Ministry of Government Services
Office of the Corporate Chief Information Officer
Corporate Security Branch

Acceptable Use of Information and Information Technology (I&IT) Resources Policy

March 2011

Table of Contents

1. INTRODUCTION

Information and Information Technology (I&IT) resources simplify government work and enhance communications across the OPS. They have been acquired by the Government of Ontario and allocated to users for the purpose of conducting government business, and are the property of the government.

Use of government resources is governed by the employment and ethical frameworks of the Public Service of Ontario Act, 2006 (PSOA). Ontario Public Service (OPS) I&IT resources are to be used for Ontario government business purposes only. Inappropriate use of OPS I&IT resources poses risks and potential liability for the Ontario government. Unacceptable use of these resources may result in disciplinary action. It is the responsibility of public servants, as users of OPS I&IT resources, to understand and comply with related mandatory requirements and to conduct their actions accordingly.

2. PURPOSE

1. To protect the government's interest in ensuring that I&IT resources are used only for government business and other approved purposes.

2. To define the security requirements for the use of Ontario government I&IT resources.

3. To ensure that the use of I&IT resources does not result in unacceptable risks to the government of Ontario.

3. TERMS

Within this document, certain words have been assigned specific meanings. There are precise requirements and obligations associated with the following terms:

Must: This requirement is mandatory.

Should: The requirement ought to be adhered to, unless exigent business needs dictate otherwise and the full implications of non-compliance are understood.

Related directives, policies, standards, procedures and other documents are listed and linked at the end of this document, in the section called "Supporting Documents".

4. APPLICATION AND SCOPE

The authority to issue this Policy is established in the Information and Information Technology (I&IT) Directive.

This policy applies to:

- all ministries and public bodies (formerly agencies, boards and commissions) that use Ontario government I&IT resources; and,
- all third party individuals and organizations that have been authorized by the Ontario government, for government purposes, to have access to the OPS integrated network and use of computerized devices.

The scope of information includes all information that is created, received, owned by or held in custody on behalf of the Ontario government. The scope of information technology resources includes, but is not limited to the following:

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

Also included in the scope of this document are information systems and resources that are used by, or on behalf of the Ontario government to create, enter, process, communicate, transport, disseminate, store or dispose of information.

5. PRINCIPLES

1. Use of I&IT resources must be in compliance with the employment and ethical frameworks of the PSOA, 2006 and in keeping with the OPS organizational values of trust, fairness, diversity, excellence, creativity, collaboration, efficiency and effectiveness. As such, I&IT resources are to be used for government business purposes that support the operations and service delivery objectives of ministries and public bodies.

2. Each ministry and public body employee or contractor is personally accountable for his/her use of any Ontario government I&IT resources.

3. Use of government computers, networks, systems and software may be subject to monitoring.

4. Unacceptable use of I&IT resources may result in progressive discipline up to and including dismissal, and/or criminal charges when warranted.

6. MANDATORY POLICY REQUIREMENTS

The mandatory requirements of the policy are as follows:

6.1. Education and Training

All users **must** receive training on:

- The *Acceptable Use of Information & Information Technology Resources Policy* and other related OPS policies, standards and operating procedures as they apply to the use of government I&IT resources;

- The procedures for determining the sensitivity classification and safe handling of all information, as established in the *Information Security and Privacy Classification Policy* and *Operating Procedures*;

- The procedures for promptly reporting any suspected security compromises of computerized devices, applications, services or sensitive information.

To satisfy this requirement, the following e-learning courses have been developed: *Information Security – It's Everyone's Responsibility!* and *Information Security and Privacy Classification*, both geared at all staff. Management training includes *Module 1: Acceptable Use of Information and Information Technology Resources* and *Module 2: Disposal, Loss and Incident Reporting of Computerized Devices*. All courses can be accessed by logging into MyOPS, and following the links for Learning and Development.

6.2. Unacceptable Use of I&IT Resources

Government of Ontario Information Technology (IT) resources are to be used exclusively for government business, unless otherwise approved by your manager. In addition, government business must only be conducted on government resources, unless otherwise explicitly approved by your manager. This includes, but is not limited to computers, laptops, email, internet, intranet, extranet, personal digital assistants, cellular phones, memory sticks, etc.

- IT resources **must not** be used for activity which is prohibited by federal and provincial statutes, or the common law, and may result in criminal or civil liability.

