Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Policy on Acceptable Network and Device Use

Published: Mar 06, 2014

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT22-144/2014E-PDF
ISBN: 978-0-660-09512-7

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Politique sur l'utilisation acceptable des dispositifs et des réseaux

Policy on Acceptable Network and Device Use

1. Effective Date

1.1 This policy takes effect on October 1, 2013.

1.2 It replaces the *Policy on the Use of Electronic Networks* of February 12, 1998.

1.3 All policy requirements will be effective October 1, 2013, with the exception of 6.1.3. which will come into effect April 1, 2014.

2. Application

2.1 This policy applies to "departments" as defined in section 2 of the *Financial Administration Act* (FAA), with the exception of paragraphs (b) and (c), and unless otherwise excluded by specific acts, regulations or orders-in-council. However, the requirements of Sections 6.1.1, 6.1.2 and 6.1.4 below only apply to the core public administration as defined in section 11.1 of the FAA, unless otherwise excluded by specific acts, regulations or orders-in-council. Other departments or separate agencies not subject to these provisions are encouraged to meet these requirements as good practice.

2.2 Sections 7.1b, 7.2 and 8.2 relating to the role of the Treasury Board of Canada Secretariat (TBS) in monitoring compliance and directing consequences for non-compliance do not apply with respect to the Office of the Auditor General, the Office of the Privacy Commissioner, the Office of the Information Commissioner, the Office of the Chief Electoral Officer, the Office of the Commissioner of Lobbying, the Office of the Commissioner of Official Languages and the Office of the Public Sector Integrity Commissioner. The deputy heads of these departments are solely responsible for monitoring and ensuring compliance with the policy within their departments, as well as for responding to cases of non-compliance in accordance with any Treasury Board instruments that provide principles and guidance on the management of compliance.

3. Context

3.1 The Government of Canada recognizes that open access to Government of Canada electronic networks and devices, including the Internet, is essential to transforming the way public servants work and serve Canadians. Open access to the Internet including Government of Canada and external Web 2.0 tools and services will enhance productivity, communication and collaboration, and encourage the sharing of knowledge and expertise to support innovation.

3.2 This policy applies to the use of Government of Canada electronic networks for conducting government business and professional and limited personal use, regardless of location of access or device used.

3.3 This policy is issued by the Treasury Board under the authority of sections 7 and 11.1 of the FAA.

3.4 The Treasury Board has delegated to the Secretary of the Treasury Board the authority to issue, amend, and rescind directives and standards to support this policy.

3.5 This policy is to be read in conjunction with the *Foundation Framework for Treasury Board Policies*, the *Policy on Government Security*, the *Operational Security Standard: Management of Information Technology Security (MITS)*, *Values and Ethics Code for the Public Sector*, *Policy on Conflict of Interest and Post-Employment*, and the *Directive on Privacy Practices*.

4. Definitions

4.1 For definitions of terms used in this directive, refer to Appendix A – Definitions.

5. Policy Statement

5.1 Objective

The objective of this policy is to ensure acceptable and efficient use of Government of Canada electronic networks and devices to support enhanced communication and collaboration thereby improving productivity, and program and service delivery to individuals and businesses.

5.2 Expected results

The expected results of this policy are the following:

- Authorized individuals use Government of Canada electronic networks and devices in an acceptable manner; and
- Authorized individuals have open access to the Internet including Government of Canada and external Web 2.0 tools and services, in accordance with the Policy on Government Security.

6. Policy Requirements

6.1 Deputy heads are responsible for ensuring that:

6.1.1 Effective management and monitoring practices for the acceptable use of Government of Canada electronic networks and devices are implemented.

6.1.2 Authorized individuals are informed of the following:

a. Expectations for acceptable use of Government of Canada electronic networks and devices per Appendices B and C;
b. Electronic network monitoring practices being applied by their own department and/or Shared Services Canada (SSC) per Appendix D; and
c. Consequences for unacceptable use of such networks and devices.

6.1.3 Authorized individuals have open access to the Internet including Government of Canada and external Web 2.0 tools and services that enhance productivity, communication and collaboration, in accordance with the *Policy on Government Security* and Appendix E.

6.1.4 Learning opportunities regarding the acceptable use of Government of Canada electronic networks and devices and Government of Canada and external Web 2.0 tools and services are provided to authorized individuals.

6.2 For departments that receive their network services from SSC, the Deputy Head of SSC is responsible for managing tools to support monitoring and providing reports monthly, and as required, about the use of Government of Canada electronic networks and devices to assist deputy heads in the identification, investigation and implementation of corrective action on issues that arise regarding unacceptable use.

