BRITISH COLUMBIA | Office of the Chief Information Officer

# Security 101 Guidebook - The Basics of Information Security in the Government of British Columbia

## Information Security Branch

*"It is the responsibility of every employee to protect government information"*

*Gary Perkins, Chief Information Security Officer*

Security Classification: **Low Sensitivity**

Document created October 2012 – Last revised January 2014

# TABLE OF CONTENTS

**INTRODUCTION ..... 3**

Why Have a Guidebook on Information Security? ..... 3
What is Information Security? ..... 3
What Kind of Information Do You Need to Protect? ..... 3
Employee Roles and Responsibilities in Relation to Information Security ..... 4
What are Information Security Policies and How Do They Relate to You? ..... 5
What If There is an Information Security Breach (including a Privacy Breach)? ..... 5
Who Should You Contact Regarding Information Security? ..... 6

**SECURITY THREATS AND RISKS ..... 7**

Identity Theft/Identity Fraud ..... 7
Malicious Code or Malware ..... 7
Internet Hoaxes ..... 10
Spam ..... 9
Phishing ..... 8
Social Engineering ..... 8

**SECURITY TIPS FOR EMPLOYEES ..... 11**

Protect Your Workstation ..... 11
Protect Your IDIR Account ..... 11
Protect Your Passwords ..... 11
Protect Your Workplace ..... 13

**GENERAL INFORMATION ..... 14**

Installing Software on Your Government Computer ..... 14
Using B.C. Government Email ..... 14
Accessing Personal Email ..... 15
Using the Internet ..... 15
Using Portable Storage Devices ..... 15
Protecting the Laptop, Tablet, BlackBerry, Mobile Phone or Other Similar Device ..... 16
Reporting the Loss or Theft of Your Government Device ..... 16
Protecting Information on Paper ..... 17
Classifying Information ..... 17
Working Outside of the Workplace ..... 17

**REFERENCE GUIDE TO MANY OF THE POLICIES RELATED TO INFORMATION SECURITY ..... 19**

**APPENDIX A – SHORT DESCRIPTIONS OF VARIOUS TYPES OF MALWARE ..... 20**

*Please note that some listed resources or references in this document may only be accessible to B.C. government employees. Links with https://gww and the lock symbol 🔒 are internal to government.*

# INTRODUCTION

## Why Have a Guidebook on Information Security?

After all, don't the "techies" take care of all that? Yes, they do a great deal of work to protect the information and the technology of the B.C. government. Research and experience have shown, however, that most breaches of information security in organizations occur because the people that use the information – the employees – were not given the guidelines and education they needed to take the simple actions designed to prevent breaches. Employees can be the 'weakest link'.

> ***Information Security Branch Vision:***
> *Leaders in Information Protection: Security, Trust, Excellence*
> ***Mission:*** *Enable Government to provide services in a trusted and secure manner*

The purpose of this Guidebook is to help you protect government information. It was prepared by the Information Security Branch in the Office of the Chief Information Officer as part of the security awareness program. This Guidebook provides an overview of the British Columbia government policies on information security, describes security threats and risks, outlines employee roles and responsibilities, and provides security tips for all employees to follow.

While this Guidebook is intended for employees handling government information, the security threats and tips described will generally also apply when you are on your home computer or using the various types of mobile devices (e.g. laptops, tablets, e-readers and smartphones) available on the market. By becoming aware of the ways in which to protect information, you can adopt a 'security state of mind' and reduce the likelihood of being a victim of cybercrime.

## What is Information Security?

Information is an asset and the information that government collects, uses, maintains, stores, transmits and may eventually dispose of, is central to the work of every part of the government. The B.C. government is aware of the responsibility it has to protect that information and to ensure that the public has confidence in government's ability to protect the privacy and security of their personal information. This includes financial details, medical records, drivers' records and more.

Information security is about protecting information, software, and equipment from problems relating to disclosure, modification, interruption and disposal. With the information itself, requirements for privacy, confidentiality, integrity and availability must also be addressed.

## What Kind of Information Do You Need to Protect?

As a government employee, you have access to a tremendous amount of information; therefore, the Office of the Chief Information Officer recommends that you become familiar with the contents of this Guidebook. In the B.C. government, there are three types of information that need to be protected: Personal, Confidential and Sensitive.

**Personal Information:**
Personal information means recorded information about an identifiable individual other than business contact information. Personal information can be about government employees, government clients or others and may be held by government or administered by service providers on behalf of government.

Personal information includes, but is not limited to:

- name, address, telephone number, email address
- race, national/ethnic origin, colour, religious or political beliefs or associations
- age, gender, sexual orientation, marital status
- identifying number or symbol such as social insurance number or driver licence number
- fingerprints, blood type, DNA prints
- health care history
- educational, financial, criminal, employment history
- anyone else's views or opinions about an individual and the individual's personal views or opinions unless they are about someone else.

Personal information also includes separate pieces of information that may seem unrelated, but when put together would allow someone to accurately infer information about an individual.

**Confidential Information:**
There are various types of confidential information, but generally confidential information can be described as:

- Cabinet confidences (e.g., a briefing note to Cabinet or a Cabinet submission)
- government economic or financial information (e.g., proposed budget before it is announced)
- information harmful to intergovernmental relations (e.g., information received in confidence from another government)
- third-party business information, where the disclosure of the information would harm the third party.