- IT resources **must not** be used for unacceptable activity. Unacceptable activity includes, but is not limited to:

    - The use of government I&IT resources for personal use, without a manager's approval.
    - Using personal IT resources (including, but not limited to, personal home

computers and laptops, personal email accounts, cell phones, etc.) to conduct government business, unless approved by a manager.
- Accessing, displaying, downloading, creating, distributing or storing 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 (as per the *Workplace Discrimination and Harassment Prevention (WDHP) policy*).
- Using Internet sites for sharing files such as music files, video clips, digital image files or software programs, unless for government business and approved by your manager. Approved files must not violate copyright laws.
- Streaming audio or video from the Internet, unless for government business purposes.
- Using government resources to play games.
- Operating a private business or using these resources for personal gain or political activity, as specified in the *Public Service of Ontario Act* and related regulations.
- Misrepresenting the Government of Ontario's views on a matter.
- Discrediting others in the government through electronic communications.
- Sending anonymous messages or impersonating others.
- Sending chain letters or "spam" (broadly distributed, unsolicited emails).
- Using offensive, threatening, abusive language in electronic communications.
- Using IT resources to discriminate against or harass, threaten or intimidate other employees or to create a hostile or humiliating work environment.
- Performing unauthorized network scans on, or conducting unauthorized access attempts to government systems, applications or services, or spreading viruses or malicious codes to other systems.

The *Acceptable Use of I&IT Resources Guidelines*, which can be found at http://intra.security.gov.on.ca provide additional information for determining what constitutes unacceptable use of I&IT resources based on up-to-date threats and technologies.

6.3. Security of Government I&IT Resources

A variety of system and network security measures, such as anti-virus software, firewalls, Internet address screening programs and other security systems have been installed to assure the safety and security of the Government's electronic networks. Users **must not** attempt to disable, defeat, circumvent or otherwise tamper with any installed government security measures, or attempt to use or install their own security software or hardware.

Some Internet sites are blocked to OPS users. If you have a business requirement to access blocked sites, an exemption process is available. The "Request for Access" form can be found in Appendix B.

6.4. Monitoring

Systems 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 I&IT resources is identified, the result of the systems monitoring may be used in further investigation and may result in disciplinary actions.

Personal Monitoring
Personal monitoring of a particular individual's usage will take place if there is reasonable belief that I&IT 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 Chief Administrative Officer (CAO) or equivalent prior to monitoring and evidence gathering.

6.5. 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. Each password owner is responsible for any access to Ontario government systems gained through the use of their password. Detailed rules for password management and use can be found in the *GO-ITS 25.15 Security Standard: Security Requirements for Password Management and Use* which is posted on the Office of the Corporate Chief Technology Officer (OCCTO) website at http://www.mgs.gov.on.ca/stdprodconsume/groups/content/@mgs/@goits/documents/resourcelist/173720.pdf.

- Passwords MUST:
  - be chosen so that they are easy enough to remember but not easily guessed by someone else;
  - contain at least 8 characters;
  - contain at least one digit and at least one capital letter.
- Passwords must NOT:
  - include easily identifiable personal information about the owner (for example, names of family members, pets, birthdays, anniversaries or hobbies);
  - be any words, phrases or acronyms that are part of the broadly recognized Ontario Public Service culture;
  - be the same as all or part of a user's login id, actual last or given names, or a commonly known nickname;

- be shared with anyone (including system administrators and management).

- Users who suspect their password has been breached must change it immediately and report the incident to their manager or the IT Service Desk.

6.6. Information Security and Privacy Classification

All information must be classified and safeguarded according to its sensitivity classification level. The *Information Security & Privacy Classification Policy and Operating Procedures* provide guidance for classifying and safeguarding information, which can be found here: OPS Directives & Policies.

6.7. Virus Protection

- Ministry 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 IT Service Desk.

6.8. Remote Access, Mobile Devices & Wireless Communication

Computerized devices used for remote access to the integrated network are a de facto extension of that network, and as such, are subject to the same policies and standards as computerized devices physically located in government offices. Only government-issued computing devices should be used for remote access to the Government of Ontario network.

Remote Access

All Remote Access Service users are responsible for:

- Complying with government policies and procedures when using government equipment and services off-site;
- Adhering to the *GO-ITS 25.7 Standard: Security Requirements for Remote Access Services* (which can be found at http://www.mgs.gov.on.ca/stdprodconsume/groups/content/@mgs/@goits/documents/resourcelist/stdprod_102020.pdf) and the *GO-Security Token Policy* (which is found at http://intra.security.gov.on.ca) and related procedures;
- Ensuring security safeguards installed to protect their remote device are not disabled or tampered with;
- Ensuring that Government information and devices are protected from access by unauthorized individuals (e.g., friends, family members); and,
- Reporting any suspected security incidents to their program manager.

