# DecorativeCOR310 Security Control Content

Version: March 2024

## Table of Contents

[Table of Contents 2](#_Toc157778387)

[Introduction 3](#_Toc157778388)

[Security Screening 5](#_Toc157778389)

[Business Continuity Management 8](#_Toc157778390)

[Security in Contracts and Other Arrangements 10](#_Toc157778391)

[Physical Security 12](#_Toc157778392)

[Information Technology Security 16](#_Toc157778393)

[Information Management Security 21](#_Toc157778394)

[Security Event Management 28](#_Toc157778395)

[Security Awareness and Training 30](#_Toc157778396)

## Introduction

“Do Your Part - Be Security Smart”

We all use information and assets as part of our daily work, and we are all responsible for protecting and managing them effectively, regardless of our workplace location. The [Policy on Government Security](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16578) (PGS) requires you to know your security responsibilities and the potential consequences of not fulfilling them. The PGS is made up of eight security controls that ensure programs, services, information, individuals and assets are safeguarded. These controls are:

 Security Screening

 Physical Security

 Information Technology Security

 Information Management Security

 Security in Contracts and Other Arrangements

 Security Event Management

Business Continuity Management

 Security Awareness and Training

As an individual employed with the Government of Canada, you have a role in helping to mitigate security risks within your department. Regardless of your work location, taking part in security awareness and training helps to ensure you have the necessary knowledge and skills to promote a secure workplace while performing your duties. Not knowing your responsibilities can put your department at risk of compromise, which in turn, can have potential consequences for you and the Government of Canada.

### Resources

* [Directive on Security Management](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611)
* [Policy on Government Security](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16578)

## Security Screening

The **purpose of security screening** is to ensure that those who have access to government information, assets and facilities are reliable, honest, trustworthy and, when applicable, loyal to Canada.

Valid security screening is a condition of employment in the federal government. You **cannot** be appointed to a position within the Government of Canada without the required security status or clearance.

A decision to deny or revoke a security screening level would mean that you no longer meet the conditions of employment, and your employment, contract or assignment could be terminated.

Upon employment with the federal government, you may have received a security briefing with your departmental security office. By signing the Security Screening Certificate and Briefing Form (SSCBF), you acknowledge that you have been granted a security screening level and that you formally agree to abide by the security requirements, including the policies and safeguards identified in the [Policy on Government Security](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16578) (PGS), and any other departmental or agency-specific security requirements that may apply in consideration of the department’s operating and risk environment.

### Aftercare

Aftercare practices are aimed at providing confidence in an individual’s continued reliability and, when applicable, loyalty to Canada. These practices are essential to helping build and maintain a culture of security, where individuals understand and implement security policies and practices to safeguard information, assets and facilities to help ensure that security is not compromised, either negligently or unknowingly.

Aftercare comprises formal, planned security briefings, security awareness, updates and upgrades, the reporting of changes in personal circumstances, behaviours and unusual contacts or incidents.

### Duty to report

Your behaviour, both at work and in your personal life, may impact the security screening outcome. It is extremely important to notify your departmental security office of any change in personal circumstances, such as marital status, name change, financial situation, criminal activity, change in residential address or living situation, etc.

### Updating security levels

An update focuses on determining whether changes in personal circumstances pose a potential security risk in light of the duties you perform.

Your departmental security office will advise you when your security screening file needs to be updated. Security screening update cycles are every 5 or 10 years, depending on your security screening level or circumstances at the time.

The established update cycles do not preclude an update from being done more frequently for cause.

### Resources

* [*Canadian Security Intelligence Service Act*](https://laws-lois.justice.gc.ca/eng/acts/c-23/)
* [Conducting Security Interviews for Security Screening (COR303](https://catalogue.csps-efpc.gc.ca/product?catalog=COR303&cm_locale=en))
* [Directive on Identity Management](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16577)
* [Directive on Security Management – Appendix A: Mandatory Procedures for Security Screening Control](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611#appA)
* [FAQ on Completing the Government of Canada Security Screening Application and Consent Form: Questions and Answers](https://www.gcpedia.gc.ca/gcwiki/images/1/16/FAQs_SSACF_EN.pdf) (PDF)
* [*PGS Security Controls (GCpedia) – Security Screening*](https://www.gcpedia.gc.ca/wiki/PGS_Security_Controls#Security_Screening) *(must be connected to the Government of Canada network)*
* [Policy on Government Security](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16578)
* [Position Analysis Tool (PAT)](http://www.gcpedia.gc.ca/gcwiki/images/a/ad/Position_Analysis_Tool_-_GCpedia_link.xlsx) (must be connected to the Government of Canada network)
* [Security Screening (COR302)](https://catalogue.csps-efpc.gc.ca/product?catalog=COR302&cm_locale=en)
* [[Security Screening Application and Consent Form](https://intranet.canada.ca/wg-tg/tbsf-fsct/ssacf-en.pdf)](https://intranet.canada.ca/wg-tg/tbsf-fsct/ssacf-en.pdf) (PDF, must be connected to the Government of Canada network)
* [Standard on Security Screening](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=28115)
* [Standard on Security Screening - Appendix B Security Screening Model and Criteria](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=28115#appB)

