BRITISH COLUMBIA

Office of the Chief Information Officer

Privacy and Information Sharing:

Awareness Training for Contractors and Services Providers

Course Manual

Contents

TRAINING PURPOSE

This course is specifically designed for Contractors and Service providers to the BC Government. It is intended to instil confidence in handling information incidents (including privacy breaches) and provide opportunities to explore best practices in information sharing.

The goal of this training is to:

- Promote a culture of awareness of responsible privacy and information sharing; and
- Develop capacity to respond effectively and correctly when information incidents (including privacy breaches) occur.

LEARNING OBJECTIVES

Upon completion, you will be able to:

1. Promote a culture of responsible information sharing and privacy management;
2. Understand information sharing, privacy policy and processes;
3. Recognize your role and responsibilities in information sharing and privacy management; and,
4. Realize when an information incident, including a privacy breach, has occurred and know how to manage it.

WELCOME PARTICIPANTS

Thank you for participating in this course.

Contractors and Service Providers play a pivotal part in preventing breaches and encouraging appropriate information sharing.

This course is called, Privacy and Information Sharing: Awareness Training for Contractors and Service Providers. It is an awareness course on the policies, process and best practices related to effective and appropriate information sharing, privacy, information integrity, and information incident management.

A privacy breach is any situation where personal information is collected, used, disclosed, accessed, disposed of or stored, either accidentally or deliberately, that is not authorized by the Freedom of Information and Protection of Privacy Act (FOIPPA).

Thank you for continuing to manage information and protect privacy properly.

We trust that you will learn something and enjoy the course.

Kindest regards, The Office of the Chief Information Officer

BRITISH
COLUMBIA

Office of the Chief
Information Officer

WHAT IS CONFIDENTIAL AND PERSONAL INFORMATION?

Confidential information: includes, but is not limited to:

- Cabinet confidences (e.g., a briefing note to Cabinet);
- Economic or financial information (e.g., information about a proposed administrative plan that has not yet been implemented or made public);
- Information harmful to intergovernmental relations (e.g., information received in confidence from another government);
- Third party business information, where its disclosure would harm the third party;
- Personal information, where its disclosure is not authorized by FOIPPA or another enactment.

Personal information is a type of confidential information, the collection, use, storage, disclosure and disposal of which is specified in legislation. Under the *Freedom of Information and Protection of Privacy Act* (FOIPPA)*,* "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, e-mail;
- Race, national/ethnic origin, colour, religious or political beliefs or associations;
- Age, sex, sexual orientation, marital status;
- Identifying number or symbol such as social insurance number or driver's license number;
- Fingerprints, blood type, DNA prints;
- Health care history;
- Educational, financial, criminal, employment history;
- Personal recommendations or evaluations, character references or personnel evaluations about the third party.

Each Contractor or Service provider is accountable for the protection of personal information in its custody or control.

When does confidential (including personal) information become sensitive?

All confidential (including personal) information is sensitive. The significance of designating information as sensitive depends on factors such as the value of the information and the probability and impacts of unauthorized use, alteration, loss or destruction. The cost for managing sensitive information (e.g., witness protection, adoption data) are likely to be significantly greater than that for other types of information (e.g., public or for internal use only information).

As a Contractor or Service Provider working for the Government of BC, you should be aware of the BC Government's security classification standards. Government uses an Information Security Classification Standard that has three security levels (high, medium or low) to classify and define information sensitivity. These security levels are consistent with risk classifications used in other areas of government.

Ministries are required to identify, categorize and protect information, based on the degree of damage that could reasonably be expected to result from compromise of the information. Each classification level signifies the potential level of risk or harm in the financial, personal, and operational aspects. Specifics will vary from ministry to ministry. Consult your government contract manager for more information.

WHAT ARE THE ROLES AND RESPONSIBILITIES?

Contractors and Service Providers have roles and responsibilities in the following areas:

1. **Information Sharing;**
2. **Working Outside of the Workplace; and**
3. **Managing Information Incidents.**

1. INFORMATION SHARING

Information is an asset that must be managed effectively and shared appropriately in order to realize its true value for British Columbians.

Information sharing creates a culture of collaboration and ultimately provides and promotes better service delivery to citizens; it addresses the complexities that distinct and "siloed" programs cannot.

Benefits of improved information sharing include:

- Consistent service delivery approaches – the public can expect the same or similar service no matter where they are receiving services from;
- Employees, particularly front-line workers who sometimes have to make Decisions about citizens' well-being quickly, have the information they need at the right time and for the right purpose;
- Appropriate integration of services and support for complex service delivery strategies to better meet the needs of clients, resulting in better outcomes and reduced risk to vulnerable persons;
- Policy and program development and evidence-based decision-making informed by best practice; and
- Efficiencies created by eliminating duplicative work, thereby saving money.

It is important for Contractors and Services Providers to embrace information sharing as a key objective so that:

- Information is treated and managed as an asset;
- Information sharing occurs in a privacy protective way; and
- Appropriate security and compliance measures are implemented.

Your Information Sharing Responsibilities:

- Communicate the benefits of information sharing within your organization.
- Set an example - share your knowledge and information with your colleagues.
- Ensure confidential (including personal) information is protected.
- Support information sharing initiatives within your organization and with other organizations as appropriate.
- Promote information sharing strategies and tools;
- Review existing relationships, within and outside of organizational boundaries to ensure information is leveraged as appropriate and to the greatest extent possible.
- If you are unsure of any information sharing proposals between your work unit and another - either inside or outside of your organization - contact your government contract manager

Assess Your Risks

Before sharing information within your organization or with another organization, the risks should be assessed and strategies created to mitigate those risks.

Contractors and Service Providers need to address the following foundational questions to gain valuable insight and visibility into their current information exposure risks, so they can proactively manage the risk in a coordinated approach. The information exposure assessment is a collaborative process. You may need to consider the following:

- What government data under your care is most critical and is sensitive information?
- What data retention policies apply?
- Do you have the legal authority to use and share this information for what purpose?
- What legislation and policy is governing use of the information?
- Where and how is this information being stored?
- What controls are in place to protect it?
- Which threats represent the greatest risk to safeguarding the government information in your custody?