Mobile Devices

The same features (i.e., portability, processing power, access connectivity, input capability, data storage capacity) that make mobile devices so useful also make them a serious security risk that requires appropriate mitigation. The use of mobile devices must not jeopardize the security of more traditional government I&IT resources. Mobile device users must adhere to the *GO-ITS 25.10 Standard: Security Requirements for Mobile Devices* (which is found at http://www.mgs.gov.on.ca/stdprodconsume/groups/content/@mgs/@goits/documents/standard/stdprod_086169.pdf.

Wireless Communications

Wireless Local Area Networks (WLAN) provide a means to quickly network local computing devices and enable users to roam with their portable computing devices within a building or facility. However, without proper risk mitigation measures, data from WLANs can be captured easily by individuals within or outside the building and used to intercept confidential program information and/or gain unauthorized access to resources.

WLANS should not be used when high sensitivity program information or services are involved. All WLAN users are responsible for adhering to *GO-ITS 25.5 Security Standard: Security Requirements for Wireless Local Area Networks*, which can be found at http://www.mgs.gov.on.ca/stdprodconsume/groups/content/@mgs/@goits/documents/resourcelist/stdprod_102018.pdf.

6.9. Reporting Security Incidents

A security incident is any activity that could compromise the security of government information or systems. A security incident could be a social engineering attempt such as a request for a password, loss of a laptop or blackberry, a computer virus infection, degradation of a system, unauthorized changes to files or file sizes, or the unauthorized addition of files.

- All OPS system users are responsible for immediately reporting all security incidents (including lost or stolen information or IT assets) to their managers and to the IT Service Desk (at 1-888-677-4873, 416-246-7171 or OPSSD@ontario.ca). This also includes internal and external devices or parts.
- Managers must report security incidents to both the department heads and their Cluster Security Officers.
- If high sensitivity Cabinet information is disclosed without authorization, the ADM, ministry Communications Branch, Cluster Security Offices and Cabinet Office must be informed.
- All privacy breaches, or suspected privacy breaches, should be responded to in accordance with the recommended practices in *Taking the Right Steps – A Guide to Managing Privacy and Privacy Breaches*.
- Further information on reporting security incidents can be found in the *Operating*

Procedures for Disposal, Loss and Incident Reporting of Computerized Devices at http://intra.security.gov.on.ca.

6.10. Service Partners

Ministries must ensure that service partners (including other ministries, agencies, jurisdictions, the broader public sector and private sector organizations) who use government I&IT resources are made aware of and adhere to this policy. Appropriate use must be included in contracts and Service Level Agreements where applicable.

7. RESPONSIBILITIES

7.1. Users

All users are responsible for:

1. Complying with government legislation, directives, policies, operating procedures and standards when using I&IT resources.

2. Complying with ministry/cluster I&IT security procedures.

3. Using I&IT resources only as authorized by management.

4. Using government I&IT resources only for government business or approved purposes.

5. Reporting all I&IT security incidents to their Program Manager and the OPS IT Service Desk (at 1-888-677-4873, 416-246-7171 or OPSSD@ontario.ca).

7.2. Program Managers

Program managers are responsible for:

1. Ensuring their use of government I&IT resources is in compliance with government policies and standards.

2. Ensuring that users of government I&IT resources are aware of and adequately trained in their responsibilities as set out in this document and other related government policies.

3. Ensuring that users are individually accountable for using information systems and for following ministry or agency policies, standards, procedures, guidelines and best practices.

4. Reporting any I&IT security exposures or suspected breaches of computerized devices and sensitive information to the OPS IT Service Desk (at 1-888-677-4873, 416-246-7171 or OPSSD@ontario.ca).

5. Reviewing, authorizing and approving user access privileges.

6. Determining the sensitivity of information under their control, and ensuring that it is safeguarded according to its sensitivity classification level.

7. Ensuring that job descriptions reflect program accountability requirements for I&IT security.

7.3. Cluster Security Offices

Cluster Security Offices are responsible for:

1. Assisting program areas and ministries in safeguarding government I&IT resources.

2. Communicating the availability of tools to assist ministries and agencies in the implementation of appropriate safeguards to mitigate security risks.

3. Participating in efforts to prevent, detect and respond to security threats utilizing incident reporting and management for containment, notification and corrective action.