7. Monitoring and Reporting Requirements

7.1 Deputy heads are responsible for:

a. Monitoring compliance with this policy within their department and taking corrective action as needed; and
b. Providing an annual confirmation of the compliance with this policy as requested by the Chief Information Officer of the Government of Canada or TBS.

7.2 TBS is responsible for:

a. Oversight and monitoring of the compliance with this policy by deputy heads through an annual confirmation that policy requirements are being met, leveraging existing reporting mechanisms where applicable;
b. Recommending that corrective action be taken when a department has not complied with the requirements of this policy; and
c. Establishing a framework for the review of this policy and ensuring that a review is initiated within five years of the effective date of this policy.

8. Consequences

8.1 The deputy head is responsible for investigating and acting when issues arise regarding policy compliance. The deputy head is also responsible for ensuring that appropriate remedial actions are taken to address these issues within the department.

8.2 If TBS determines that a department may not have complied with any of the requirements of this policy, the Secretary of the Treasury Board in consultation with the Chief Information Officer of the Government of Canada may request that the deputy head:

a. Conduct a review or an audit to assess whether requirements of this policy have been met. The cost of such an audit or review will be paid from the department's reference level; and
b. Take corrective actions, in keeping with the *Framework for the Management of Compliance*, and report back on the results achieved.

8.3 Consequences of non-compliance with this policy, or failure to take corrective actions requested by the Chief Information Officer of the Government of Canada, may include recommending to the Treasury Board the following:

a. Limits on the spending authority of the department; and
b. Imposition of any other measures determined appropriate in the circumstances.

9. Roles and Responsibilities of Government Departments

This section identifies other significant departments that have a role in this policy domain. In and of itself, it does not confer an authority.

9.1 The Chief Information Officer Branch of TBS is responsible for providing policy advice and guidance as well as communicating with, and engaging departments on the plans, progress, risks and challenges associated with implementing this policy and related instruments.

10. References

Charter

- *Canadian Charter of Rights and Freedoms*

Legislation and regulations relevant to this policy

- *Access to Information Act* and *Access to Information Regulations*
- *Canada Labour Code*
- *Criminal Code*
- *Financial Administration Act*
- *Privacy Act* and *Privacy Regulations*
- *Public Service Labour Relations Act*
- *Public Servants Disclosure Protection Act*
- *Public Service Employment Act*
- *Security of Information Act*

Related policies and publications

- *Communications Policy of the Government of Canada*
- Departmental Codes of Conduct
- *Policy on Access to Information*
- *Policy on Conflict of Interest and Post-Employment*
- *Policy on Government Security*
- *Policy on Information Management*
- *Policy on Legal Assistance and Indemnification*
- *Policy on Management of Information Technology*
- *Policy on the Management of Materiel*
- *Policy on Privacy Protection*

Directives

- *Directive on Departmental Security Management*
- *Directive on Privacy Impact Assessment*
- *Directive on Privacy Practices*

Standard

- *Operational Security Standard: Management of Information Technology Security (MITS)*

Guidelines

- *Guideline on Acceptable Network and Device Use*
- *Guideline to Acceptable Use of Internal Wikis and Blogs Within the Government of Canada*
- *Guidelines for Discipline*
- *Guideline on the Official Use of Social Media*

11. Enquiries

For questions on this policy instrument, please see the Secretariat's Treasury Board Secretariat website.

Appendix A: Definitions

acceptable use — permitted use of Government of Canada electronic networks and devices by authorized individuals

- To perform activities as a part of their official duties;
- For career development and other professional activities; and
- For limited personal use that is conducted on personal time; that is not for financial gain; that does not incur any additional costs for the department; and that does not interfere with the conduct of business.

All use of Government of Canada electronic networks and devices must be in compliance with the *Values and Ethics Code for the Public Sector* and all other related Treasury Board policies and departmental codes of conduct and policies. Use of Government of Canada electronic networks and devices must not give rise to a real, potential or apparent conflict of interest or in any way undermine the integrity of the department. (Also see Appendix B)

access

Gaining entry to an electronic network that the federal government has provided to Government of Canada authorized individuals. Access to such electronic networks may be from inside or outside government premises. Access may support

telework and remote access situations, or situations where authorized individuals are using electronic networks provided by the federal government on their own time for limited personal use.

authorized individuals

Individuals working with the Government of Canada, including employees of the federal government as well as casuals, contractors, students and other persons who have been authorized by the deputy head to access Government of Canada electronic networks and devices.

electronic network

Groups of computers and computer systems that can communicate with each other, including without limitation, the Internet, Government of Canada electronic data networks, voice and video network infrastructure, and public and private networks external to a department. The network includes both wired and wireless components.

external networks

Networks reached from the Government of Canada network, to which authorized individuals are granted access. They include permissible sites across the public Internet and via the World Wide Web, including services provided by parties such as collaborative software.