**Sensitive Information:**
Personal and/or confidential information are examples of sensitive information that, if compromised, could result in serious consequences for individuals, organizations or government. For example, personal information about an individual within a witness protection program is deemed as sensitive information because, if compromised, it could lead to serious harm to the individual. It also violates the requirements of the *Freedom of Information and Protection of Privacy Act*. Similarly, the architectural drawings of a correctional facility are examples of sensitive information because of the nature and function of the building and how the information could be used.

## Employee Roles and Responsibilities in Relation to Information Security

B.C. government employees are required to take an Oath of Employment and to abide by the Standards of Conduct. Both require that employees uphold the confidentiality of government information. These expectations are not unique – employers everywhere expect employees to respect the importance of the information they access on the job.

B.C. government employees are also responsible for complying with the Information Security Policy, other information management policies, and approved standards and practices while accessing government information, services and equipment.

*Information Security enables Citizen Participation, Self-Service and Business Innovation in the Province of British Columbia*

As of 2010, all B.C. government employees are required to take a mandatory online training course - IM 111: Information Sharing and Privacy Awareness Training for Employees, to learn about information sharing. The course also focuses on how to avoid an information incident or privacy breach, and how to respond if a breach is suspected or has occurred. This is only one of the IM/IT courses provided by The Learning Centre of the B.C. Public Service Agency.

Beyond the mandatory IM 111 course, other information security courses are IM 110: Managing Our Information Assets, IM 113: An Overview of Information Security and You, and IM 114: A Day in the Life; Information Security and You – Knowledge Check. It is the employee's responsibility to learn more about information sharing, privacy and security by participating in these online courses. All that is needed is your supervisor's approval. The courses are available online and can be taken at your convenience. For information and to register, visit the Privacy & Information Sharing Courses page.

Your contribution to ensuring and maintaining information security benefits every British Columbian, including you, as an employee and as a citizen who accesses and receives government programs and services.

## What are Information Security Policies and How Do They Relate to You?

Policy is intended to enable things to happen by giving people the direction they need to do their work properly and consistently. Information security policies document appropriate behaviour and clearly describe what must be done, and what is or is not allowed.

As an employee, you need to know and follow government policies. In June of 2006, the British Columbia government adopted a comprehensive Information Security Policy (ISP), based on international standards, which applies to all employees and the work they do. The ISP (version 2.2) is available at the Office of the Chief Information Officer's Information Security website: http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf.

To simplify interpretation and application of the policies, a series of more than 30 Information Security Policy Summaries was produced that cover many subject areas and provide the specific references from the ISP, as well as other resources. Subject areas include portable storage devices, wireless networking, security awareness, and information security classification. The list of Policy Summaries can be found at http://www.cio.gov.bc.ca/cio/informationsecurity/policy/isp_summaries.page.

## What If There is an Information Security or Privacy Breach?

The B.C. government has a comprehensive Information Incident Management Process for responding to privacy and security breaches. An information incident (a broader term than "breach") occurs when unwanted or unexpected events threaten privacy or information security. They can be accidental or deliberate and include the theft, loss, unauthorized alteration or destruction of information. An information incident can be especially serious when it is a privacy breach where the compromised data includes personal information such as names,

birthdates, health or financial details, or social insurance numbers, or involves sensitive information such as Cabinet documents.

The key to responding to information incidents is to take action as soon as possible! You are responsible to report any actual or suspected information incident immediately to your supervisor. You or your supervisor must also immediately notify the Office of the Chief Information Officer by dialling the Shared Services BC (SSBC) Service Desk at 250 387-7000 or toll-free at 1-866-660-0811 and selecting Option 3. You will then be contacted shortly by the Office of the Chief Information Officer's Investigations Unit (in the Information Security Branch), which will seek further details and may give advice on next steps.

*See the Easy Guide for Responding to Information Incidents: The "3RP" - Report, Recover, Remediate and Prevent*

If there is a desktop computer, laptop or mobile device involved in the information incident – do not touch it, do not shut it down; secure it until the situation has been reported and you receive information from the Investigations Unit.

The Information Incident Management Process policy document, Checklist, Easy Guide, Process for Responding and the Report Form all can be found at http://www.cio.gov.bc.ca/cio/information_incident/index.page.

## Who Should You Contact Regarding Information Security?

Every ministry has a Ministry Information Security Officer (MISO) who is the single point of contact for information security issues and related concerns in their ministry. The MISO in your ministry has a good understanding of current information security threats and risks and will know when it is appropriate to conduct Security Threat and Risk Assessments (STRAs) and Privacy Impact Assessments (PIAs) on projects or initiatives within the scope of your work. The MISO's responsibilities are described here: http://www.cio.gov.bc.ca/cio/informationsecurity/MISO/MISORole.page?.

B.C. government employees can obtain the contact list of MISOs for each ministry at the following internal website: https://gww.cio.gov.bc.ca/MISO/MISOs.htm

Ministries also have a Ministry Chief Information Officer (MCIO). The Core Policy and Procedures Manual, Chapter 12, provides a description of the MCIO's responsibilities. A list of the MCIOs is available at: http://www.cio.gov.bc.ca/cio/about/governance/role_cio/mcio_contact_list.page

You may also contact the Information Security Branch at CITZCIOSecurity@gov.bc.ca to ask questions about information security or this Guidebook.