## Business Continuity Management

**Business Continuity Management (BCM)** is a vital component of departmental resilience.It’s a process that outlines the actions your department would take should a disruption occur like a flood, wildfire, power outage, tornado, etc. It ensures the continued delivery of critical services and activities by preventing impacts to business operations as well as ensuring the timely recovery of resources required to deliver other services and activities, such as facilities, people, equipment, assets, IT and data.

**A critical service is** a service or activity whose disruption would result in a high or very high degree of injury to the health, safety, security or economic well-being of Canadians or to the effective functioning of the Government of Canada.

If you **are** identified as an individual who supports a critical service or other impacted service, your manager (service owner) will advise you of your responsibilities during a disruption.

If you **are not** identified as an individual who supports a critical service or other impacted service, it’s still important to have a general understanding of BCM within your department so that you’re better prepared should a disruption occur.

Individuals employed with the Government of Canada should participate in BCM awareness and training activities to be able to so that they respond appropriately during a disruption.

If you’re unsure what your role would be during a disruption, speak to your manager or your departmental security office.

Your department may have complementary operational policies and standards that are specific to its mandate and mission.

### Resources

* Business Continuity Management (COR 311); forthcoming
* [Business Continuity Management - Lead Security Agency (GCpedia, must be connected to the Government of Canada network)](https://www.gcpedia.gc.ca/wiki/Business_Continuity_Management_-_Lead_Security_Agency)
* [Business Continuity Management Program Guide: A Government of Canada approach to building organizational resilience](https://www.gcpedia.gc.ca/gcwiki/images/0/02/Business_Continuity_Management_Program_Guide%2C_2023_Edition.pdf) (must be connected to the Government of Canada network)
* [Centre for Resiliency and Continuity Management (CRCM) (GCxchange)](https://can01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgcxgce.sharepoint.com%2Fteams%2F1000424%2FSitePages%2FProjectHome.aspx&data=05%7C02%7Crosella.ingriselli%40csps-efpc.gc.ca%7C00611be5a1014fc105a708dc2d8f8169%7Cedc33e68da6e4071b181ce7ba461fbae%7C0%7C0%7C638435341590865515%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=8iODqx7LxPzOjbYxF7Q%2FGr95SnCvM2DBlnk4QtRU9SI%3D&reserved=0)
* [Critical Services Framework](https://www.gcpedia.gc.ca/gcwiki/images/e/eb/Critical_Services_Framework_-_Job_Aid_-_EN.pdf) (must be connected to the Government of Canada network)
* [Criticality Impact Scale](https://gcxgce.sharepoint.com/:w:/t/1000424/EaBvd_D_6QlDv5SzlwB5VngBljq2nvojSw0oa09LOsJTIA?e=zheiJi&CID=528F6B4C-14C4-471A-A103-827907B3E648)
* [Directive on Security Management – Appendix D: Mandatory Procedures for Business Continuity Management Control](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611#appD)
* For any questions related to BCM, contact the Centre for Resiliency and Continuity Management at [crcm-cgcr@ps-sp.gc.ca (opens a new message in Outlook)](mailto:crcm-cgcr@ps-sp.gc.ca)
* [PGS Security Controls (GCpedia) – Business Continuity Management](https://www.gcpedia.gc.ca/wiki/PGS_Security_Controls#Business_Continuity_Management) (must be connected to the Government of Canada network)

## Security in Contracts and Other Arrangements

Some projects, programs, or services require collaboration with private sector and/or other public sector organizations.

In order for contractors to have access to government information, systems or buildings, they must undergo security screening as a minimum requirement.

When procuring goods or services, the **Security in Contracts and Other Arrangements** control ensures security requirements are identified and documented to adequately safeguard Protected and Classified Government of Canada information and assets.

Before access can be granted to a contractor, they must have the appropriate security screening level. It’s important that all security requirements be monitored and implemented throughout all stages of the contracting or arrangement process. This provides reasonable assurance that information, individuals, assets and services associated with the contract or arrangement are adequately safeguarded.

The **Security Requirements Check List (SRCL)** is aform that is used to identify and document security requirements associated with a contract and helps to ensure that security risks are reduced to an acceptable level. The SRCL ensures that appropriate safeguards, including security clauses, are in place to provide reasonable assurance and uphold the integrity of the Protected and Classified information and assets that are entrusted to the contractor.