Internet

A global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve users worldwide.

learning opportunities

Diverse learning methods or tools, formal or informal, to generate awareness or acquire knowledge about the acceptable use of Government of Canada electronic networks and devices and Government of Canada and external Web 2.0 tools and services. These approaches can include, but are not limited to, information or orientation sessions, YouTube video, information provided on departmental intranet sites, manager debriefs, account sign-on notifications and electronic newsletters.

monitoring practices

Use of a software system that monitors an electronic network for slow or failing components, and notifies the network administrator in cases of outages, and that can monitor the network activity of specific individuals for which there is suspicion of unacceptable network usage. Recording and analysis of the use of electronic networks are used for operational purposes and for assessing compliance with government policy.

open access

Refers to the provision of Internet access, in accordance with the *Policy on Government Security*, to authorized individuals via Government of Canada electronic networks and devices that, from the perspective of firewall settings, is substantively equivalent irrespective of department or access medium. Internet sites that enhance productivity, communication and collaboration are not blocked with the exception of those that present a legitimate IT security threat and where content substantively falls into the category of unacceptable use.

unacceptable use

Any activity that violates Treasury Board or departmental policy instruments or other published requirements, including, but not limited to, activity or behavior that:

- May give rise to criminal offences;
- Violates federal and provincial statutes;
- Impacts negatively on the performance of Government of Canada electronic networks and devices;
- Impedes departmental operations or the delivery of services;
- Breaches the Duty of Loyalty requirement for public servants (i.e., does not refrain from public criticism of the Government of Canada); and
- Could be deemed to reasonably result in civil lawsuits. (Also see Appendix C)

user devices

Physical devices found or brought into the work environment that are used by authorized individuals to access Government of Canada electronic networks and databases. The physical devices can include, but are not limited to, the following: desktop workstations, laptops, notebooks, tablets, smartphones, cellphones, peripherals such as printers and scanners, memory devices such as USB flash drives, CD drives and DVD drives, webcams and any other computer hardware used to obtain, store or send information.

Web 2.0

Includes Internet-based tools and services that allow for participatory multi-way information sharing, dialogue, syndication, and user-generated content. This can include social media and collaborative technologies.

Appendix B: Examples of Acceptable Use (non-exhaustive list)

Open access to the Internet, including Government of Canada and external Web 2.0 tools and services, can assist authorized individuals to conduct the business of government more efficiently and effectively. The acceptable use of Government of Canada electronic networks, devices and internal and external Web 2.0 tools and services will support the transformation of how public servants perform their work duties, enhance collaboration and networking with their peers, augment professional development opportunities and enable limited and reasonable personal use during work hours.

As well, informing users of expected behaviours when using networks, devices and Government of Canada and external Web 2.0 tools and services will help them to protect against potential confidentiality or privacy breaches and to comply with the *Policy on Government Security*, the *Communication Policy of the Government of Canada*, the *Values and Ethics Code for the Public Sector*, and other related Treasury Board policies and departmental codes of conduct and policies.

The following are non-exhaustive lists of examples of acceptable use of internal and external Web 2.0 tools and services that could be conducted via Government of Canada electronic networks and devices.