2. WORKING OUTSIDE OF THE WORKPLACE

Wherever you work – whether at home, a hotel or another location outside your regular workplace – you need to be aware of BC Government policies in place to safeguard information.

The Working Outside of the Workplace Policy applies when remotely accessing digital information and handling sensitive materials outside of the workplace. Working remotely comes with specific responsibilities. As a Contractor or Service Provider, you must ensure you make arrangements with your supervisor or contract manager before removing confidential (including personal) information from the workplace. As a Contractor or Service Provider, you should reach agreement with your supervisor or contract manager on the following:

- Removing electronic or paper-based confidential (including personal) information from the workplace.
- Ensuring encryption of confidential (including personal) information in electronic form, when stored or transported outside the workplace.
- Overseeing the physical security of items and information while working outside the workplace when:

   a. travelling outside Canada;
   b. undertaking work in public areas; and
   c. mailing or couriering information.

There are three main ways to work outside the workplace which vary in degrees of security (check with your government contract manager with regard to any specific ministry policies around their use):

1. Using a government-issued computer such as a laptop/tablet is the most secure. Supervisor approval is required.
2. Using Desktop Terminal Services (DTS) and Remote Desktop Connection (RDC) with Virtual Private Network (VPN) is still very secure. Supervisor approval is required.
3. For web access to email, use *Summer*.

Remember, you should not open, download, or save to the local hard drive, or print confidential (including personal) information using the above methods. Doing so would create a copy that could be recovered.

Encrypted USB sticks (also called Flash or Jump Drives) should only be used for sensitive (including personal) information as a last resource. Sensitive (including personal) information should remain on a secure Local Area Network (LAN) or within the information system and be accessed using secure remote technology such as VPN or DTS.

When it comes to removing files or other papers with confidential (including personal) information - from the workplace - remember you first have to be authorized to do so. Any paper-based information used away from the office must be returned for shredding or storage. Refer to the following guides which can be found in the Working Outside of the Workplace (WOW) policy link below.

- *Home Technology Assessment Guide*
- *Information Incident Management Process*

Your Working outside of the Workplace Responsibilities

When preparing or allowing employees to work outside of the workplace, supervisors are responsible for the following:

- Approve any working outside the workplace arrangement(s) with staff.
- Provide direction on when and how to record confidential (including personal) information before it leaves the workplace.
- Ensure employees are aware of: where to find information and assistance to ensure the safeguarding of electronic and/or paper-based confidential (including personal) information when working outside of the workplace; and how to report an information incident.
- Communicate appropriate safeguarding, physical security and transportation measures of electronic and/or paper-based confidential (including personal) information, as included in this policy or established within the work area as a result of this policy.
- Ensure government-approved devices and tools are available for employees to securely transport and work with electronic and/or paper based confidential (including personal) information at alternative worksites.
- Undertake periodic reviews to ensure that employees are using appropriate handling and transportation methods.
- Ensure a Home Technology Assessment is completed and that any recommended updates are confirmed with the employee prior to using a home computer.

3. MANAGING INFORMATION INCIDENTS

Information Incident Management Role

Contractors and Services Providers are encouraged to develop a culture of prudent management of information. Supervisors and Managers in particular, have a primary role to ensure their employees understand their responsibilities to report all actual and suspected information incidents. Depending on the situation Contractors and Services Providers may be required to take action to contain the incident and/or recover the information that may be exposed.

Your Responsibilities in Managing Information Incidents

When it comes to information incident management, Contractors and Services Providers have the following responsibilities:

Report:

- To ensure that its employees, sub-contractors or any other person who discovers a suspected or actual information incident (including a privacy breach) immediately notify their supervisor or manager and report the incident to their government contract manager.

- Where the supervisor or manager is unavailable, to ensure the employee, service provider or other person immediately reports the information incident to their government contract manager.

- Where the government contract manager is unavailable or not able to be reached immediately, Contractors and Service Providers are required to immediately report the information incident by calling the Shared Services BC Service Desk at 250-387-7000 (toll-free: 1-866-660-0811), selecting option 3, and stating that they are reporting an information incident.

Recover:

- To take steps to recover confidential or personal information if possible, and to take additional action to contain the incident and lessen the impacts and implications for government and individuals.

  Note: If the incident involves government information technology, seek the direction of the government contract manager to seek the assistance of the Security Investigations and Forensics Unit before taking any containment steps.

Remediate:

- Take action to remediate and resolve the incident:
  - With the government contract manager as the incident owner;
  - By working collaboratively with the government contract manager, OCIO Investigator(s), and other members of the investigation team that may be involved (e.g. Ministry CIO)
  - By notifying individuals or parties affected by the incident, where and as directed by OCIO Investigator(s), and the government contract manager.

Prevent:

- Take steps and implement measures to prevent similar incidents from happening by:
  - Ensuring that employees know and understand how to apply changes in the handling of confidential or personal information;
  - Being diligent in the handling of confidential or personal information;
  - Implementing recommendations from the Information Incident Management Process; and reporting the results to the Chief Information Security Officer (Information Security Branch) and the Director of the Privacy Investigations Unit (Privacy and Legislation Branch);
  - Developing a culture for the prudent management of information, including by providing training; and
  - Ensuring employees understand their responsibility in reporting information incidents, including containing the loss and/or recovering the information.

RESPONDING TO INFORMATION INCIDENTS

Information incidents happen when privacy or information security is threatened. They don’t have to be large scale. Incidents happen anytime information is lost, stolen, accessed, used or modified in an unauthorized way. Information incidents are called privacy breaches when they involve personal information, such as names, birthdates, social insurance numbers, or client file details.

The *Information Incident Management Process* provides instruction on what to do in the event of a privacy breach or other information incident.

