the following:

a) Possessing, downloading, distributing or displaying any pornography or child pornography including obscene or sexually explicit material;

b) Possessing, downloading, distributing or displaying any material of a harassing nature in violation of the Ontario Human Rights Code, the EO Code of Conduct, or The Occupational Health and Safety Act including any form of harassment on the basis of race, creed, religion, colour, gender sexual orientation, marital status, family status, disability, physical size or weight, age, nationality, ancestry or place of origin. This includes any form of hate propaganda or messages that promote hatred or incite violence against identifiable groups;

c) Violating or infringing the Copyright Act or the Trademarks Act by, for example, violating another person's copyright without permission or authorization or by making unauthorized use of patents or trademarks;

d) Possessing, downloading, distributing or displaying any type of defamatory statements or providing inaccurate or misleading information which may lead to complaints or civil lawsuits against the employee and/or EO;

e) Circumventing the supplied Internet access from an EO issued device within EO's *headquarters network* is prohibited.

f) Activities relating to hacking and/or breaches of computer security such as attempts to defeat security features of electronic networks including making, possessing or distributing computer programs designed to obtain unlawful access to computer systems, or an attempt to spread viruses;

g) Any use relating to personal and/or commercial activity that may result in personal financial gain, including but not limited to, any personal or commercial advertising, solicitations or promotions that do not directly benefit EO;

h) Unauthorized access to another employee's personal Internet account, including obtaining or modifying of files, data or passwords belonging to others, or intercepting any private communication or electronic mail without authorization, other than as required by EO for business purposes;

i) Disclosure of trade secrets or confidential business information of EO (e.g., procurement/vendor information) or data partners/suppliers, without prior authorization.

j) Uploading or transmittal of highly sensitive information to non-secure and unencrypted cloud-based storage sites (e.g., Dropbox, personal email accounts)

Employees who encounter a prohibited activity must immediately report the incident to the Director of Technology Services via email or phone within one hour of identifying a prohibited activity and by completing the Privacy and Security Incident Management Form (for Headquarter employees) and the Incident Report Form (F0040) (for all RO employees), in accordance with the Privacy and Security Breach Management Protocol. The Director of Technology Services will work with the Chief Privacy Officer as required, to determine whether an investigation must be undertaken. Issues relating to respect in the workplace must be reported to a human resources manager and will be handled in accordance with EO's Mutual Respect in the Workplace Policy. Confidentiality will be maintained throughout the investigation process to the extent practical and appropriate under the circumstances. If a reported activity warrants an investigation, employees involved will be notified and kept up to date on the status of the investigation.

5.8.5. Communicating Via the Internet

There is no guarantee of privacy with the Internet. Users must treat any transmission like an electronic postcard; if the content is not appropriate on a postcard, it must not be posted to the Internet. Users must apply good judgement when using the Internet. Security and confidentiality of EO business and elector information is to be everyone's first concern.

5.8.6. Internet Users' Accountability

a) All users must be aware of, and understand this policy and apply it to the usage of any Internet available information or service;

b) Users who create and transmit messages are responsible for the content of the message including any attachments;

c) No information classified as *Confidential* must be sent or received using Internet communications, unless encrypted;

d) Users corresponding over the Internet shall identify themselves honestly and accurately;

e) Any computer executable software or other material obtained from Internet sources must be subject to comprehensive virus scanning processes before being enabled;

f) The Internet access gateway may be monitored, audited and even blocked if required;

g) Reviews will be conducted from time to time to ensure compliance to policy.

5.9. Communicating via E-mail and Fax

The following communications should be attached to all electronic communications to external stakeholders where highly-confidential information is included:

Email Message

Confidentiality Warning: This message and any attachments are intended only for the use of the intended recipient(s), are confidential, and may be privileged. If you are not the intended recipient, you are hereby notified that any review, retransmission, conversion to hard copy, copying, circulation or other use of this message and any attachments is strictly prohibited. If you are not the intended recipient, please notify the sender immediately by return e-mail, and delete this message and any attachments from your system.