# SECURITY THREATS AND RISKS

Cybercrime is a business – a very large and lucrative world-wide illegal business, operating in "the Underground Economy". It is no longer primarily a hobby for individual hackers seeking new computer challenges. Cybercrime operations function much like legitimate organizations, with a hierarchy of management, job descriptions, distributors, low level helpers and advertising on their own hidden networks. They also operate on a global level with connections in many countries to avoid detection. Cybercriminals who want to operate on their own can purchase the hacking software and tools they require. The option also exists to hire or outsource this business, much the same way legitimate organizations do.

It is very important for all employees, at every level, to understand the role that they constantly play in protecting information and the many types of devices we use. In fact, employees that are not aware of the ways they can prevent security breaches pose a potential risk to their employer. Employee awareness has become an essential component of information security in all organizations world-wide, regardless of their business. Security researchers consistently emphasize that employee awareness must be part of every organization's security budget and priorities.

Cybercrime in general has two major goals: (1) to steal whatever personal and sensitive information is considered important to commit identity theft/fraud, and (2) to install malicious code into the computer system that will continue to perform tasks without the knowledge of the owner. Cybercriminals are continuously creating new methods of infiltrating computers and networks to make money by stealing information and manipulating people, via social engineering, into unknowingly assisting them. Following are descriptions of the major threats to information security that can apply not only at work but also on home computers and mobile devices. Every technology user should become familiar with these threats and how to avoid them.

## Identity Theft/ Identity Fraud

Identity theft is fraud. It occurs when someone else uses your personal information without your knowledge or consent to commit a crime. The fraud may involve using your credit card for making transactions, selling your information in the underground economy, or actually setting up a separate identity that can involve taking out loans, buying homes, buying goods and services or travelling over a period of time, in your name and without your knowledge. Identity theft also includes fraudulently using your work or personal email address (and those of your contacts) to send out spam email that appears to come from you. When a data breach captures the names and email addresses of online users, the hackers might not get the users' financial information, but they can still benefit by having their email addresses. Your personal information, which includes your work credentials - IDIR account name and password - can be stolen using the Internet in various ways which are described below. Your home/personal email holds the key to unlocking much of your online identity.

## Malicious Code or Malware

Malicious code is the term used to describe software (a computer program or application) designed to exploit, infiltrate or damage a computer system without the informed consent of the computer user. It is also referred to as "malware" and includes computer viruses, worms, Trojan horses, rootkits, spyware, dishonest adware, and other

*In the first three quarters of 2013, 72 cyber security investigations were undertaken.*

unwanted software. Malicious code is typically distributed over the Internet, by email or via compromised web pages. A user can click on a link in a phishing email that results in the hacker planting malware on the computer. Hackers have also corrupted or substituted websites so that visiting the sites has the same impact. See Appendix A for a list of common types of malware.

## Social Engineering

Social engineering refers to manipulating others. People who cheat others for personal gain have always been part of society, unfortunately. Con artists, frauds, cheats, and social engineers rely upon the fact that other people are essentially trusting and considerate, and do not go through life being suspicious. People are likely to respond to offers that sound "too good to be true".

Social engineers use methods such as shoulder-surfing (looking at your monitor, your keystrokes or papers on the desk), mass marketing telephone calls and texts, or fraudulent emails to obtain sensitive details. Generally, it is easier for hackers to take advantage of people in this way, rather than trying to locate and exploit computer security vulnerabilities. Many large breaches of security in companies world-wide started by social engineering an employee, usually with a phishing email, into innocently providing information that gave the cybercriminals access. Social engineering has always been used to breach physical security. Many criminals have gained access to a secure workplace by fraudulently presenting themselves as workers, contractors or tradespeople that are supposed to be there, and were not asked to provide proof of their identity.

Be suspicious of unsolicited telephone calls or emails requesting personal, financial or account information, or information about the government's network, its employees or clients. Ask yourself if you should be giving out the information – it is better to tell the person you will call back so you can talk to someone else about it. Use your instincts (also called your "gut feeling") – if something just does not quite "feel right", don't give the person what they are seeking without getting confirmation. If you see someone in your work area that might not belong there, ask questions. If you are even slightly suspicious, do not provide access or information and report the matter to your supervisor or manager, and if appropriate, to building security. Remember to secure (or 'Lock') your computer when you walk away from it so that no one else can use your computer.

## Phishing

The use of phishing email is a common type of online fraud, identified as one of the top Internet-based threats used for credit card fraud and identity theft. Phishing attempts to trick people into disclosing credit card numbers or online banking information. The method involves sending a fake email that appears to come from a legitimate and reputable source, such as a bank or other financial institution, an online shopping company, or a Help Desk. The email asks the recipient to enter their financial information (credit or debit number and password) or their credentials (username or IDIR ID and password) due to a problem, thereby preying upon the person's concern about their personal accounts and information.