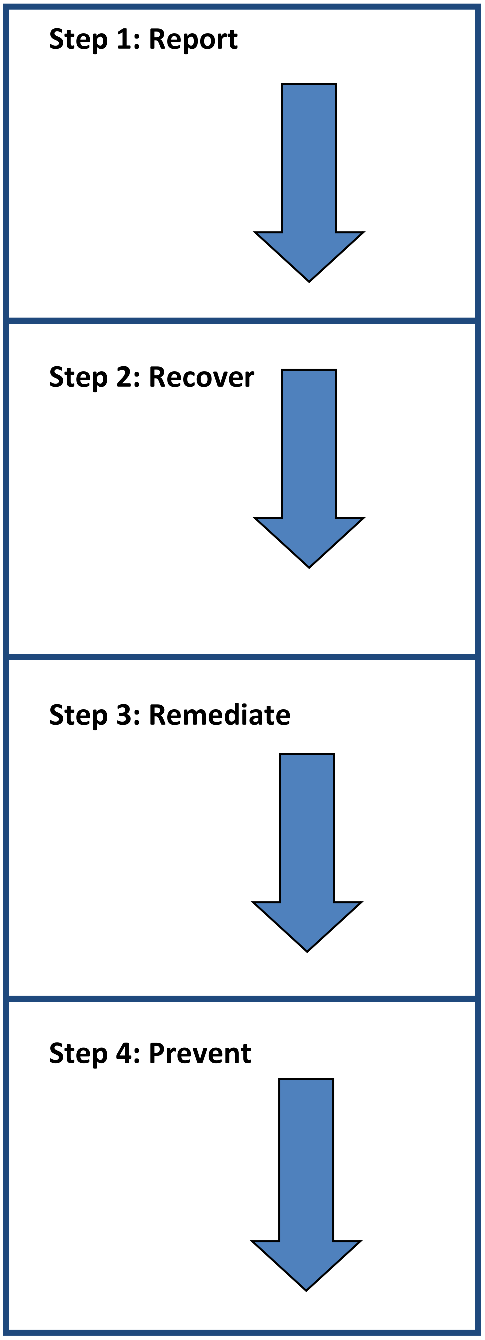
The *Process for Responding to Privacy Breaches* explains this process further. The*Information Incident Checklist* and *Easy Guide* (also on the next page) provide a high level reference to guide you through the process.

Always refer to the online versions of the policy and process to be sure you are working with the most up-to-date information.

Easy Guide for Responding to Information Incidents including Privacy Breaches

The **KEY** to responding to information incidents is to take action as soon as possible.
An **information incident** is a single, or series of unwanted or unexpected events, actual or suspected, that threaten privacy or information security.

Information incidents are also called **privacy breaches** when they involve personal information, such as names, birthdates, social insurance numbers, or client file information. The following easy steps (called the **3RP** for "report, recover, remediate and prevent") are intended to guide workers who encounter information incidents.


Step 1: Report

Step 2: Recover

Step 3: Remediate

Step 4: Prevent

Step 1: Report the information incident immediately to your contract manager or supervisor who will notify your government contract manager. If your manager or supervisor is not available, immediately report the incident to your government contract manager directly. If your government contract manager is not available, you must immediately notify the Office of the Chief Information Officer (OCIO) by dialing the Shared Services BC Service Desk at 250 387-7000 (toll-free: 1-866-660-0811) and selecting Option 3. You will be contacted by an OCIO Investigator, who will seek further details and may give advice on next steps.

Step 2: Recover the confidential or personal information if possible, or otherwise contain the incident to lessen the impacts for government and individuals. Appropriate actions are contextual but include recovering the information, records or equipment, correcting physical security, and isolating the activity that led to the incident. (Note: If the incident involves information technology, seek the direction of the Security Investigations and Forensics Unit before taking any steps).

Step 3: Remediate the information incident by working with your government contract manager, OCIO Investigators, and others to determine the specifics of the incident, to resolve it and, if necessary, to notify affected individuals.

Step 4: Prevent information incidents by making any needed changes to your processes, understanding your responsibilities, being diligent in the handling of all information and being an active participant in developing a culture of prudent information management.

PROCESS FOR RESPONDING TO PRIVACY BREACHES

1. Purpose

This document sets out the steps that must be followed when responding to a privacy breach. It must be read in conjunction with the *Information Incident Management Process*, which says:

1. The Government Chief Information Officer is responsible for the coordination, investigation, and resolution of information incidents.
2. All actual or suspected information incidents must be reported immediately to your government contract manager and to the Government Chief Information Officer, using the Information Incident Management Process.
3. The Government Chief Information Officer is solely responsible for liaising with the Office of the Information and Privacy Commissioner regarding an actual or suspected privacy breach.

2. What is a Privacy Breach and what is an Information Incident?

A **privacy breach** is a collection, use, disclosure, access, disposal, or storage of personal information, whether accidental or deliberate, that is not authorized by the Freedom of Information and Protection of Privacy Act.

A privacy breach is a type of information incident. **Information incidents** occur when unwanted or unexpected events threaten privacy or information security. They can be accidental or deliberate and include the theft, loss, alteration or destruction of information.

Other **definitions** can be found at the back of this course manual or in the*Information Incident Management Process*.

3. Process

All known or suspected privacy breaches require immediate remedial action, no matter the sensitivity of the personal information. Given the varied nature of privacy breaches, no "one-size-fits-all" response is possible, and actions are proportional and appropriate to each privacy breach.

The following steps are used to address privacy breaches. As the circumstances for each privacy breach vary, these steps might occur concurrently or in quick succession; they do not necessarily need to follow the order given below:

A. Report Immediately - Step 1 Report

Contractors and Service Providers must report privacy breaches immediately to their government contract manager. The government contract manager and/or employee (who discovered the breach), or their supervisor or manager must also immediately report the incident to the Office of the Chief Information Officer 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 and state that you are reporting a "privacy breach".

Where the government contract manager is unavailable, Contractors and Service Providers are responsible for immediately reporting the incident directly to the Office of the Chief Information Officer according to the above steps.

This will invoke the *Information Incident Management Process*.

Privacy breaches must also be reported to the Ministry Chief Information Officer.

B. Contain the Privacy Breach - Step 2 Recover

Employees, business owners (including Contractors and Service Providers) or others should take immediate action to contain the privacy breach and to limit its impact. Appropriate actions will depend on the nature of the breach and may include:

- Isolating or suspending the activity that led to the privacy breach;
- Correcting all weaknesses in physical security;
- Taking immediate steps to recover the personal information, records or equipment from all sources, where possible;
- Determining if any copies have been made of personal information that was breached and recovering where possible.

Note: Where the privacy breach involves information technology, the direction of the Security Investigations & Forensics Unit must be sought before taking any containment steps.