Your department may have additional criteria relative to security requirements integrated into their contracts or other arrangements, as they can vary from one department to another, depending on the security risks involved. Your departmental security office will advise you of such conditions or criteria, as applicable.

Public Services and Procurement Canada (PSPC) plays an important role in providing leadership, advice and guidance for matters related to contract security. PSPC developed a [Contract Security Manual](https://www.tpsgc-pwgsc.gc.ca/esc-src/msc-csm/index-eng.html) that details the requirements of private sector organizations who are awarded a government contract in safeguarding government information and assets provided to or produced by them.

Your department may have complementary operational policies and standards that are specific to its mandate and mission.

### Resources

* [Contract Security Manual: A guide for organizations on federal government security standards and procedures](https://www.tpsgc-pwgsc.gc.ca/esc-src/msc-csm/index-eng.html)
* [Directive on Security Management – Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611#appF)
* [Managing Contracts for Services (COR404)](https://catalogue.csps-efpc.gc.ca/product?catalog=COR404&cm_locale=en)
* [PGS Security Controls (GCpedia) – Security requirements associated with contracts and other arrangements](https://www.gcpedia.gc.ca/wiki/PGS_Security_Controls#Security_requirements_associated_with_contracts_and_other_arrangements) (must be connected to the Government of Canada network)
* [Security requirements for contracting with the Government of Canada](https://www.tpsgc-pwgsc.gc.ca/esc-src/index-eng.html) - Public Services and Procurement Canada (PSPC) –
* [Security Requirement Check List (SRCL) Form](https://www.tbs-sct.canada.ca/tbsf-fsct/350-103-eng.asp)

## Physical Security

After obtaining your security screening level, on your first day of onboarding, you will receive an identification (ID) card. It provides you with access to your building and other secure work areas based on the requirements of your position and the screening level you obtained. This control provides assurance that you, your colleagues and Government of Canada assets are protected.

**Physical Security** refers to the use of safeguards that maintain workplace safety, protect against unauthorized access and detect attempted or actual unauthorized access.

### ****Access**** Control

Access control is the first line of defence in the protecting the Government of Canada’s information, assets, facilities and people. There are a variety of methods to control access, including having visitors sign in and out, having individuals employed with the Government of Canada show ID cards to security personnel, and the use of physical or mechanical barriers to control access (for example, locked doors, turnstiles and gates).

### Building access

Access controls ensure that only authorized individuals, who have been screened at the appropriate level and have a need-to-know clearance, have access to information and assets within a facility or restricted area. This is done by screening visitors and material at entry points and, where required, escorting them within the facility or restricted areas.

**Reminder:** The need-to-know principle refers to the need for someone to access and know information in order to perform their duties. This and the appropriate security screening level correspond with the level of information and/or assets being accessed.

**ID/Access Cards:** ID cards are different from access cards. Although they may appear similar, they serve different purposes. In some cases, ID and access cards are combined in one electronic access control card.

* **ID Cards:** ID cards are used to confirm that the individual is employed with the Government of Canada.
* **Access Cards:** Access cards are used to provide an individual with authorized access to specific areas within a facility.

 Your ID/access card should be carried with you and be visible at all times while on government premises. However, while in public places, it should be kept out of sight. This includes being on public transit, at a restaurant, shopping, eating lunch at the park, etc. For example, you never know if someone might take a picture of your ID/access card and create a copy to try and access Government of Canada information or assets.

You must never lend your ID/access card to anyone, even a colleague or a friend, because you’re responsible for any activities occurring with your card. Remember to remain vigilant in following proper security procedures for control of access.

In addition, you must not make any alterations to your ID/access card like punch a hole in the card to run a lanyard through it. Your ID card needs to be renewed periodically, especially if it’s worn or damaged or when your appearance changes to such an extent that you cannot be recognized from the current photo. The photo on your ID card should match your current appearance and people should be able to clearly identify you when you are accessing government facilities. If you think you need a new card, or if you have misplaced your ID/access card, contact your departmental security office.

 It is not uncommon to encounter unfamiliar individuals throughout your workday. It’s your duty to be vigilant and to take appropriate action if you see strangers in or near any restricted zones. If you notice anyone without an ID/access card in restricted zones, you must say something. You may approach the stranger yourself or immediately report suspicious activity to your manager or departmental security office. If you feel safe approaching them, respectfully question them to ensure that they have a valid reason to be there. Ask them politely to show you their ID/access card. If they do not have an ID/access card, consider redirecting them to the front desk/Commissionaires desk or informing your manager. Your department may have specific steps you should take in this situation. If a person refuses to accompany you, consider your own safety, and don’t hesitate to contact your departmental security office.