*Every day, roughly…*

- *156 million phishing emails are sent globally*
- *16 million make it through filters*
- *8 million are opened*
- *800,000 links are clicked*
- *80,000 fall for a scam every day and share their personal information*

***Don't take the bait!***

The B.C. government firewalls are constantly being updated to block evolving phishing attempts and spam. Unfortunately, phishing email does arrive in

employee's Inboxes despite these efforts, and because of this, some employees believe they must be legitimate emails. Making matters worse, most phishing/spam emails originate from the account of someone who previously was phished and that individual's legitimate-looking email address was used without their knowledge.

The government will continue to receive refined, legitimate looking phishing emails that make it through the government email firewall. Don't be the one to get caught phishing! Be wary and take a moment to examine unsolicited email. Hover your cursor over the links just to see if they show the same in the viewing box. You can also copy and paste a link into a new browser window to see what comes up. A phishing email will usually have a tone of urgency and will ask the recipient to take some action – usually by clicking on a link or opening an attachment. Recent phishing emails have pretended to be from system administrators advising users that they have exceeded the space available on their computer. Other recent phishing emails appear as if they are from PayPal, Canada Post, UPS, Apple or one of the banks. The emails urge the recipient to act now or there will be a negative consequence such as cancellation of their accounts. Some emails will offer a positive outcome, such as a prize.

There are other methods of phishing to be aware of:

- Spear Phishing is the targeted version with attacks that are customized to the recipient, usually corporate executives, and include details only an insider would know.
- SMS Phishing or Smishing uses cell phone or smartphone text messages.
- Vishing scams make use of Voice over Internet Protocol (VoIP) which allows people to talk over their computer lines (e.g., Skype or FaceTime). The criminals leave an automated message saying the person's credit card or account has been compromised, and to call a number for information. The Caller ID can be altered to appear that it comes from a legitimate source.

Remember that there is no business reason for anyone in the B.C. government, including a Help Desk, or any financial institution or online account to contact you and ask you to provide name, account numbers, passwords or any other personal or financial information. Do not click on any links, and do not open attachments – these are vehicles for hackers to install malware. Do not respond in any way and Delete the email. Do not click on 'Unsubscribe' as it lets spammers know they hit a live address. If you think the email might be valid, contact the company directly by phone. Never disclose your IDIR password to anyone! If you think you have inadvertently responded to one, do not worry about feeling embarrassed - contact the Shared Services BC (SSBC) Service Desk at 250 387-7000 or toll-free at 1-866-660-0811 and select Option 3. Reporting could prevent the spread of further emails or potential damage.

## Spam

Spam emails (the electronic version of 'junk' mail) represent the vast majority of emails sent world-wide on any given day. There are constant reports of B.C. government employees receiving spam email which was not blocked by spam filters. Internet hoax emails are spam, as are offers of loans and mass marketing emails trying to sell goods at great prices that are counterfeit (e.g., prescription drugs without a prescription, designer goods such as purses, shoes and jewellery, and even anti-virus software and college diplomas). Spam emails are almost always offers that are "too good to be true", which should serve as a warning in itself. It is usually because of these

*Of the 33,096,355 emails coming into the B.C. government network in the month of October 2013 - 23,509,265 (71%) were identified as **Spam** and blocked at the Internet Gateway.*

claims, however, that people are fooled and robbed via spam emails. Never click on links in these emails. Spam email should be Deleted without opening, and never forwarded to others. (Use the Auto Preview or Reading Pane features in View to peek at an email without opening it.)

## Text Spam

As technology continues to evolve and offer more features for consumers, new threats and risks emerge. The rapidly growing popularity of hand-held devices has spawned "mobile marketing" using cell phones and smartphones. The success of this new mobile cybercrime, as with other forms of fraud, depends upon our naturally trusting nature and our tendency to be in a hurry. The results for the user can be unwanted charges on your bill, unwanted text messages, and the potential for your device to be infected with malicious code that can steal your information and continue to cause harm.

Text spam usually comes in the form of fun things like quizzes and games. Recipients respond to a text or enter a code, after which they become a subscriber and can find "third party charges" for "premium services" that are outside of an unlimited or fixed incoming text plan. B.C. government employees have innocently texted a response on their work device that resulted in unauthorized charges on their bills. The charges can come repeatedly and cost anywhere from 10 cents to 25 dollars each time and show as premium services.

If the price plan on your government-issued cell phone or smartphone includes text messaging, incoming text messages are free, however, these plans usually exclude premium messages (roaming, international, alerts, contests and promotions). If you do receive a spam message simply text the 10 digit number of the received message to short code 7726 (SPAM) – this works for all cell service providers.

Another form of smartphone spam is a phone number with an unfamiliar area code or prefix. An automated message might tell the user to just hit a number to go to a website and receive some reward. Entering the number is the same as clicking on a link in a phishing email – it can result in the capture of your information, future charges on your bill, and possibly the installation of malicious code or malware on your device.

## Internet Hoaxes

Internet Hoaxes are the email equivalent of chain letters (i.e., send to ten other people for good luck) and unwanted junk mail sent in bulk through the postal system. These emails are successful because they are very manipulative and prey upon the trusting emotions of the victims. The goals in sending these emails are to install malicious code and/or to capture personal and financial information or the names and email addresses of the recipient's contacts when the email is forwarded.