C. Assess the Extent and Impact of the Privacy Breach – Step 3 Remediate

As part of the Information Incident Management Process, business owners (including Contractors and Service Providers) or others will work with the Investigations Unit, Standing Response Team, Incident Response Lead, or others to determine the:

(i) Personal Information Involved

- What personal information has been breached?
- Is the personal information sensitive? Examples are health information, social worker case histories, social insurance numbers, financial information or information that can be used for identity theft. A combination of personal information is typically more sensitive than a single piece of personal information.

(ii) Cause and Extent of the Breach

- What was the cause of the breach?
- What programs and systems are involved?
- Is the personal information encrypted or otherwise not readily accessible?
- Has the personal information been recovered?
- What steps have already been taken to minimize the harm?
- Is this a one-time occurrence or an ongoing problem?

(iii) Individuals Affected by the Breach

- Who is affected by the breach? For example, employees, public, contractors, clients, service providers, other organizations.
- How many individuals are, or are estimated to be, affected by the breach?

(iv) Foreseeable Harm from the Breach

- What possible use is there for the personal information? Can the information be used for exploitation, fraud or other harmful purposes?
- Who is in receipt of the personal information? For example, a stranger who accidentally receives personal information and voluntarily reports the mistake is less likely to misuse the information than an individual suspected of criminal activity.
- Is there a relationship between the unauthorized recipient(s) and the data subject(s)? A close relationship between the two might affect the likelihood of harm.
- Is there a risk of significant harm to the individual as a result of the breach? For example:
    - security risk (e.g., physical safety);
    - identity theft or fraud;
    - access to assets or financial loss;
    - loss of business or employment opportunities;
    - breach of contractual obligations, hurt, humiliation, embarrassment, damage to reputation or relationships.

- Is there a risk of significant harm to the public body or organization as a result of the breach? For example:

- loss of public trust
- loss of assets
- financial exposure
- loss of contracts or business
- risk to public health
- risk to public safety

D. Document the Privacy Breach and Corrective Action Taken

As part of the Information Incident Management Process, Contractors and Service Providers will work with the government contract manager, the OCIO Investigators and others to:

1) ensure that evidence of the privacy breach is preserved; and
2) document the privacy breach in detail, including:

- what happened and when;
- how and when the privacy breach was discovered;
- the personal information involved and scope of the breach;
- who was involved, if known;
- individuals interviewed about the breach;
- whether the privacy breach has been contained and any lost personal information retrieved;
- who has been notified;
- the corrective action taken, including any steps to assist affected individuals in mitigating harm (for example, providing credit watch services if appropriate); and
- recommendations, including corrective action that still needs to be taken.

E. Consider Notifying Affected Individuals

The impact of privacy breaches must be reviewed to determine if it is appropriate to notify individuals whose personal information has been affected by the breach. As part of the Information Incident Management Process, the OCIO Incident Lead will work with the affected ministry so the ministry can decide how to notify affected parties and take other required actions, as appropriate.

(i) Notifying affected individuals

The key consideration in deciding whether to notify an affected individual is whether it is necessary to avoid or mitigate harm to an individual, such as:

- A risk of identity theft or fraud (usually because of the type of information that has been compromised such as SIN, banking information, identification numbers);
- A risk of physical harm (for example, if the compromised information puts an individual at risk of stalking or harassment);

- A risk of hurt, humiliation or damage to reputation (for example, when the compromised information includes medical or disciplinary records, criminal histories or family case files); or
- A risk to business or employment opportunities.

Other considerations in determining whether to notify individuals include:

- Legislative requirements for notification;
- Contractual obligations requiring notification;
- A risk of loss of confidence in the public body and/or good customer/client relations dictates that notification is appropriate.

(ii) When and how to notify

Contractors and Service Providers are responsible for notifying individuals or parties affected by the incident, where and as directed by the government contract manager, OCIO Investigators and others, as appropriate.

If it is determined that notification of individuals is appropriate:

- **When:** Notification should occur as soon as possible following the breach. (However, if law enforcement authorities have been contacted, it may be appropriate to work with those authorities in order to not impede their investigation.)
- **How:** Affected individuals should be notified directly – by phone, email, letter or in person – whenever possible. Indirect notification using general, non-personal information should generally only occur when direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of notification – website publication, posted notices, media – in certain cases may be the most effective approach.

(iii) What should be Included in the notification

Notifications should include the following information, as appropriate:

- Date of the breach.
- Description of the breach (extent).
- Description of the information compromised.
- Risk(s) to individual caused by the breach.
- Steps taken to mitigate the breach and any harms.
- Next steps planned and any long-term plans to prevent future breaches.
- Steps the individual can take to further mitigate the harm or steps the public body has taken to assist the individual in mitigating harm. For example, how to contact credit reporting agencies to set up a credit watch, or information explaining how to change a personal health number or driver’s licence.

- Contact information of an individual within the public body or organization who can answer questions or provide further information.
- The right to complain to the Office of the Information and Privacy Commissioner and the necessary contact information. If the public body has already contacted the Commissioner's office, include this detail in the notification letter.

Notifications should not include the following information:

- Personal information about others or any information that could result in a further privacy breach.
- Information that could be used to circumvent security measures.
- Information that could prompt a misuse of the stolen information (for example, if hardware was stolen for simple 'wiping and resale', but the breach notification prompts someone to realize that personal information is on the hardware and could be of some value if accessed).

F. Inform Other Parties as Appropriate

As part of the Information Incident Management Process, the Incident Response Lead will work with the affected ministry so the ministry can notify affected parties and take other required actions, as appropriate. Affected parties may include, for example: insurers, professional or other regulatory bodies, third-party contractors, internal business units, or unions.

The Government Chief Information Officer is solely responsible for liaising with the Office of the Information and Privacy Commissioner regarding an actual or suspected privacy breach.

The following factors are relevant in determining whether to report a privacy breach to the Office of the Information and Privacy Commissioner:

- The sensitivity of the personal information;
- Whether the breached information could result in identity theft or other harm, including pain and suffering or loss of reputation;
- A large number of people are affected by the breach;
- The information has not been fully recovered;
- The breach is the result of a systemic problem or a similar breach has occurred before.