Work-related and Professional Development Activities

- Conduct consultations within the federal government via internal wikis and forums to support the development of policies and programs;
- Share knowledge and information intra- or inter-departmentally to support planning and decision-making or facilitate project collaboration;
- Perform research through accessing online reports, presentations, and data-sets;
- Watch online broadcasts of work-related content, such as a parliamentary committee meeting via ParlVU;
- Remain up-to-date with official announcements published on social media platforms by federal departments and agencies, provincial or municipal governments, or international jurisdictions or organizations;
- Document corporate knowledge on Government of Canada wikis to facilitate employee orientation and knowledge transfer;
- Participate in a video or audio conference with colleagues or clients from other organizations or jurisdictions through tools such as Skype or Google Hangouts;
- Develop and share code repositories in collaboration with departments, other jurisdictions and private sector organizations via code sharing tools such as GitHub;
- Leverage expertise from across government by creating or participating in online communities of interest on topics of shared professional interest such as #w2p (Web 2.0 Practitioners community);
- Access or share unclassified information through cloud-based tools such as SlideShare;
- Collaborate on joint initiatives and projects, via open discussions or closed groups as appropriate, with other departments and levels of government through the use of wikis, professional networking applications, internal tools such as GCDocs or external cloud-based tools such as Google Docs;
- Maintain an up-to-date profile on professional networking sites such as LinkedIn;
- Follow thought leaders and government officials on blogs or micro-blogs such as Twitter;
- Tweet, re-tweet or share links to professional activities and events, or interesting and relevant articles;
- Read, contribute to, or edit articles in work-related wikis, online forums or discussion groups;
- Discuss professional issues or participate in professional associations via online forums or social networking sites;
- Participate in online professional training activities (e.g. webcasts, online learning products via CSPS, podcasts);
- Find a colleague or client's contact information or directions to a meeting;
- Make arrangements for work-related travel, including booking tickets and searching for information about accommodations via Government of Canada or third-party travel review services; and
- Complete an online job application or participate in an online interview.

Note: Public opinion research conducted through Web 2.0 tools must also comply with the Procedures for Planning and Contracting Public Opinion Research

Note: Open access in departments will occur incrementally as departmental bandwidth restrictions are resolved.

Limited Personal Use

Examples of limited personal use that is conducted on personal time, that is not for financial gain, that does not incur any additional costs for the department, and that does not interfere with the conduct of business include:

- Search for information online;
- Keep up-to-date with news and current events;
- Subscribe to Web feeds (such as RSS) ;
- Get directions for a trip or search for addresses and contact information;
- Make personal travel arrangements;
- Post or read ratings/reviews of products or services or make online purchases;
- Check the weather forecast;
- Confirm bus schedule information;
- Pay bills or conduct personal banking online;
- Read or contribute to online forums, blogs, discussion groups, or wikis on topics of personal interest;
- Update a personal blog, micro-blog, social networking page, or Web page that is for non-commercial purposes or does not otherwise constitute Unacceptable Use as per Appendix C; and
- Visit social networking sites to connect with family and friends.

Appendix C: Unacceptable Use (non-exhaustive list of examples)

The legal consequences of unacceptable use will be determined by the section of the law in default. The employment consequences of unacceptable use will be determined by existing policy instruments and guidance from appropriate organizational human resources or labour relations advisors. Departments can limit the use of Government of Canada electronic networks and devices or impose employment consequences if the activity or behaviour:

- Is unacceptable or criminal in nature;
- Violates Treasury Board or organizational policies and codes of conduct and other published requirements;
- Impacts negatively the performance of Government of Canada electronic networks and devices;
- Impedes organizational operations or the delivery of services; or
- Breaches the Duty of Loyalty requirement for public servants (i.e., does not refrain from public criticism of the Government of Canada).

Criminal offences

The following is a non-exhaustive list of examples of criminal activity that could take place on Government of Canada electronic networks or devices:

- Child pornography—Possessing, downloading or distributing any child pornography.
- Copyright infringement—knowingly distributing infringing copies of a copyrighted work.
- Defamation—Causing a statement to be read by others that is likely to injure the reputation of any person by exposing that person to hatred, contempt or ridicule, or that is designed to insult the person.
- Denying right of access under the *Access to Information Act*: destroying, mutilating, altering, falsifying or concealing a record, or making a false record with intent to deny a right of access under the Access to Information Act.
- Hacking and other crimes related to computer security.
- Gaining unauthorized access to a computer system—Using someone else's password or encryption keys to engage in fraud or obtaining money, goods or services through false representations made on a computer system.
- Trying to defeat the security features of the electronic networks.
- Spreading viruses with intent to cause harm.
- Destroying, altering or encrypting data without authorization and with the intent of making the data inaccessible to others who have a lawful need of access.
- Interfering with others' lawful use of data and computers.
- Harassment—Sending electronic messages that cause people to fear for their safety or the safety of anyone known to them.
- Hate propaganda—Disseminating messages that promote hatred or incite violence against identifiable groups in statements outside of private conversations.
- Interception of private communications or electronic mail (in transit)—Unlawfully intercepting someone's private communications or unlawfully intercepting someone's electronic mail.
- Obscenity—Distributing, publishing or possessing for the purpose of distributing or publicly displaying any obscene material.
- Various other offences—The Criminal Code (and a few other statutes) provide for a range of other offences that can take place in whole or in part using electronic networks. For example, fraud, extortion, blackmail, bribery, illegal gambling, and dealing in illegal drugs can all occur, at least in part, over electronic networks and are criminal acts.