Hoax emails contain messages that are typically untrue and commonly contain warnings about computer viruses or supposedly hazardous products or they present tragic stories or pleas for financial assistance. These emails often appear following a natural disaster, soliciting money to help those affected. You might receive an email saying you have won a lottery or contest you did not enter, or have a large inheritance in another country. They can even contain positive messages to pass along to inspire other people. Do not click on any links in these emails. In the B.C. government, it is a violation of Information Security Policy to forward these emails to other employees or to your personal contacts.

# SECURITY TIPS FOR EMPLOYEES

## Protect Your Workstation

The B.C. government network is protected by up-to-date anti-virus software that provides protection from the various forms of malware described in Appendix A, such as rootkits and botnets. Because this is being done by information technology specialists, you may not have to worry about this aspect of computer security at work. You should, however, 'Restart' your computer at the end of the day so the network can push any new updates, especially security patches or fixes, to your computer.

Lock your computer every time you leave your desk. This will prevent unauthorized users from accessing either your personal systems or the government network, and prevent others from reading your screen. In some offices, you may be required to Log Off your computer when you are away from your desk. Ask your manager for clarification.

Whenever possible, ensure your computer is powered up and connected to the network at the end of the day for system updates and patches.

*To **Lock** your computer:*

- *Click the **Start button** in the bottom left corner, click on the **arrow** to the right of Shut down, then choose **Lock***

***OR:***

- *Press **Ctrl, Alt and Delete**, then choose **Lock this computer** from the list on your screen*

***OR:***

- *Press the **Windows key** and **L key** to Lock your workstation*

## Protect Your IDIR Account

Individuals require authorization in the form of an IDIR account to gain access to the B.C. government network. Your IDIR account is your government user ID (an abbreviation of your name) which in combination with your password provides a secure single sign-on that is unique to you. They are your "credentials" and you have responsibility for actions taken using those credentials.

It is essential that you protect your IDIR ID/password combination. If someone gets this information, they have access to everything that you have access to, which includes the government network. Serious harm could come to the government and its assets, so treat the protection of this information very diligently.

## Protect Your Passwords

User IDs and passwords are personal and confidential and must not be divulged to anyone, for any reason. Your password must be known only to you, and be complex enough that it cannot be easily guessed. B.C. government Information Security Policy states that *you are not permitted to share your IDIR ID and password with anyone, not even your co-workers, support staff or manager*. The most common reasons given for sharing user ID and password information is to enable someone to access another employee's files, to act on their behalf, or to perform a task that has been delegated. Tools such as shared drives and permissions, are available to enable employees to properly delegate authority to another employee. These tools all have appropriate security controls and audit trails in place to protect you. Contact your Ministry Information Security Officer.

As a B.C. government employee, if you ever receive a phishing email designed to trick you into providing your IDIR ID and password – Delete it, as there is no business reason for anyone in the B.C. government to phone or send you an email asking for this information. If such an email is addressed from another government employee, that person likely was a victim of a successful phishing attack. Do not contact that person.

There are some circumstances in which you should report a spam or phishing email:

- when it appears to come from a government source
- when it is threatening
- if you clicked on a link or attachment
- if you disclosed your IDIR ID and password

In these cases, spam/phishing emails should be reported as an Information Incident by calling the Shared Services BC Service Desk at 250 387-7000 or toll-free at 1-866-660-0811 (available 24 hours a day), and selecting Option 3.

You are accountable for all actions performed using your IDIR ID and password. It is your password - Keep it Secret and Keep it Safe. Do not write it down. If you are asked for the use of your password, or someone offers you their password to access their account, remind that person (including your 'boss') it is a security risk and a violation of the Information Security Policy. Don't be afraid to say 'No'. Tools are available for delegating.

Do not use your B.C. government password on your home computer or personal devices. It is good computing practice to use different passwords for various accounts on your home computer and mobile devices, so that anyone obtaining your password will not have access to all your accounts.

B.C. government network passwords automatically expire after 90 days. You will receive an automatic notification prompting you to change your password, beginning 14 days before it expires. If you do not want to change your password at that time, you can close the notice but you will receive further reminders and must change your password before it expires.

You can also change your password at any time by pressing **Ctrl**, **Alt** and **Delete** and selecting **Change Your Password**. It is advised that you change your password after travelling with your B.C. government-issued devices (laptop, tablet or cell/smartphone), especially if you were out of the country.

When you create your password, follow these rules:

- Minimum length is 8 characters.
- Must contain at least one character from 3 of the 4 categories below:
  - English upper case characters (A-Z)
  - English lower case characters (a-z)
  - Base 10 digits (0-9)
  - Symbols ($,#,*,%).

More discussion on the importance of passwords can be found at:
http://www.cio.gov.bc.ca/cio/informationsecurity/isawareness/idir_passwords.page
and Chapter 7.3.1, Information Security Policy at:
http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf

## Protect Your Workplace

Developing and implementing security-conscious work habits will reduce the likelihood of someone seeing business information they should not. Security-conscious work habits include:

- ensuring only documents required for current work are removed from file cabinets
- covering up, filing or storing confidential or personal paper documents when visitors are present in the work area
- clearing, changing or turning off the computer screen (e.g., minimize open windows) when people without authorization are close by
- using privacy screens on your monitor to reduce the angle that your monitor can be viewed from by other people
- Locking your workstation when you are away from your desk so that sensitive information is not displayed, and no one can access your computer
- not discussing confidential or personal client or business information in open work spaces or public areas
- clearing desktops and work areas when you plan to be away from the office
- securing documents and portable storage devices in a locked desk or file cabinet and storing the key in a safe place
- ensuring that outgoing and incoming postal mail is appropriately secured
- locking doors and windows
- checking fax machines and printers to ensure that no confidential or personal information is waiting to be picked up

If you need to discard any personally identifiable information, or drafts of any confidential government documents, do not place them in an open recycling container. Use one of the locked records destruction bins provided in many offices for record shredding, or alternatively, use an office shredder (cross-cut shredders are preferable and many of these also shred compact disks).