### ****Tailgating/****piggybacking

**Tailgating/piggybacking** refers to an individual tagging along or following an authorized individual employed with the Government of Canada through a security checkpoint or doorway without being registered through the system. This method of entry is unacceptable, and you must be vigilant in following proper security procedures for control of access. Letting someone in without access could pose a risk to the safety and security of everything and everyone in the building.

### ****Visitors****

Visitors, whether they’re from another department or a member of the public, must be registered prior to accessing government facilities and must be escorted at all times while accessing restricted government areas. This is another way to control access. The person who signed in the visitor is responsible for them while they are in the government facility. As an individual employed with the Government of Canada, it’s your responsibility to be aware of the different security zones in government facilities (for example, public, restricted or secure) and of who can and cannot be present in them. Verify with your departmental standards and operational policies and guidelines for specific considerations.

Access control procedures may be heightened or you may be asked to be more vigilant by your departmental security office if there is an increased threat or disruption.

Here are some best practices around Physical Security in a hybrid or remote work environment:

* Only use devices (mobile, laptop, tablet, USBs, etc.) and online tools (applications, software, internet browsers, programs, etc.) that have been approved by your department, as they will have more control over the security controls and configurations.
* Be mindful of your work-related conversations. Turn off or disconnect your virtual assistant (for example, Google Home, Amazon Alexa, Siri, etc.) to prevent the devices from recording and listening to your work-related conversations.
* No matter where you’re working, have a designated workspace and/or use headsets or designated rooms (like a quiet room) to reduce the risk of others hearing your work-related conversations.

Your department may have complementary operational policies and standards that are specific to its mandate and mission.

### Resources

* [Directive on Security Management – Appendix C: Mandatory Procedures for Physical Security Control](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611#appC)
* [Fundamentals of Physical Security (COR304)](https://catalogue.csps-efpc.gc.ca/product?catalog=COR304&cm_locale=en)
* [PGS Security Controls (GCpedia) – Physical Security Control](https://www.gcpedia.gc.ca/wiki/PGS_Security_Controls#Physical_Security) (must be connected to the Government of Canada network)
* [RCMP Lead Security Agency for Physical Security Homepage](https://www.rcmp-grc.gc.ca/physec-secmat/index-eng.htm)
* [RCMP Physical Security Considerations for Remote and Telework Environments - Employee Responsibilities](https://www.rcmp-grc.gc.ca/physec-secmat/pubs/gcpsg-gsmgc-008-eng.htm#a9_3)
* [RCMP Security Equipment Guide](https://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_e.htm) (must be connected to the Government of Canada network)

## Information Technology Security

You’re required to protect government information systems, digital devices and the information the devices and systems hold, whether you’re working remotely, in the office or on travel status, and whether you’re connected to the virtual private network (VPN).

**Information Technology (IT) Security** provides reasonable assurance that information systems can be trusted to adequately safeguard information, are used in accordance with the sensitivity of the information, and support government programs, services and activities.

You’re responsible for safeguarding the information stored on Government of Canada digital devices such as computers, laptops, portable media storage devices, mobile devices and networks, regardless of your work location.

As individuals employed with the Government of Canada, you may encounter daily IT security risks or threats, especially given the digital nature of our work. Threats can be deliberate, accidental or a result of natural hazards. However, users should be particularly concerned about deliberate threats and human errors. Your action or inaction can significantly increase the risk to the integrity of the Government of Canada.

### Encryption

Encryption technologies are used to secure many of the applications and websites you use daily. For example, online banking or shopping, email applications and secure instant messaging use encryption. Encryption technologies secure information while it’s in transit (such as connecting to a website) and while it’s at rest (stored in encrypted databases). Encryption encodes (or scrambles) information.

 The purpose of encrypting a storage device, file or email is to ensure that it is safely transmitted to the intended recipient and prevents unauthorized access. The level of injury for not encrypting could vary from minor to severe as it depends on who the information was sent to and the topic.

### MyKEY

MyKEY is the government standard for the purposes of encrypting and decrypting files, emails and accessing various other Government of Canada online self-service tools such as the Compensation Web Applications (CWA). MyKEY is approved to secure information up to Protected B. Your department will also provide encryption tools to protect portable storage devices.

Your departmental security office or IT security services can provide additional guidance.

### ****Passwords****

Strong passwords provide a direct means of safeguarding a system or account information and are the first line of defence against threat actors. Passwords should include upper- and lower-case letters, numbers and special characters, and be at least 8 to 12 characters in length. It is also helpful to avoid dictionary words and common names like Canada01, password123, or dogsrock!, for example. Keep in mind, the shorter the password, the easier it is to crack.

### Passphrases

A passphrase is a memorized phrase consisting of a sequence of mixed words with or without spaces. Your passphrase should be at least 4 words and 15 characters in length. For example, you might create a passphrase using words to describe what you see around you such as “Closet Lamp Bathroom Mug.”