Violations of federal and provincial statutes

The following is a non-exhaustive list of examples of illegal (though not criminal) activity that could take place while accessing the Internet through Government of Canada electronic networks or devices:

- Disclosing sensitive information without authorization.
- Disclosing personal information—Failing to respect the privacy and dignity of every person.
- Disclosing business trade secrets—Revealing business trade secrets without authorization, other than in response to a formal request under the Access to Information Act.
- Disclosing sensitive government information—Revealing sensitive government information without authorization.
- Intellectual property infringement: infringing or otherwise using without authorization another person’s intellectual property (copyright, trade-mark or patent).
- Harassment—It is a discriminatory practice to harass an individual on a prohibited ground of discrimination. The prohibited grounds are race, national or ethnic origin, colour, religion, age, sexual orientation, marital status, family status, disability and conviction for which a pardon has been granted.
- Privacy breaches—Include, but is not limited to, any of the following without authorization: reading someone else's electronic mail or other personal information, listening in on someone's private conversations or intercepting electronic mail while it is in transit, for example.

Violation of organizational and/or Treasury Board policies and publications

The following is a non-exhaustive list of examples of activities that contravene Treasury Board policies (and may contravene comparable organizational policies):

- Causing congestion and disruption of Government of Canada electronic networks and systems through such means as sending chain letters and receiving list server electronic mail unrelated to a work purpose. These are examples of excessive use of resources for non-work related purposes (*Policy on Government Security*).
- Using the Government of Canada electronic networks for unauthorized activities as laid out in this policy and related guidance

(*Policy on Conflict of Interest and Post-Employment*).
- Using Government of Canada electronic networks to make public comments about government policies, except when acting as the official spokesperson, or to engage in political activity that could impair his or her ability to perform duties in an impartial manner (*Public Service Employment Act*, *Values and Ethics Code for the Public Sector*, and *Policy on Conflict of Interest and Post-Employment*
- Representing personal opinions as those of the organization, or otherwise failing to comply with organizational procedures concerning public statements about the government's positions (*Policy on Conflict of Interest and Post-Employment*
- Providing authorized individuals with access to systems, networks or applications used to process sensitive information before such personnel are properly security screened (*Policy on Government Security*).
- Failing to revoke system access rights of personnel when they leave the organization due to the end of employment or the termination of a contract, or when they lose their reliability status or security clearance (*Policy on Government Security*).
- Unauthorized removal or installation of hardware or software on government owned informatics devices or electronic networks (*Policy on Government Security*).
- Furthermore, unless for valid work-related purposes, authorized individuals cannot use Government of Canada electronic networks or devices to access or download websites or files, or send or receive electronic mail messages or other types of communication, that fall into the following categories:
    - Documents that incite hatred against identifiable groups contained in personal messages (the Criminal Code prohibits incitement of hatred against identifiable groups in public conversations, also listed under criminal offences);
    - Documents whose main focus is pornography, nudity and sexual acts.

Activity that can expose authorized individuals or the employer to tort liability

Various kinds of conduct can expose a person or an employer to civil liability. The employer's liability will be triggered when a public service employee or authorized individual performs the activity. The following is a non-exhaustive list of examples of torts from which liability may stem from activity on Government of Canada electronic networks or devices:

- Disclosing or collecting sensitive data—Revealing or obtaining such information without authorization. In addition to the statutory provisions mentioned above, an unauthorized disclosure or collection of personal information can result, in some circumstances, in a civil action for invasion of privacy, nuisance or trespass under common law, and similar actions under the Civil Code of Québec (articles 3, 15–41), for breach of contract and for breach of trust or breach of confidence (e.g., if confidential commercial information is disclosed).
- Defamation—Spreading false allegations or rumours that would harm a person's reputation. In addition to criminal libel, publishing defamatory statements without a lawful defence can result in a civil action.
- Inaccurate information—Posting inaccurate information, whether negligently or intentionally. This can lead to civil lawsuits for negligent misrepresentation.

Note: The above is a non-exhaustive list of unacceptable use. Other activities could be deemed unacceptable at the discretion of the deputy head.