Also be aware of people who walk through your work area. A popular and simple form of social engineering is for strangers to show up and talk their way into a secured office area or storage room by pretending to be authorized workers. Another popular way for outsiders to access a secure area is to 'tailgate' or follow someone through an entry point. If you do not recognize someone, do not hesitate to ask who they are and ask to see their credentials. It is easy to make the assumption that the person is there to meet with someone in your office premises. Don't be afraid to ask questions – it shows that you are security conscious!

# GENERAL INFORMATION

## Installing Software on Your Government Computer

B.C. government policy prohibits employees from installing unlicensed, unauthorized or non-work-related software onto their government-issued computers, laptops, tablets or mobile devices. The Windows 7 operating system image potentially has given employees a change in security settings with a newer set of tools for conducting their work, all intended to offer users more flexibility and ease of use. This change in settings gives local administrator privileges to users which permits them to load software and change system settings.

The change with Windows 7 involves a relaxing of certain restrictions which result in an increased requirement for ministries and end users to be aware of and manage some additional security risk. With this privilege comes the responsibility of the individual user to know and to practice safe computing behaviour and to follow government's policies and procedures.

Even though you may now be able to download software and apps, it is *essential* that there is no increased risk of data loss and exposure of information. Users still need to have ministry approval to purchase and download non-standard software (meaning not available from government). Both a Privacy Impact Assessment (PIA) and a Security Threat and Risk Assessment (STRA) must be completed for any new applications (Apps). For additional information on the Windows 7 settings, go to:
https://gww.gov.bc.ca/wiki/items/windows-7-what-you-need-know
https://ssbc-client.gov.bc.ca/servicenews/service_bulletin_379.html (Installation of Windows 7)

It is important to point out that employees are not allowed to install file-sharing software programs that allow users to share music and/or videos. See Appendix B – Appropriate Use of Government Resources.

## Using B.C. Government Email

It is advisable to make sure you double-check the email address and attachments before sending email. When in a hurry, it is easy to accidentally click on the contact name or the file name listed above or below the one you wanted. This type of accident has resulted in personal, confidential and sensitive information going to the wrong destination, causing embarrassment to government and the need for a formal information security investigation. Make it a habit to open, then close, the attachment, and check the intended recipient's name and email address before hitting Send.

You may be able to encrypt the information, so that if the email is intercepted, the information is not accessible. Personal or confidential information can be placed in an encrypted attachment, rather than in the text of the email, where an approved encryption service is available. Other options to consider are registered mail services or personal/hand delivery. For advice on using different methods of transmission contact your Ministry Information Security Officer (MISO).

Since the B.C. Government Directory, with employee names, phone numbers and email addresses, is posted on a public website (and available by doing a search on your name), employees may receive unwanted spam email in the form of phishing attempts, internet hoaxes or mass marketing. The spread of Internet hoaxes via email is

one threat that you as an employee can stop. Do not forward hoax emails or chain letters to other employees or people you know outside of work. As mentioned previously, never click on a link or open an attachment in an unsolicited email. If you have any suspicions about an email, Delete it without opening.

Employees can access their B.C. government Outlook account remotely to connect to Email, Calendar, Contacts and Tasks from any computer, including some mobile devices, using their web browser and their IDIR ID and password. Use https://summer.gov.bc.ca.

Some employees have used their government email to send work documents to their home email address, to work on the file at home. This is not a security best practice and is discouraged, as the email could be intercepted, and the potential risk for data loss is too high. There are safe and approved alternatives available. See the upcoming section on Working Outside the Workplace.

## Accessing Personal Email

As a government employee, you are allowed to access your personal email accounts (e.g., @shaw, @yahoo, @gmail) over the Internet while at work in order to conduct reasonable personal affairs and to help foster work-life integration. It is important to follow the Standards of Conduct and the Appropriate Use Policy (see below).

## Using the Internet

*In 2012, 36% of the Security Investigations conducted by that Unit were related to the inappropriate use of IT resources.*

You do have access to the Internet as a government employee, but this does not mean that you can have unlimited access to visit websites. You are not allowed to visit any website that has inappropriate material, such as sexual content of any kind, racism, hate literature, or anti-government messages. Many of these types of sites are screened, and if an employee does attempt to visit one, a prominent "red screen" will appear on your monitor, saying that you are not permitted to view the site and access is blocked.

If you think you will want to access non-work-related websites during work hours, you will find the rules on Internet use in the Appropriate Use Policy at http://www.cio.gov.bc.ca/cio/appropriate_use/index.page.