Don’t display, reuse or share your passwords and passphrases, and don’t use your personal account passwords or passphrases for your work accounts.

Be sure to select proper passwords and passphrases in accordance with your department’s password guidelines for number of characters, special characters, etc.

Access to Government of Canada devices and networks like the VPN and departmental networks is only granted to authorized individuals for the conduct of official business, including activities that are necessary for your job functions.

All use of Government of Canada devices and networks must not give rise to a real, potential or apparent conflict of interest or in any way undermine the integrity of your department, whether you’re connected to the VPN or not.

You may use your device for work-related and professional development activities like participating in online professional training activities (for example, webcasts, online learning products via the School, podcasts) or making arrangements for work-related travel, including booking tickets and searching for information about accommodations via Government of Canada or third-party travel review services. You may also use your device for limited personal use like checking the weather forecast or confirming the bus/train schedule information. However, you need to be mindful that the websites you’re visiting or the person or company hosting the webcast are reputable. Some websites may try to install viruses (or malware) without your knowledge.

* Unacceptable use can have criminal or legal consequences, as determined by the applicable section of the law. Unacceptable use can also lead to disciplinary action, as determined by policies and recommendations of human resources or labour relations advisors and lead to corrective administrative measures, up to and including suspension and/or termination of employment in the Government of Canada.

To ensure that your computer is working optimally, follow these three golden rules:

1. Always **sign out** at the end of the day. This way, your computer stays connected to the network overnight to receive important software and security updates.
2. Always **restart** your computer before signing on to begin your workday.
3. **Always log in** and connect to your departmental VPN to ensure you’re working on a secure network.

### ****Mal****icious software

Malicious software, or malware, is software used by cyber attackers to disrupt your device operations, gather sensitive information like banking credentials or gain unauthorized access to device.

Malware comes in a wide variety of forms, and can be used to steal passwords, files or other sensitive information. Some malwares can remain undetected for prolonged periods of time, stealing large volumes of sensitive information.

The most common means for malware to enter government systems is through phishing emails.

### Phishing

Phishing is the act of sending communications like emails, texts, phone calls and so on that appear to be legitimate but are fake. These communications often contain malicious attachments or links that threat actors want you to click on.

Here are a few additional tips to help you spot a phishing email:

* Check for subtle changes to the email address and links like .gc/.ca/.org. Domains should reference a valid department or organization and be consistent with the message.
* Research their website, company or LinkedIn page to confirm the request using a verified telephone number or web address from another source. Do not use the contact information provided in the message.
* You can also use the HALT method (Hover, Analyze, Look, Test) to determine if this is a suspicious email.
* If available, use the Report Message button within Outlook to flag and report suspicious emails or contact your IT security office. Otherwise, ask your departmental IT help desk how best to report a phishing email.

 When in doubt, ask your departmental IT security office or departmental security office for more information.

Your department may have complementary operational policies and standards that are specific to its mandate and mission.

To learn more, refer to these resources or take the cyber security courses offered by the School.

### Resources

* [Best practices for passphrases and passwords](https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032) - Canadian Centre for Cyber Security
* [Cyber security at home and in the office: Secure your devices, computers, and networks](https://www.cyber.gc.ca/en/guidance/cyber-security-home-and-office-secure-your-devices-computers-and-networks-itsap00007) - Canadian Centre for Cyber Security
* [Cyber Security in the GC and Online Exposure (DDN233)](https://catalogue.csps-efpc.gc.ca/product?catalog=DDN233&cm_locale=en)
* [Cyber Security in the GC for Non-IT Employees (DDN231)](https://catalogue.csps-efpc.gc.ca/product?catalog=DDN231&cm_locale=en)
* [Directive on Security Management, Appendix B: Mandatory Procedures for Information Technology Security Control](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611#appB)
* [Directive on Service and Digital](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601)
* [Directive on Telework](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32636&section=html)
* [Discover Cyber Security course (DDN235)](https://catalogue.csps-efpc.gc.ca/product?catalog=DDN235&cm_locale=en)
* [GetCyberSafe.ca](https://www.getcybersafe.gc.ca/)
* [Password Guidance - Executive summary](https://www.canada.ca/en/government/system/digital-government/online-security-privacy/password-guidance.html#toc1)
* [PGS Security Controls (GCpedia) – Information Technology](https://www.gcpedia.gc.ca/wiki/PGS_Security_Controls#Information_Technology_Security) (must be connected to the Government of Canada network)
* [Protect your organization from malware](https://www.cyber.gc.ca/en/guidance/protect-your-organization-malware-itsap00057) - Canadian Centre for Cyber Security
* [Policy on Communications and Federal Identity](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=30683&section=html)
* [Using encryption to keep your sensitive data secure](https://www.cyber.gc.ca/en/guidance/using-encryption-keep-your-sensitive-data-secure-itsap40016) - Canadian Centre for Cyber Security
* [Values and Ethics Code for the Public Sector](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=25049)

## Information Management Security

Safeguarding sensitive information is vital to the business of the Government of Canada and can only be achieved through sound information management and security practices.