Information confidentielle: Le présent message, ainsi que tout fichier qui y est joint, est envoyé à l'intention exclusive de son ou de ses destinataires; il est de nature confidentielle et peut constituer une information privilégiée. Nous avertissons toute personne autre que le destinataire prévu que tout examen, réacheminement, impression, copie, distribution ou autre utilisation de ce message et de tout fichier qui y est joint est strictement interdit. Si vous n'êtes pas le destinataire prévu, veuillez en aviser immédiatement l'expéditeur par retour de courriel et supprimer ce message et tout document joint de votre système. Merci.

Fax Message

Confidentiality Warning: This message and any attachments are intended only for the use of the intended recipient(s), are confidential, and may be privileged. If you are not the intended recipient, you are hereby notified that any review, retransmission, conversion to hard copy, copying, circulation or other use of this message and any attachments is strictly prohibited. If you are not the intended recipient, please notify the sender immediately by return fax 1-416-326-6200, and delete this message and any attachments from your system.

Information confidentielle: Le présent message, ainsi que tout fichier qui y est joint, est envoyé à l'intention exclusive de son ou de ses destinataires; il est de nature confidentielle et peut constituer une information privilégiée. Nous avertissons toute personne autre que le destinataire prévu que tout examen, réacheminement, impression, copie, distribution ou autre utilisation de ce message et de tout fichier qui y est joint est strictement interdit. Si vous n'êtes pas le destinataire prévu, veuillez en aviser immédiatement l'expéditeur par retour fax 1-416-326-6200 et supprimer ce message et tout document joint de votre système. Merci.

5.10. Appropriate Use Software

This policy applies to all shareware, freeware, personal, test and corporate software. Only software on the approved software list (maintained by Technology Services) is authorized to be installed on EO's systems. Installation of any other software requires written permission from the Director of Technology Services.

EO requires that all users strictly adhere to the terms and conditions of any software license and copyright agreements associated with the individual software products in their possession or control. Knowledge of all software license and copyright agreement requirements is a prerequisite for use of all software. Unfamiliarity with a software licensing agreement is not a valid excuse for non-compliance. To assure compliance with the terms and conditions regarding software license and copyright:

a) Documented proof of license and registration must be available and in control of the Technology Services for all proprietary software installed on EO processing equipment. Proprietary software is software copyrighted by someone other than EO.

b) All copies of the software are to be made by Technology Services in accordance with the terms and conditions specified in the software licensing agreements.

c) Adhere to the version and upgrade provisions identified in the licensing agreements.

d) Ensure any software utilized on non-EO provided processing equipment be appropriately licensed if it is used for any EO related business purposes.

e) Remove proprietary software after completing demonstrations, evaluations or diagnostic testing while it is not licensed.

f) Be aware that any non-EO provided software may not be supported by EO and may be subject to removal from EO equipment if conflicts or problems are encountered with the coexistence with EO provided software.

g) In the event that unlicensed software is encountered by Technology Services within the EO environment, it must be removed or an appropriate license must be ordered for continued operation of the software.

5.10.1. Practices that Violate Software Licenses and Copyrights

Users must not violate any software licenses or copyright laws while using any of EO's systems or network. Violation of this policy is considered an unacceptable use by EO. Examples of software license and copyright violations include:

a) Copying software for testing purposes prior to purchase without authorization from the vendor;

b) Creating temporary copies of software products to use until a purchased copy is available without authorization from the vendor;

c) Using software specifically deemed as shareware/freeware for non-commercial use in a corporate environment;

d) Copying EO provided software for use on other than the licensed processor;

e) Retaining any evaluation or demo copies of software past the expiration of an authorized trial period.

5.11. Virus Protection

EO employees must not knowingly introduce a virus, or any other malicious code, to any information technology resource. All suspected virus incidents must be reported to the appropriate program manager or the Director of Technology Services.