## Using Portable Storage/Mobile Devices

Portable storage devices are compact devices with storage capacity that can be attached to a computer. They include USB drives (also called thumb drives, memory sticks, or USB sticks), removable or external hard drives, laptops, tablets, netbooks, CDs and DVDs, portable digital assistants (PDAs), BlackBerrys, iPhones/iPods and other smartphones, game consoles, some e-book readers and other types of media players.

B.C. government information, including presentations, must only be stored on government-approved portable storage devices. Your office manager can arrange for the purchase of portable storage devices that will encrypt sensitive or personal information to ensure protection from data loss, compromise or unauthorized disclosure. Information temporarily stored on a portable storage device should be transferred to the government network as soon as practicable and then the content fully deleted and wiped from the device.

For more information on the use and best practices for government-owned portable storage mobile devices, employees can refer to the following Information Security Tip article on @Work's Wikilumbia: https://gww.gov.bc.ca/wiki/items/government-owned-devices

The B.C. government, as part of its *Citizens @ the Centre* strategy, has been researching and analyzing the implications and options for future adoption of a Core Government Device Strategy that will provide more flexibility for employees. One of the objectives of the strategy is to allow for device choice. As of this writing, according to the Information Security Policy, employees are not permitted to use their own personal portable devices for work purposes, or to connect their personal devices to their work computer. While there are some examples of employees using their personal device for work purposes, usually as part of the development process, there is no approved policy or procedure in place to support Bring Your Own Device (BYOD).

Policy Summary No. 3, Portable Storage Devices, is available at:
http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/summaries/3_portable_storage_dev.pdf

Employees should also refer to the Working Outside the Workplace Policy:
http://www.cio.gov.bc.ca/cio/working_outside_workplace/index.page?

## Protecting Mobile Devices

You are responsible for protecting both the device itself and the information contained on the device. Every make and model of electronic device comes with built in safety and security features, outlined in a manual, usually available online from the manufacturer. It is the responsibility of the employee that is issued a mobile device to protect the information on it, by learning about the device itself and security best practices.

Be very conscious of where the device is at all times. Remember that the device can connect to the government network and has a hard drive that stores government information. Do not leave any mobile device unattended, e.g., on a work space or in your car, when you are not there and it can be stolen. Government-issued devices are regularly lost or stolen, with the number going up along with the increased use of mobile devices. In 2012, 29% of the investigations conducted by the Security Investigations Unit were related to lost or stolen devices, and the information contained on them.

## Reporting the Loss or Theft of Your Government Device

If the device is lost or stolen, follow the Information Incident Management Process and take action as soon as possible. You need to report the information incident immediately to your supervisor. The Information Incident Management Process was discussed at the beginning of this Guidebook (under What If There is an Information Security Breach (including a Privacy Breach). The documents, including the Report Form can be found at http://www.cio.gov.bc.ca/cio/information_incident/index.page.

You will need to complete a General Incident or Loss Report (GILR) in accordance with Core Policy and Procedures Manual, Chapter L. The directions and the link to the GILR form, which is available online, are on the Risk Management Branch and Government Security Office website at http://gilr.gov.bc.ca/.

## Protecting Information on Paper

While the emphasis in recent years has been on computer hacking and threats to electronic information security, theft of information in paper form continues to flourish. As an employee, your responsibility to protect information on paper is more important than ever, as criminals create new ways to perpetrate theft and fraud, particularly identity fraud. In the B.C. government, many programs and services are paper-based, not computer based. They often record clients' personal information on documents such as application forms and may have copies of personally identifiable information attached, such as birth certificates.

If you need to discard any personally identifiable information, or drafts of any sensitive government documents, put them in a shredder (if employees do this themselves) or a shredder receptacle (if you have pick-up service from a company), rather than putting documents in a recycle container. If people other than employees come through your work area, cover any sensitive information when you walk away from your desk, in the same way that you would lock your computer. Do not leave client or business papers, or any confidential, personal or sensitive documents on a fax, photocopier, or multi-function device – retrieve it promptly. Contact your ministry Records Management Officers for other guidelines.

## Classifying Information

An information security classification system is one of the critical components of good information security practices, because it assists everyone involved in determining the value and sensitivity of information as well as the protective measures to be applied.

In the absence of a classification system, there is a risk that:

- All information may be regarded as highly classified and the cost of the measures to protect the information would far exceed the value and sensitivity of the information; or
- Highly sensitive information is not sufficiently protected.

The B.C. government approved the Information Security Classification Standard in 2006 for implementation across government. In addition to the Standard, an implementation framework and supporting guidelines were developed. The Information Security Classification documents can be found at: http://www.cio.gov.bc.ca/cio/informationsecurity/classification/information_security_classification_framework.page.

An Information Security Classification online training module has been developed to assist with the use and application of the Information Security Classification Framework *(government login is required)*. The training incorporates practical exercises and includes references to other related resources, policies and standards. The link to the online training is https://infosecurity.gov.bc.ca/sps/isc-learn/default.aspx.

## Working Outside of the Workplace

The B.C. government has created the Working Outside the Workplace Policy, in recognition of the fact that there are increasing instances of employees wanting to use available technology to work from home. The Working Outside the Workplace Policy outlines the permission required and the best practices for employees to follow.