G. Prevent Future Privacy Breaches – Step 4 Prevent

Business owners (including supervisors and Service Providers) or others will work with the government contract manager, OCIO Investigators and others to investigate and recommend improvements resulting from the privacy breach.

Government, the ministry, and/or Contractors and Service Providers will, as applicable, implement recommendations in accordance with the Information Incident Management Process.

TOOLS AND RESOURCES

Supporting the policy statements are various tools and resources, including checklists and "guidelines." These additional tools serve to support and expand on information contained in the policy statements. While policy statements include high level mandatory requirements, guidelines and checklists offer guidance and recommended approaches, based on sound management and best practices.

Relevant Policy and Legislation

Legislation that applies to information management - Found at www.bclaws.ca

Freedom of Information and Protection of Privacy Act **(FOIPPA)** – applies to all "public bodies" (such as ministries, local governments, universities and hospitals and professional governing bodies) in BC and to service providers to public bodies in BC. It allows for access to information held by public bodies and determines how they may collect, use and disclose personal information.

Personal Information Protection Act **(PIPA)** – sets out how private organizations (including businesses, charities, associations and labour organizations) may collect, use and disclose personal information. BC's PIPA applies to commercial activity within BC (non-federally regulated business) as PIPA is deemed substantially similar to PIPEDA. But activity over borders by those same non-federally regulated business may be caught by PIPEDA.

Document Disposal Act **(DDA)** – establishes the rules and structures under which government creates, classifies, manages and destroys records under its custody and/or control.

Electronic Transactions Act **(ETA)** – establishes the criteria and conditions under which government will receive and use information in an electronic format and provides legal status to information supplied to government in an electronic format. Provides equivalence for paper and electronic records and establishes commonality within Canada for documents needed for inter- provincial trade.

Canada's ***Access to Information Act*** and also the ***Privacy Act*** are the federal equivalents to the BC FOIPPA (access and privacy obligations for federal government institutions and the federally regulated institutions).

Canada's ***Personal Information Protection and Electronic Documents Act (PIPEDA) -*** applies to federal works, undertakings or businesses (banks, airlines, and telecommunications companies); applies to the collection, use and disclosure of personal information in the course of a commercial activity and across borders.

Ministry specific acts may also include requirements for the management of certain types of information, e.g., *Adoption Act.* Contact your government contract manager for more information on how specific legislation may affect sharing information in your organization or business area.

Privacy Protection and Contractors

When Contractors and Service Providers are handling personal information, it is their responsibility to ensure that they comply with the terms and conditions outlined in the General Services Agreement (GSA) - Schedule E Privacy Protection.

Schedule E Privacy Protection – General Services Agreement (GSA)

This Schedule forms part of the agreement between Her Majesty the Queen in right of the Province of British Columbia represented by____ (the "Province") and _______________________________________ (the "Contractor") respecting ____ (the "Agreement").

Definitions

1. In this Schedule,

   (a) "**access**" means disclosure by the provision of access;
   (b) "**Act**" means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as amended from time to time;
   (c) "**contact information**" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
   (d) "**personal information**" means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Province and the Contractor dealing with the same subject matter as the Agreement but excluding any such information that, if this Schedule did not apply to it, would not be under the "control of a public body" within the meaning of the Act.

Purpose

2. The purpose of this Schedule is to:
   (a) enable the Province to comply with its statutory obligations under the Act with respect to personal information; and
   (b) ensure that, as a service provider, the Contractor is aware of and complies with its statutory obligations under the Act with respect to personal information.

Collection of personal information

3. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

4. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.

5. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:

   (a) the purpose for collecting it;
   (b) the legal authority for collecting it; and
   (c) the title, business address and business telephone number of the person designated by the Province to answer questions about the Contractor's collection of personal information.

Accuracy of personal information

6. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Province to make a decision that directly affects the individual the information is about.

Requests for access to personal information

7. If the Contractor receives a request for access to personal information from a person other than the Province, the Contractor must promptly advise the person to make the request to the Province unless the Agreement expressly requires the Contractor to provide such access and, if the Province has advised the Contractor of the name or title and contact information of an official of the Province to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Correction of personal information

8. Within 5 business days of receiving a written direction from the Province to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.

9. When issuing a written direction under section 8, the Province must advise the Contractor of the date the correction request to which the direction relates was received by the Province in order that the Contractor may comply with section 10.

10. Within 5 business days of correcting or annotating any personal information under section 8, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Province, the Contractor disclosed the information being corrected or annotated.

11. If the Contractor receives a request for correction of personal information from a person other than the Province, the Contractor must promptly advise the person to make the request to the Province and, if the Province has advised the Contractor of the name or title and contact information of an official of the Province to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Protection of personal information

12. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Storage and access to personal information

13. Unless the Province otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

Retention of personal information

14. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Province in writing to dispose of it or deliver it as specified in the direction.

Use of personal information

15. Unless the Province otherwise directs in writing, the Contractor may only use personal information if that use is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

Disclosure of personal information

16. Unless the Province otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Province if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

17. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

Notice of foreign demands for disclosure

18. In addition to any obligation the Contractor may have to

provide the notification contemplated by section 30.2 of the Act, if in relation to personal information in its custody or under its control the Contractor:

(a) receives a foreign demand for disclosure;
(b) receives a request to disclose, produce or provide access that the Contractor knows or has reason to suspect is for the purpose of responding to a foreign demand for disclosure; or
(c) has reason to suspect that an unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure

the Contractor must immediately notify the Province and, in so doing, provide the information described in section 30.2(3) of the Act. In this section, the phrases "foreign demand for disclosure" and "unauthorized disclosure of personal information" will bear the same meanings as in section 30.2 of the Act.

Notice of unauthorized disclosure

19. In addition to any obligation the Contractor may have to provide the notification contemplated by section 30.5 of the Act, if the Contractor knows that there has been an unauthorized disclosure of personal information in its custody or under its control, the Contractor must immediately notify the Province. In this section, the phrase "unauthorized disclosure of personal information" will bear the same meaning as in section 30.5 of the Act.

Inspection of personal information

20. In addition to any other rights of inspection the Province may have under the Agreement or under statute, the Province may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

Compliance with the Act and directions

21. The Contractor must in relation to personal information comply with:

    (a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the commissioner under the Act; and
    (b) any direction given by the Province under this Schedule.

22. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

Notice of non-compliance

23. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Province of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

24. In addition to any other rights of termination which the Province may have under the Agreement or otherwise at law, the Province may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

25. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.

26. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply

with this Schedule.

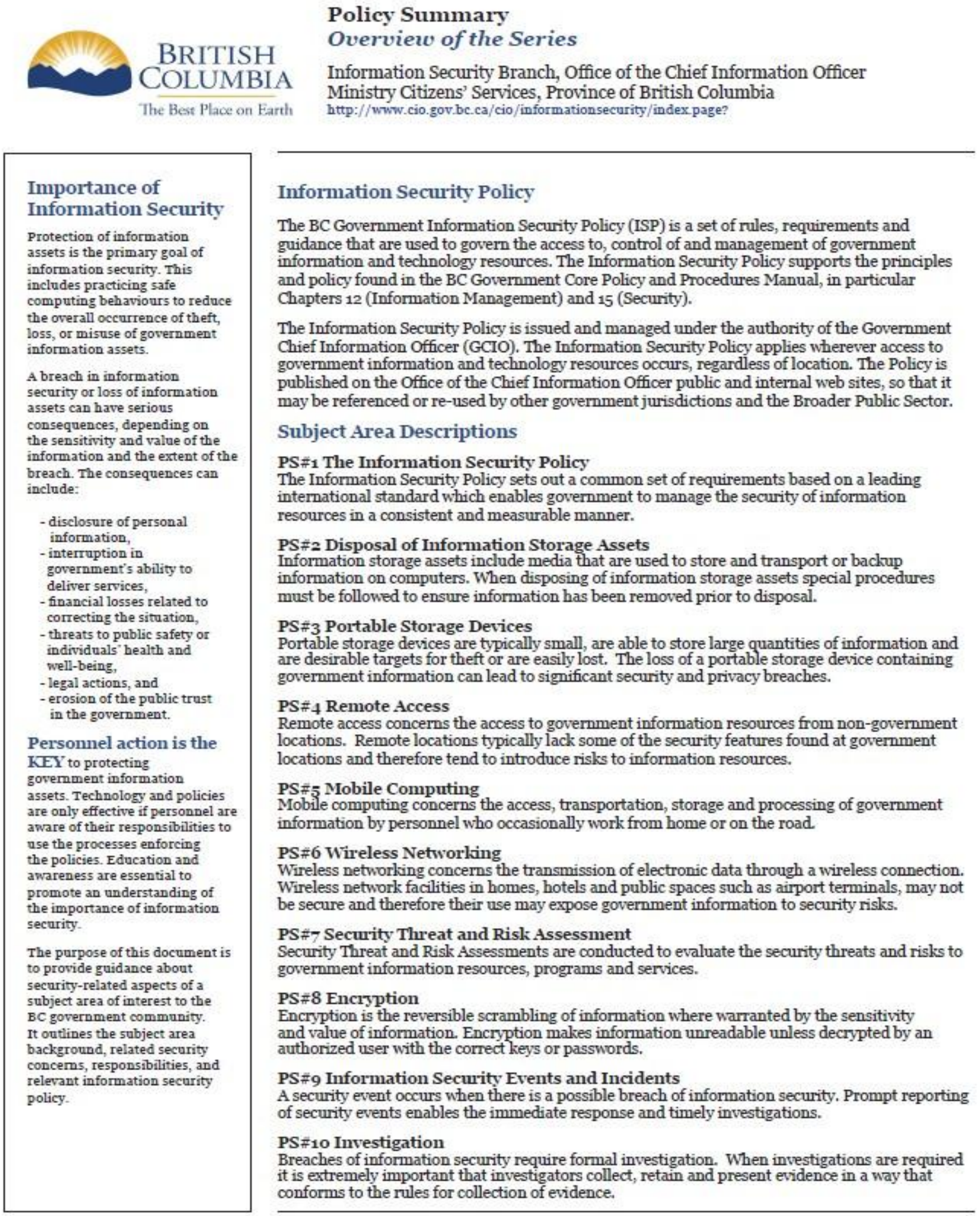
27. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.

28. If a provision of the Agreement (including any direction given by the Province under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.

29. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or, subject to section 30, the law of any jurisdiction outside Canada.

30. Nothing in this Schedule requires the Contractor to contravene the law of any jurisdiction outside Canada unless such contravention is required to comply with the Act.

Information Security Policy Summary: Overview of the Series



BRITISH COLUMBIA
The Best Place on Earth

Policy Summary
Overview of the Series

Information Security Branch, Office of the Chief Information Officer
Ministry Citizens' Services, Province of British Columbia
http://www.cio.gov.bc.ca/cio/informationsecurity/index.page?

Importance of Information Security

Protection of information assets is the primary goal of information security. This includes practicing safe computing behaviours to reduce the overall occurrence of theft, loss, or misuse of government information assets.

A breach in information security or loss of information assets can have serious consequences, depending on the sensitivity and value of the information and the extent of the breach. The consequences can include:

- disclosure of personal information,
- interruption in government's ability to deliver services,
- financial losses related to correcting the situation,
- threats to public safety or individuals' health and well-being,
- legal actions, and
- erosion of the public trust in the government.

Personnel action is the KEY to protecting government information assets. Technology and policies are only effective if personnel are aware of their responsibilities to use the processes enforcing the policies. Education and awareness are essential to promote an understanding of the importance of information security.

The purpose of this document is to provide guidance about security-related aspects of a subject area of interest to the BC government community. It outlines the subject area background, related security concerns, responsibilities, and relevant information security policy.

Information Security Policy

The BC Government Information Security Policy (ISP) is a set of rules, requirements and guidance that are used to govern the access to, control of and management of government information and technology resources. The Information Security Policy supports the principles and policy found in the BC Government Core Policy and Procedures Manual, in particular Chapters 12 (Information Management) and 15 (Security).

The Information Security Policy is issued and managed under the authority of the Government Chief Information Officer (GCIO). The Information Security Policy applies wherever access to government information and technology resources occurs, regardless of location. The Policy is published on the Office of the Chief Information Officer public and internal web sites, so that it may be referenced or re-used by other government jurisdictions and the Broader Public Sector.