We all create, receive, organize, collect, use, disseminate, maintain, transfer and dispose of information resources as part of our daily work, and we are all responsible for effectively managing these resources, regardless of our workplace location.

**Information Management (IM) Security** ensures appropriate protection of all Government of Canada information.

As an individual employed with the Government of Canada, you have a responsibility to follow IM policy requirements and departmental best practices to ensure the secure management of information throughout its life cycle. Throughout your career, you will manage information and assets in all forms of media, including both electronic and hard copy. Appropriate records relating to your work, whatever the form, need to be categorized and safeguarded in the appropriate manner.

Government of Canada information can be categorized as Protected or Classified.

To determine a security category, you should apply the injury test to determine whether information is categorized as having a low, medium, high or very high degree or level of injury that could be reasonably expected due to:

1. Loss of confidentiality (resulting from unauthorized disclosure; for example, reports or files sent to the wrong person)
2. Loss of integrity (resulting from unauthorized modification or destruction; for example, changing a report to alter the meaning or results)
3. Loss of availability (resulting from unauthorized removal or other disruption; for example, deleting information so it’s no longer available)

### Level of Injury

|  |  |  |  |
| --- | --- | --- | --- |
| Low | Medium | High | Very High |
| Equate to Unclassified or Protected A | Equate to Protected B or CONFIDENTIAL | Equate to Protected C or SECRET | Equate to TOP SECRET |

### Protected Information

Information is identified and categorized as Protected (A, B and C) when unauthorized disclosure could reasonably be expected to **cause injury outside the national interest** (for example, to individuals or businesses).

* **Protected A** applies to information that, if compromised, could reasonably be expected to cause **limited or moderate injury** **outside the national interest**. Examples include:
* Personal information such as date of birth, home address, exact salary
* Personal or business-related information that could lead to a loss of reputation/ competitiveness
* Impediments to criminal investigations
* **Protected B** applies to information that, if compromised, could reasonably be expected to cause **serious injury** **outside the national interest**. Examples include:
* Personal information such as medical information, finances/credit, or personnel assessments
* Aggregate of social insurance number (SIN) and other personal information
* Business information related to trade secrets, competitive position or contract negotiations
* **Protected C** applies to a very limited amount of information that, if compromised, could reasonably be expected to cause **extremely grave injury** **outside the national interest**. Examples include:
* Witness protection program
* Police informants
* Criminal intelligence

### Classified Information

Information is identified and categorized as Classified (Confidential, Secret or Top Secret) when unauthorized disclosure could reasonably be expected to **cause injury to the national interest**. National interest includes national security and the social, political and economic stability of Canada.

* **Confidential** applies when unauthorized disclosure could reasonably be expected to cause **limited or moderate injury** **to the national interest**. Examples include:
  + Cause damage to diplomatic or federal-provincial relations (for example, cause formal protest)
  + Damage to national finances or economic interests
  + Disrupt significant national operations or critical national infrastructure
* **Secret** applies when unauthorized disclosure could reasonably be expected to cause **serious injury** **to the national interest**. Examples include:
* Cause serious damage to relations with foreign governments
* Threaten life directly, seriously prejudice public order, safety or national security
* Cause substantial material damage to national finances or economic interests
* Shut down or substantially disrupt critical national infrastructure
* **Top Secret** applies to the very limited amount of information that, if compromised could reasonably be expected to cause **exceptionally grave injury** **to the national interest**. Examples include:
* Lead directly to widespread loss of life
* Disrupt foreign relations vitally affecting national security
* Cause substantial instability or loss of continuity of the Government of Canada
* Compromise vital national defence plans or sensitive intelligence operations

In addition to categorization, departments may have other markings (sometimes called caveats) for specific types of documents, including unclassified, Cabinet confidence or solicitor-client privilege.  To ensure you are safeguarding information in your daily work, familiarize yourself with your department’s mandate and complementary operational IM policies and standards.

If you’re not sure which level of categorization is appropriate, ask your manager or supervisor. It’s important to categorize information at the appropriate level.

### Security Marking

No matter where you work, you need to assign a security category to departmental information resources, and physical and electronic forms that corresponds with the degree of injury that could reasonably be expected because of its compromise. You must apply the security marking to alert users of the level of safeguarding that should be applied to the information.