Where the employee has approval to use a home computer to connect to the government network, a Home Technology Assessment must first be completed and appropriate safety measures installed. Contact your

Ministry Information Security Officer to assist with the Home Technology Assessment. In this way, government can ensure that security weaknesses will be properly assessed and necessary actions taken.

It is also important to consider security on your home computer, to protect it from intrusion. The document Tip Sheet: How to Protect Your Home Computer provides information and resources of value to all computer users, even if they are not Working Outside the Workplace.

Here is the link to the Working Outside the Workplace Policy:
http://www.cio.gov.bc.ca/cio/working_outside_workplace/index.page
The Working Outside the Workplace Policy page has links to the Home Technology Assessment and the Tip Sheet: How to Protect Your Home Computer.

For employees who need remote access to the B.C. government network while working outside of the office on a regular basis can have an account set up for this purpose. The most commonly used remote access options are DTS and VPN. The DTS (Desktop Terminal Service) can be used on your personal or government-issued (SSBC provisioned) device. You must download the CITRIX client for use of DTS on your personal device. If you need access to your email, use of Microsoft Office, access to corporate web services (Time On Line, eForms) and access to shared files, DTS should be used. VPN (Virtual Private Network) is a popular option for employees who are not connecting to the government network, or those with SSBC provisioned devices who require access to unique software options. See the Shared Services BC site https://ssbc-client.gov.bc.ca/rao/OptionList.html for the complete list of remote access options.

# Reference Guide to Many of the Policies Related to Information Security

Appropriate Use Policy
http://www.cio.gov.bc.ca/cio/appropriate_use/index.page?

Information Security Policy (Version 2.1) and Policy Summaries
http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf
http://www.cio.gov.bc.ca/cio/informationsecurity/policy/isp_summaries.page

Information Incident Management Process http://www.cio.gov.bc.ca/cio/information_incident/index.page

Information Security Classification Standard, Framework and Guidelines
http://www.cio.gov.bc.ca/cio/informationsecurity/classification/information_security_classification_framework.page

General Incident or Loss Report (GILR) Online Report Form http://gilr.gov.bc.ca/

Working Outside the Workplace Policy, the Home Technology Assessment Form and How to Protect Your Home Computer http://www.cio.gov.bc.ca/cio/working_outside_workplace/index.page

**Other Resources**
References and links to source documents, other materials and websites have been provided throughout this Guidebook. You are also encouraged to visit the following websites:

Office of the Chief Information Officer: http://www.cio.gov.bc.ca/cio/index.page (external) and https://gww.cio.gov.bc.ca/ (internal)

Information Security Branch: http://www.cio.gov.bc.ca/cio/informationsecurity/index.page (external) and https://gww.cio.gov.bc.ca/services/security/default.htm (internal)

Legislation, Privacy and Policy Branch (for privacy legislation and information):
http://www.cio.gov.bc.ca/cio/priv_leg/lpp.page

Ministry Information Security Officers (MISOs)
http://www.cio.gov.bc.ca/cio/informationsecurity/MISO/MISORole.page

Ministry Chief Information Officers (MCIOs)
http://www.cio.gov.bc.ca/cio/about/governance/role_cio/mcio_contact_list.page

Information Security Tips articles on the @Work Wikilumbia site: https://gww.gov.bc.ca/wiki/topic/476

Security News Digest is a compilation of global news stories about current security breaches, threats, and research, and is available online at:
http://www.cio.gov.bc.ca/cio/informationsecurity/securitynewsdigest/securitynews_digest.page

# Appendix A – Short Descriptions of Various Types of Malware

**Viruses and Worms** – A computer virus is a computer program that can copy itself and infect a computer. A virus that replicates by resending itself as an e-mail attachment or as part of a network message is known as a worm. Both can delete or change files or overload networks.

**Trojans** – A Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do damage by installing a "backdoor", allowing outsiders to access and control your computer.

**Keyloggers** – A keylogger, sometimes called a keystroke logger or system monitor is a hardware device or small program that monitors each keystroke a user types on a specific computer keyboard (or an ATM or Interac/debit keypad), records everything that is typed (including passwords) and passes that information to outsiders (usually using Bluetooth or similar technology). Keyloggers can be purchased in retail stores and legally installed on home computers, for example, to monitor children's usage.

**Spyware** – Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet, spyware is programming that is put into a person's computer to secretly gather information about the user (such as what sites are visited) and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program on the computer.

**Rootkits** – A rootkit is a collection of tools (programs) that enables administrator-level access to a computer or computer network, and controls, attacks or gathers your information. They often run silently on computer systems and are generally not detected by anti-virus or anti-spyware software.

**Botnet** – A botnet is a number of computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. Any such computer is referred to as a zombie – in effect, a computer "robot" or "bot" that serves the wishes of a master Spam or virus originator. Most computers compromised in this way are home-based. Botnets are often installed because the user responds to a fraudulent request received via e-mail, or opens an e-mail attachment. (Storm and Conficker are both botnets that received media attention for the large number of computers they infected around the world.) Security researchers consider botnets to be the greatest threat to security because they can be spread to such a vast number of computers world-wide, remain dormant without the knowledge of the user, and controlled by a central person at their will.

**Back Door** – A back door is a feature programmers often build into programs to allow special privileges normally denied to users of the program, such as access to fix bugs. If hackers or others learn about a back door, the feature may pose a security risk.