4. Developing operational procedures, guidelines and best practices that specifically address any ministry or cluster-specific technology.

5. Assisting in the development and delivery of security awareness, education and training programs.

6. Monitoring the implementation and effectiveness of security measures in the cluster.

7. Reporting of incidents, exposures and the state of security in the cluster to the senior executive accountable for Information and Information Technology Security and to Corporate Security Branch.

7.4. Corporate Security Branch

The Corporate Security Branch, Office of the Corporate Chief Information Officer is responsible for:

1. Developing and maintaining corporate security policies and standards for the OPS.

2. Providing tools to assist ministries, clusters and ITS in the implementation of appropriate safeguards to mitigate security risks.

3. Developing and delivering general, management and professional IT security training.

4. Coordinating efforts to prevent, detect and respond to security threats and vulnerabilities utilizing incident reporting and management for containment, notification and corrective action.

5. Providing 24/7 monitoring of the Internet, Intranets and Extranets connected to the OPS network.

6. Identifying unusual system or user behaviours.

7. Identifying the location and/or identity of a system and/or end user.

8. Identifying and preventing the spread of viruses, spyware or any form of malware that is or has the potential to compromise a government system and/or government network.

9. Conducting CAO authorized IT forensic investigations or individual monitoring.

7.5. Infrastructure Technology Services (ITS)

ITS is responsible for:

1. Reporting security incidents, breaches and/or exposures to the appropriate Program Manager(s), Cluster Security Officer and Corporate Security Branch.

2. Providing network custodial duties such as ensuring all security methods for the network are in place, operational and able to be monitored for unauthorized access attempts on a regular basis.

3. Ensuring that current and operational government approved malware prevention products are installed on servers, at each desktop and on all notebooks, and are set to perform scanning on a predefined schedule.

7.6. HROntario

The HROntario is responsible for:

1. Ensuring the development of human resources policy is aligned with I&IT security policies, procedures and best practices.

2. Participating in central bodies/committees to process cases involving unacceptable use to determine discipline and ensure fair and equitable treatment of those involved with inappropriate activities/use of I&IT resources.

3. Working with Legal Services to develop guidelines for applying discipline in cases of unacceptable use.

7.7. Legal Services Branch

The Legal Services Branch is responsible for:

1. Providing legal advice/guidance as required when unacceptable/illegal use of I&IT resources is discovered.

7.8. Ontario Internal Audit

The Ontario Internal Audit is responsible for:

1. Conducting periodic audits of pertinent activities to test compliance with security policies and standards.

2. Communicating with appropriate management about risks identified and the severity of those risks.

3. Working with management to identify the needed management action plans to mitigate the risks noted during the course of an audit and conducting follow-up as required.

7.9. Chief Administrative Officers for Ministries and Agencies

Chief Administrative Officers are responsible for:

1. Authorizing investigations into suspected unacceptable usage of information technology resources involving user actions.

8. APPENDICES

8.1. Appendix A: Terms and Definitions

Term	Description
Access	Gaining entry to an electronic network or information system provided by the government to its employees and other authorized individuals on or outside government premises including telework situations and where employees or authorized individuals are using these electronic networks on their own time for personal use.
Electronic / System Monitoring	Any activity that involves the surveillance of an electronic network as it is being used or the recording and analysis of activity on an electronic network at any time. This may include monitoring of user accounts, activities, sites visited, information downloaded and computer resources used.
Extranet	An access privileged, contractual domain, using Internet technology, between two or more parties, one being an OPS ministry or agency.
Information	Knowledge communicated or received. Information in all forms (such as text, image, video and voice), in all media (such as paper, magnetic tape, disks, microfilm/microfiche) and at all stages of lifecycle (i.e., created, entered, processed, communicated, transported, disseminated, stored or disposed of) including the description of the information contents, origins, structure and relationships enabling correct interpretation of information. Forms and media for information include current and future technologies.
Information System	A combination of people, information technology hardware, software, information technology facilities, services and automated or non-automated processes that have been organized to accomplish ministry or I&IT Cluster objectives.
Information Technology Resources	Those resources (hardware, software, information, etc.) used to create, enter, process, communicate, transport, disseminate, store or dispose of information in the form of data, text, image and voice including: • Administrative policies, processes and procedures (including records retention schedules); • Information technology equipment, software, facilities and services (such as cell phones, pagers, personal digital assistants, desktop and mobile computers, servers, operating systems, application systems, utility programs, data centres, electronic networks, systems development services, disaster recovery services); • Information services (such as printing services, information and service counters, courier services, disposal services, micro-records services, storage services, fulfillment services including stock management, printing and distribution of information assets); and, • Physical assets (such as buildings, offices, filing cabinets).