### Clean Desk/Work Area Strategy

Maintaining a clean work area, regardless of whether working at the office or remotely, is an important best practice in ensuring information security. It helps reduce the risk of accidental disclosure of sensitive Government of Canada information and assets caused by information being left unattended. At a minimum, you should clear your work area at the end of each workday to prevent accidental loss of sensitive information. Examples of clean desk/work area strategies include:

* Logging out/locking your workstation ensures no one will go onto your device to look at files, gather information or send emails to other individuals employed with the Government of Canada. It has happened before. A keyboard shortcut to lock your device is pressing the Control, Alt and Delete button at the same time, or the Windows and L key
* Store all information and assets appropriately
* Secure equipment (tablet, laptop, computers, cell phones, etc.) appropriately
* Connect to your departmental VPN to ensure you’re working on a secure network

### Electronic Security

Only approved portable storage devices (for example, encrypted USB) may be used for processing information up to Protected B. Only approved systems (for example, the Government of Canada Secret Infrastructure [GCSI]) may be used for processing Protected C and Secret information. Never send an email containing sensitive information from your departmental network account to external accounts like Gmail or Hotmail. because they are not secure, and information can be intercepted.

Social media, instant messaging and text message applications are vulnerable to different security threats and should never be used for communicating sensitive information.

### Email

Always double check the recipient’s address before sending an email. Be careful not to inadvertently transmit sensitive information that’s not protected by email or to inadvertently send sensitive information to the wrong address or recipient. Human error is the most common cause of privacy breaches. Protected A and B information should be encrypted using a Government of Canada approved solution such as myKEY.

### Public spaces

You should never view, handle or discuss Protected (A, B, C) or Classified (Confidential, Secret or Top Secret) information in public spaces like a coffee shop or when travelling (for example, on a bus, airplane or train). Use an approved secure space to ensure that people nearby cannot eavesdrop on sensitive conversations. Someone who does not have the need to know could look over your shoulder to get or view the information without your knowledge. This is known as “shoulder surfing”.

Your level of security screening does not give you access to all information in the associated category. You should only have access to information that you need to do your job. This is known as the need-to-know principle. The need-to-know and the appropriate security screening level correspond with the level of information and/or assets being accessed.

The department originating or acquiring sensitive information and assets is responsible for identifying any need-to-know constraints or limitations. In some cases, distribution may be limited to a specific group of individuals with the need-to-know.

If you’re unsure what level of security screening allows you to access specific documents, ask your manager or your departmental security office for guidance. It’s important to be vigilant against possible violations.

The loss or compromise (or suspected compromise) of Protected or Classified information constitutes a security incident and must be reported immediately to your departmental security office.

Remember that security is everyone’s business and failure to report security incidents could result in more serious damage.

**Consequences** may include calling your department's integrity into question and could lead to corrective administrative measures, set out in established Government of Canada frameworks, for both institutions and individuals, up to and including suspension and/or termination of employment.

Your department may have complementary operational departmental policies and standards that are specific to its mandate and mission.

### Resources

* [Access to Information and Privacy Fundamentals (COR502)](https://catalogue.csps-efpc.gc.ca/product?catalog=COR502&cm_locale=en)
* [Big Data Fundamentals (DDN305)](https://catalogue.csps-efpc.gc.ca/product?catalog=DDN305&cm_locale=en)
* [Directive on Security Management – Appendix E: Mandatory Procedures for Information Management Security Control](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611#appE)
* [Directive on Security Management – Appendix J: Standard on Security Categorization](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32614)
* [Directive on Service and Digital](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601)
* [Fundamentals of Information Management (COR501)](https://catalogue.csps-efpc.gc.ca/product?catalog=COR501&cm_locale=en)
* [GC Security Categorization Model](https://www.gcpedia.gc.ca/gcwiki/images/3/3c/GC_Classification_Model_-_BIL.pptx) (must be connected to the Government of Canada network)
* [Guidelines for Employees of the Government of Canada: Information Management (IM) Basics](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16557#cha10)
* [Information Management Awareness Quiz (COR510)](https://catalogue.csps-efpc.gc.ca/product?catalog=COR510&cm_locale=en)
* [Information Management in the Government of Canada (COR505)](https://catalogue.csps-efpc.gc.ca/product?catalog=COR505&cm_locale=en)
* [Information Management Methods and Tools (COR509)](https://catalogue.csps-efpc.gc.ca/product?catalog=COR509&cm_locale=en)
* [Information Management: Supporting Programs and Services (COR508)](https://catalogue.csps-efpc.gc.ca/product?catalog=COR508&cm_locale=en)
* [PGS Security Controls (GCpedia) – Information Management Security](https://www.gcpedia.gc.ca/wiki/PGS_Security_Controls#Information_Management_Security) (must be connected to the Government of Canada network)
* [Privacy in the Government of Canada (COR504)](https://catalogue.csps-efpc.gc.ca/product?catalog=COR504&cm_locale=en)
* [Protecting Sensitive Information in GCdocs (COR518)](https://catalogue.csps-efpc.gc.ca/product?catalog=COR518&cm_locale=en)

## Security Event Management

We all have an important role in protecting Government of Canada information, assets and individuals.