Subject Area Descriptions

PS#1 The Information Security Policy
The Information Security Policy sets out a common set of requirements based on a leading international standard which enables government to manage the security of information resources in a consistent and measurable manner.

PS#2 Disposal of Information Storage Assets
Information storage assets include media that are used to store and transport or backup information on computers. When disposing of information storage assets special procedures must be followed to ensure information has been removed prior to disposal.

PS#3 Portable Storage Devices
Portable storage devices are typically small, are able to store large quantities of information and are desirable targets for theft or are easily lost. The loss of a portable storage device containing government information can lead to significant security and privacy breaches.

PS#4 Remote Access
Remote access concerns the access to government information resources from non-government locations. Remote locations typically lack some of the security features found at government locations and therefore tend to introduce risks to information resources.

PS#5 Mobile Computing
Mobile computing concerns the access, transportation, storage and processing of government information by personnel who occasionally work from home or on the road.

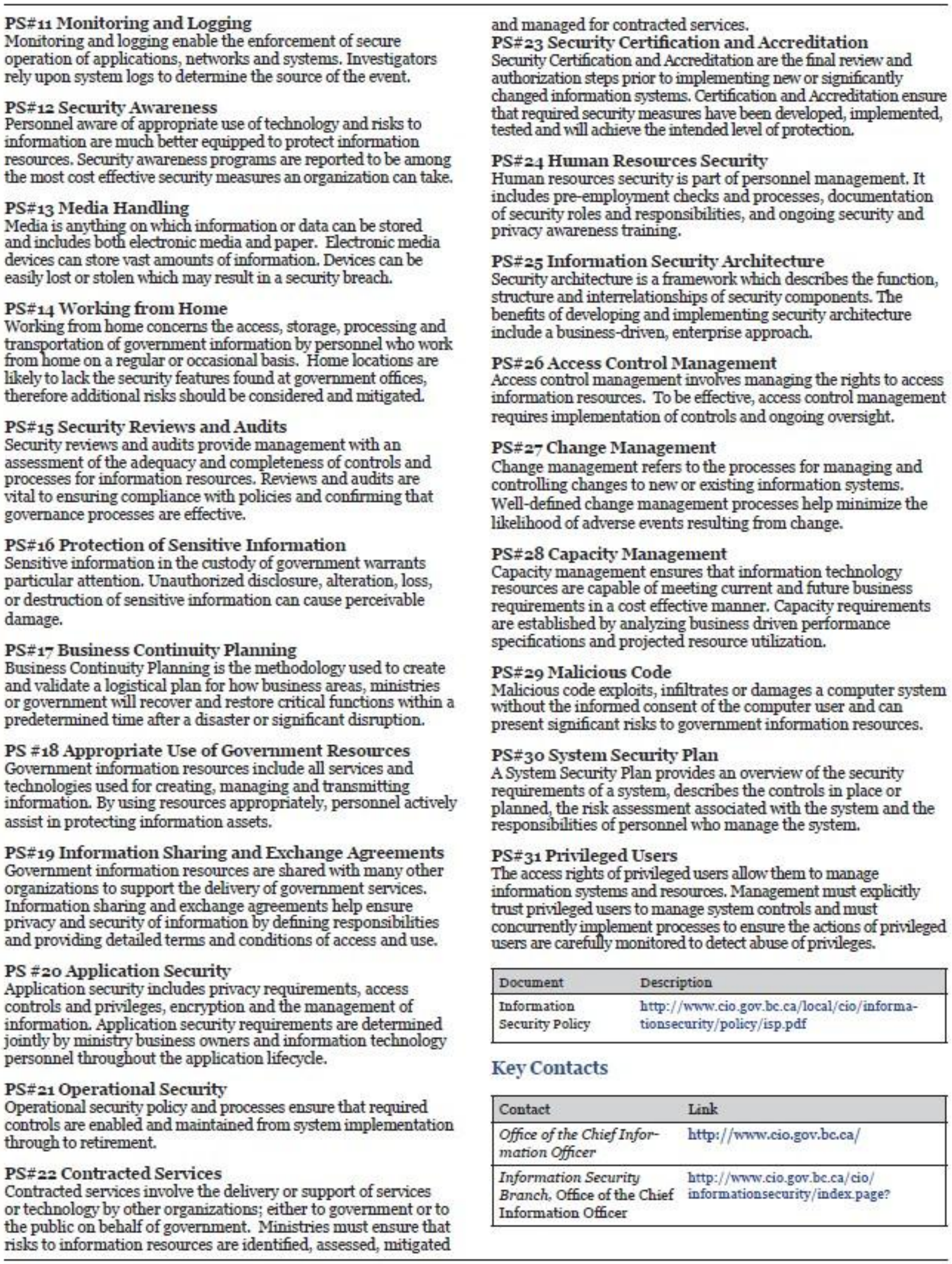
PS#6 Wireless Networking
Wireless networking concerns the transmission of electronic data through a wireless connection. Wireless network facilities in homes, hotels and public spaces such as airport terminals, may not be secure and therefore their use may expose government information to security risks.

PS#7 Security Threat and Risk Assessment
Security Threat and Risk Assessments are conducted to evaluate the security threats and risks to government information resources, programs and services.

PS#8 Encryption
Encryption is the reversible scrambling of information where warranted by the sensitivity and value of information. Encryption makes information unreadable unless decrypted by an authorized user with the correct keys or passwords.

PS#9 Information Security Events and Incidents
A security event occurs when there is a possible breach of information security. Prompt reporting of security events enables the immediate response and timely investigations.

PS#10 Investigation
Breaches of information security require formal investigation. When investigations are required it is extremely important that investigators collect, retain and present evidence in a way that conforms to the rules for collection of evidence.



PS#11 Monitoring and Logging

Monitoring and logging enable the enforcement of secure operation of applications, networks and systems. Investigators rely upon system logs to determine the source of the event.

PS#12 Security Awareness

Personnel aware of appropriate use of technology and risks to information are much better equipped to protect information resources. Security awareness programs are reported to be among the most cost effective security measures an organization can take.