Appendix D: Privacy

Privacy Notices

Authorized individuals must be informed of departmental monitoring practices via a privacy notice, prior to their implementation, by communicating at a minimum, the following information:

- A statement explaining the regular monitoring practices of electronic networks—for example, operational analysis of logs indicating the Internet sites employees and other authorized individuals have visited, the files downloaded or uploaded, or the key-word searches of files on network servers or on computer storage devices of Government of Canada employees or other authorized individuals' computers;
- A statement that electronic networks will be monitored for work-related purposes—for example, to assess system or network performance, protect government resources or ensure compliance with government policies; and
- A statement that special monitoring may be permitted without notice in instances where illegal or other unacceptable use is suspected.

Departments are directed to contact their Access to Information and Privacy office for more details on policy requirements with respect to privacy.

Departmental Considerations for Privacy

1. While the organization is required by law to protect personal information gathered with appropriate authority for business purposes, information and technology assets are assigned to individuals for authorized use only. If users choose to store their own personal information on the network or any other equipment, it is at their own risk.
2. Whenever individuals involved in an investigation are obliged to read the content of electronic communications, they must keep the information confidential and use it only for authorized purposes. The investigation must be conducted in accordance with the *Canadian Charter of Rights and Freedoms*, the *Criminal Code* and, for those institutions for which it applies, the *Privacy Act*.
3. Under the *Access to Information Act* and the *Privacy Act*, the public may request access to the Government of Canada's information or electronic records, as well as their own personal information, subject to applicable exemptions under those Acts. These records include electronic mail that Government of Canada employees or other authorized individuals have sent or

received that is stored on government computers and records showing which websites Government of Canada employees or other authorized individuals have visited.

Appendix E: Departmental Considerations for Security (non-exhaustive list of examples)

The Government of Canada recognizes that cyber threats are increasing with the global reach of the Internet and the growing interconnections of government and non-government networks worldwide.

As departments open access to their electronic networks and devices, hackers and cybercriminals have more opportunities to gain unauthorized access to sensitive government information through Government of Canada networks and systems. As a result, Government of Canada departments must be ever more vigilant in today's dynamic threat environment as malicious code can be hidden in known or trusted web sites, tools and services.

Departments remain responsible for ensuring that they comply with the requirements established in Government of Canada security policy instruments (e.g., *Policy on Government Security*, *Directive on Departmental Security Management*, the *Operational Security Standard: Management of Information Technology Security (MITS)*, *Information Technology Security Guidance-33*, and *Communications Security Establishment Canada Top 35 Mitigation Measures*).

Departments are to ensure that, based on an analysis of departmental security needs, security measures from the following non-exhaustive list are selected, properly implemented and layered in a manner that will provide defence-in-depth and will help to protect Government of Canada electronic networks, devices and information:

- Use currently supported versions of operating systems and applications (and ensure that they remain patched and up-to-date) to reduce vulnerabilities in software that can be remotely exploited;
- Disable unnecessary features in operating systems, applications and web browsers to reduce attack surface;
- Disable auto-run functionality on endpoints to prevent accidental code execution;
- Enable data execution prevention in operating systems and applications to reduce the risk of memory overflow execution by malicious code;
- Use antivirus software with up-to-date signatures and heuristic detection capabilities at the gateway and on endpoints to detect and prevent the execution of malicious code;
- Implement host-based intrusion detection/prevention (IDP) systems to improve the ability to detect and identify anomalous behaviours;
- Use whitelisting or blacklisting to prevent access to malicious websites, tools and web-based services from GC networks and devices;
- Implement centralized logging for computer events, with regular log analysis, to improve the ability to detect and identify anomalous behaviours and to assist with incident management and forensic analysis of compromised systems;
- Ensure that user accounts with administrative or root privileges are not used to search, browse or collaborate over the internet – these users should instead use normal user accounts with standard privileges; or a solution that will prevent the use of, or drop, administrator privileges;
- Use network segmentation, segregation and access controls to control how devices and systems that allow users to access Internet-based web-content are allowed to interact with other high-value systems and assets; and
- Ensure that security awareness programs include:
    - Material notifying users that they are not permitted to post or share sensitive GC information (i.e. classified, protected, proprietary or otherwise restricted-distribution material) on public web sites, tools and services;
    - Material discussing the threats and risks associated with Internet-based web-content as well as measures users can take to reduce risks;
    - Material describing the threats and risks associated with mobile device use as well as measures users can take to reduce risks; and
    - Regular reminders and updates to maintain awareness and to reflect the latest trends and threats.

Note: In the event of any discrepancy between the associated security requirements identified in this appendix and the security requirements identified in the *Policy on Government Security* and its supporting instruments, the *Policy on Government Security* is to be considered the authoritative source.