All EO hardware should have virus protection software built-in as the default setting.

5.12. Protection of Portable/Removable Devices

Stringent security measures must be used for all portable and removable devices. Users must only use EO issued portable or removable devices and all devices must have encryption enabled software. Additional security measures include but are not limited to the following:

a) All users in possession of EO owned portable/removable devices must not check these systems in transportation luggage systems. They are to remain in the possession of a traveler at all times;

b) Storage of data classified as *Confidential* on portable equipment must be protected by power on, administrator and hard disk passwords and encryption techniques must be used;

c) Access to the applications and data utilized on portable equipment must be protected by an authenticating password or other authentication mechanism;

d) Portable and removable devices must be used primarily to carry out the business of EO;

e) Cable locks must be used to secure portable devices, such as laptops both within Headquarters, the field, home offices or another off-site location;

f) All EO' equipment, especially portable equipment is the responsibility of the user to secure while in the EO user's possession (e.g. using laptop locks or lockable cabinets);

g) User must use encryption technology when using portable storage devices (e.g., blackberries, USB storage devices, laptops, tablet computers). All encryption technology will be installed and provided by Technology Services. Users are required to follow the directions given by Technology Services for using and maintaining encryption technology (e.g. storing of encryption keys); and

h) Portable/removable devices containing confidential data should only be retained for as long as required to complete the operational needs to EO and in accordance with EO's retention schedule. Once data stored on a portal/removable media device is no longer required, it must be erased in compliance with this policy and the EO destruction policy and be completed by Technology Services.

Technology Services maintains a record of users who have been issued portable/removable media devices.

5.13. Protection of Windows Desktop Equipment

Stringent security measures must be used for all desktop equipment. These include but are not limited to the following:

a) New acquisitions, replacements or upgrades have to be consistent with EO policies. These activities have to be authorized for the Director of Technology Services (or Designate);

b) Any hardware change the user may make has to be approved by the Director of Technology Services and it must be documented;

c) Software (operating systems, tools, etc.) the user may install or remove also has to be approved by the Director of Technology Services and it must be documented;

d) Windows Operating systems provide advanced security, but only if the desktops are configured with appropriate security settings, administered adequately, and kept up to date with operating system patches. Users are prohibit from making changes to these settings;

e) All confidential business data and identifiable personal information must only be stored on the EO network. Users are prohibited from storing such information on the hard drives of their computers;

f) Access to the applications and data utilized on desktop equipment must be protected by an authenticating password or other authentication mechanism; and

g) Users are responsible to operate the workstation securely and in compliance with this policy.

Technology Services maintains a record of users who have been issued desktop equipment.

6. Education and Training

All users must receive training on this policy and other related policies and procedures.

To satisfy this requirement, all users will be required to attend privacy and security training as part of their on-boarding to the organization and on an annual basis as part of their privacy and security compliance requirements. Users working in the field will be provided training through the field training process. Training will be monitored for adherence. All training materials will be available within internal sites (e.g., eoPedia, SharePoint) and easily accessible.

7. Enforcement

The Director, Technology Services is responsible for overseeing compliance with this policy. The Director, Technology Services/delegate will monitor compliance.

Any persons found not complying with this policy will be held accountable when their actions contravene training, agreements/oaths, policies or law, will be investigated in line with the Progressive Discipline guidelines set-out by the Legislative Assembly.

8. References: Related Policies and Procedures

	Document Name	Author(s)
1	*Elections Ontario Privacy Policy*	Elections Ontario
2	*Personal Information Use and Retention Procedure*	Elections Ontario
3	*Privacy and Security Breach Management Procedure*	Elections Ontario
4	*Acceptable Use of Information and Information Technology (I&IT) Resources Policy*	MGS

	Document Name	Author(s)
5	*Corporate Policy on Information and Information Technology (I&IT) Security.*	MGS
6	*Information Security and Privacy Classification Policy*	MGS
7	*Progressive Discipline Guidelines*	Legislative Assembly