Internet	The World Wide Web (www) collection of networks linked through common communications protocols.
Intranet	Internal access controlled ministry or agency network. Users are authorized to have OPS network access.
Malware (malicious software)	Software designed to infiltrate or damage a computer system without the owner's informed consent. This may include but is not limited to computer viruses, worms, rootkits, Trojan horses, key loggers, denial of service attacks, botnets, spyware and other programs that gather information about a computer system and/or user.
Network	A network is a collection of computers connected to each other. The network allows computers to communicate with each other and share resources and information.
Security Incident	Any activity that could compromise the security of government information or systems. A security incident could be a social engineering attempt such as a request for a password, loss of a laptop or blackberry, a computer virus infection, degradation of a system, unauthorized changes to files or file sizes, or the addition of files.
Security Standards	The GO ITS 25 technical Security Standards are corporate information and information technology security standards that have been approved by the Information Technology Executive Leadership Committee (ITELC), Architecture Review Board (ARB) and the Information Technology Standards Council (ITSC). The security standards cover operational principles, requirements and best practices for the protection of Ontario government electronic networks and networked computer systems. GO ITS 25 are issued by Corporate Security Branch, Office of the Corporate Chief Information Officer and are available on the intranet at http://www.mgs.gov.on.ca/en/IAndIT/STEL02_047303.html
Sensitive Information	Information defined as sensitive in accordance with the Information Security & Privacy Classification (ISPC) Policy i.e. information that must be access controlled, and, if disclosed without authorization, may cause harm and injury.
Unauthorized	Permission has not been granted to access resources according to a predefined approval scheme.
User	All government and agency employees, temporary staff, students, consultants, service providers and anyone else that is granted access to government information, systems and other IT resources.

8.2. Appendix B: Request for Access Form

Ontario

OPS WEB FILTERING EXEMPTION

This exemption will provide a user with additional access to the Internet, as may be required by their job function.

Add: Change: Delete:

Employee Name: _____
Network login name: _____
AD logon domain: _____
E-mail Address: _____
Cluster/Ministry: _____
Telephone Number: _____

Justification for Exemption:

Provide a brief business case to outline why unrestricted web access is required for you to complete your job duties.

_____

_____

_____

_____

Please note that this exemption provides you with additional Internet access. However, this access should only be used for the purpose indicated in the preceding business case. If access to additional Web sites is required during the year, then your original form must be revised, resigned, and processed through S. Order Desk Online.

I have read and understood the requirements as outlined in the *Acceptable Use of I&IT Resources Policy*.

Applicant's signature: _____

APPROVALS:

The applicant's manager must approve this form.

Manager's Approval:

_____	_____	_____
Printed Name	Signature	Title
_____	_____	
Telephone Number	Date	

The form must then be forwarded to the applicant's ADM, Commissioner, or Delegate (no lower than Level II as described in the Delegations of Authority) for authorization.

Authorization:

_____	_____	_____
Printed Name	Signature	Title
_____	_____	
Telephone Number	Date	

Once authorized, the completed form needs to be processed through S. Order Desk Online.

If you require assistance, please contact the OPS IT Service Desk:
Please direct all e-mail requests to: opssd@ontario.ca
Please direct all phone inquiries to: 1-888-677-4873 or 416-246-7171 (GTA)
TTY: 1-877-TTY-ITSD (877-889-4873)

Corporate Security Acceptable Use of I&IT Resources Policy	
Identification Name:	Acceptable Use of I&IT Resources Policy
Contact Officer:	Sylvia Nikodem Security Policy Adviser, Corporate Security Sylvia.Nikodem@ontario.ca
Contact Manager:	Charlotte Ward Manager, Security Policy & Administration Charlotte.Ward@ontario.ca
Effective Date:	March 23, 2011
Date last Amended:	March, 2011
Date of Next Review:	March, 2013
Supporting Documents:	Corporate Policy on Information and Information Technology (I&IT) Security Workplace Discrimination and Harassment Prevention Policy Information Security and Privacy Classification Operating Procedures Operating Procedures for Disposal, Loss and Incident Reporting of Computerized Devices Government of Ontario Information Technology Security Standards (GO-ITS) Taking the Right Steps – A Guide to Managing Privacy and Privacy Breaches