**Examples of security concerns:**

* Failure to appropriately categorize sensitive information
* Failure to secure protected or classified information (like leaving a cabinet unlocked in an area where not everyone has the appropriate screening level or the need to know)
* Failure to report the loss of identification cards or access cards
* Failure to safeguard keys, combinations or passwords
* Accessing or removing sensitive information or assets without authorization

 It’s your responsibility to follow these procedures and immediately report all security concerns to your manager or departmental security office so that corrective action can be taken, up to and including suspension and/or termination of your employment with the Government of Canada.

### Reporting Requirements

* Understand your role in monitoring and reporting security concerns
* Report suspected or real security concerns to your manager or departmental security office as soon as possible
* Report any changes in personal circumstances such as change in criminal record status, change in financial situation or change in marital status

Every department has its own reporting procedures and contacts. It’s your responsibility to know these procedures. If you notice something, say something. When in doubt, err on the side of caution and report it.

**Consequence:** Security concerns could have serious implications. Unreported concerns carry an increased risk of harm to you and/or your department. You could be held accountable for failing to report a security concern and this could lead to corrective administrative measures against you, up to and including suspension and/or termination of your employment with the Government of Canada.

Remember, as an individual employed with the Government of Canada, you have an important responsibility for the safety and security of colleagues, information and assets.

Your department may have complementary operational policies and standards that are specific to its mandate and mission.

### Resources

* [Directive on Security Management – Appendix G: Mandatory Procedures for Security Event Management Control](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611#appG)
* [Directive on Security Management – Appendix I: Standard on Security Event Reporting](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32613)
* [Federal Basic Emergency Management (COR308)](https://catalogue.csps-efpc.gc.ca/product?catalog=COR308&cm_locale=en)
* [PGS Security Controls (GCpedia) – Security Event Management](https://www.gcpedia.gc.ca/wiki/PGS_Security_Controls#Security_Event_Management) (must be connected to the Government of Canada network)
* [*Public Servants Disclosure Protection Act*](https://laws-lois.justice.gc.ca/eng/acts/p-31.9/)

## Security Awareness and Training

Security awareness is a shared responsibility, and everyone has a role to play. It’s important that you participate in departmental security awareness activities to learn about your responsibilities for safeguarding the people, information and assets of the Government of Canada. Most importantly, check in with your departmental security office for any questions or concerns you might have.

Participating in departmental activities provides reasonable assurance that you will not knowingly compromise security and that you understand the potential consequences of not meeting your security responsibilities. Together, we promote a strong security culture and strengthen the security posture of our department and the Government of Canada.

Stay engaged with your departmental security office.

Integrate security considerations into information management processes throughout the information life cycle by doing training, taking courses and consulting departmental standards, etc.

Pay attention to the many campaigns, messages and briefings available to ensure you do your part to be security smart!

To increase your knowledge of security, please visit the [Canada School of Public Service and browse the learning catalogue.](https://csps-efpc.gc.ca/catalogue/topics-eng.aspx)

Knowing the basics about cyber security is beneficial to all individuals working with the Government of Canada. The course [Discover Cyber Security (DDN235)](https://catalogue.csps-efpc.gc.ca/product?catalog=DDN235&cm_locale=en) provides an introduction to key cyber security concepts.

### Resources

* [Canada School of Public Service learning catalogue](https://catalogue.csps-efpc.gc.ca/?cm_locale=en)
* [Directive on Security Management](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611)
* [Policy on Government Security](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16578)
* [Security Functional Specialist Orientation Kit (COR301)](https://catalogue.csps-efpc.gc.ca/product?catalog=COR301&cm_locale=en)

## Conclusion

It’s important that you understand your role in monitoring and reporting security concerns and in reporting suspected or real security concerns to your manager or departmental security office as soon as possible. Every department has its own reporting procedures and contacts. Remember to stay vigilant as your department may conduct routine inspections to verify compliance with government and departmental security policies and procedures to detect possible security concerns.

If you notice something, say something. When in doubt, err on the side of caution and report. The consequences of doing nothing can include putting your department’s integrity in question and could lead to corrective administrative measures, set out in established Government of Canada frameworks, for both institutions and individuals, up to and including suspension and/or termination of employment in the Government of Canada.

For any questions relating to Treasury Board of Canada Secretariat (TBS) security policies, standards and directives, or for any additional information and guidance, email [SEC@tbs-sct.gc.ca](mailto:SEC@tbs-sct.gc.ca) (opens a new message in Outlook).

Remember, as an individual employed with the Government of Canada, you have an important responsibility for the safety and security of colleagues, information, and assets.

Do your part – Be security smart!

Please go back to the online course to complete the Final Assessment.