PS#13 Media Handling

Media is anything on which information or data can be stored and includes both electronic media and paper. Electronic media devices can store vast amounts of information. Devices can be easily lost or stolen which may result in a security breach.

PS#14 Working from Home

Working from home concerns the access, storage, processing and transportation of government information by personnel who work from home on a regular or occasional basis. Home locations are likely to lack the security features found at government offices, therefore additional risks should be considered and mitigated.

PS#15 Security Reviews and Audits

Security reviews and audits provide management with an assessment of the adequacy and completeness of controls and processes for information resources. Reviews and audits are vital to ensuring compliance with policies and confirming that governance processes are effective.

PS#16 Protection of Sensitive Information

Sensitive information in the custody of government warrants particular attention. Unauthorized disclosure, alteration, loss, or destruction of sensitive information can cause perceivable damage.

PS#17 Business Continuity Planning

Business Continuity Planning is the methodology used to create and validate a logistical plan for how business areas, ministries or government will recover and restore critical functions within a predetermined time after a disaster or significant disruption.

PS #18 Appropriate Use of Government Resources

Government information resources include all services and technologies used for creating, managing and transmitting information. By using resources appropriately, personnel actively assist in protecting information assets.

PS#19 Information Sharing and Exchange Agreements

Government information resources are shared with many other organizations to support the delivery of government services. Information sharing and exchange agreements help ensure privacy and security of information by defining responsibilities and providing detailed terms and conditions of access and use.

PS #20 Application Security

Application security includes privacy requirements, access controls and privileges, encryption and the management of information. Application security requirements are determined jointly by ministry business owners and information technology personnel throughout the application lifecycle.

PS#21 Operational Security

Operational security policy and processes ensure that required controls are enabled and maintained from system implementation through to retirement.

PS#22 Contracted Services

Contracted services involve the delivery or support of services or technology by other organizations; either to government or to the public on behalf of government. Ministries must ensure that risks to information resources are identified, assessed, mitigated and managed for contracted services.

PS#23 Security Certification and Accreditation

Security Certification and Accreditation are the final review and authorization steps prior to implementing new or significantly changed information systems. Certification and Accreditation ensure that required security measures have been developed, implemented, tested and will achieve the intended level of protection.

PS#24 Human Resources Security

Human resources security is part of personnel management. It includes pre-employment checks and processes, documentation of security roles and responsibilities, and ongoing security and privacy awareness training.

PS#25 Information Security Architecture

Security architecture is a framework which describes the function, structure and interrelationships of security components. The benefits of developing and implementing security architecture include a business-driven, enterprise approach.

PS#26 Access Control Management

Access control management involves managing the rights to access information resources. To be effective, access control management requires implementation of controls and ongoing oversight.

PS#27 Change Management

Change management refers to the processes for managing and controlling changes to new or existing information systems. Well-defined change management processes help minimize the likelihood of adverse events resulting from change.

PS#28 Capacity Management

Capacity management ensures that information technology resources are capable of meeting current and future business requirements in a cost effective manner. Capacity requirements are established by analyzing business driven performance specifications and projected resource utilization.

PS#29 Malicious Code

Malicious code exploits, infiltrates or damages a computer system without the informed consent of the computer user and can present significant risks to government information resources.

PS#30 System Security Plan

A System Security Plan provides an overview of the security requirements of a system, describes the controls in place or planned, the risk assessment associated with the system and the responsibilities of personnel who manage the system.

PS#31 Privileged Users

The access rights of privileged users allow them to manage information systems and resources. Management must explicitly trust privileged users to manage system controls and must concurrently implement processes to ensure the actions of privileged users are carefully monitored to detect abuse of privileges.

Document	Description
Information Security Policy	http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf

Key Contacts

Contact	Link
Office of the Chief Information Officer	http://www.cio.gov.bc.ca/
Information Security Branch, Office of the Chief Information Officer	http://www.cio.gov.bc.ca/cio/informationsecurity/index.page?

Definitions and Acronyms

1. **Confidential Information**: includes, but is not limited to:

   - Cabinet confidences (e.g., a briefing note to Cabinet);
   - Government economic or financial information (e.g., information about a proposed administrative plan that has not yet been implemented or made public);
   - Information harmful to intergovernmental relations (e.g., information received in confidence from another government);
   - Third party business information, where its disclosure would harm the third party;
   - Personal information, where its disclosure is not authorized by the FOIPPA or another enactment.

Examples of confidential information are defined in Sections 12 to 22 of the *Freedom of Information and Protection of Privacy Act Manual*.

2. **Government Information:** all recorded information, regardless of physical format, that is received, created, deposited or held by or in any ministry, agency, board, commission, Crown corporation, institution, committee or council reporting or responsible to the Government of British Columbia

3. **Government Records** include machine-readable records, data stored in information systems, film, audio and audiovisual tapes, and so on. Government records include Cabinet ministers' records that are created and/or accumulated and used by a Minister (or a Minister's office in developing, implementing and/or administering programs of government. Government records do not include legislative records (records created and/or accumulated and used by an individual or an office in the administration of the Legislative Assembly of British Columbia or by a Member of the Legislative Assembly). The retention and final disposition of most government records is governed by the *Document Disposal Act*.

4. **Information Incident**: a single or series of unwanted or unexpected events, actual or suspected, that threaten information security or privacy.

5. **Information Management:** is the organization of and control over the structure, processing, maintenance, delivery and acquisition of information; from one or more sources, to one or more audiences

6. **Information Sharing Agreement (ISA):** documents the terms and conditions related to the exchange, disclosure or collection of personal information exchanged between public bodies and persons, groups of persons or organizations within the parameters of the *Freedom of Information and Protection of Privacy Act* (FOIPPA).

7. **Personal Information:** is a type of confidential information, the collection, use, storage, disclosure and disposal of which is specified in legislation. Under the *Freedom of Information and Protection of Privacy Act* (FOIPPA), "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, e-mail;
- Race, national/ethnic origin, colour, religious or political beliefs or associations;
- Age, sex, sexual orientation, marital status;
- Identifying number or symbol such as social insurance number or driver's license number;
- Fingerprints, blood type, DNA prints;
- Health care history;
- Educational, financial, criminal, employment history;
- Personal recommendations or evaluations, character references or personnel evaluations about the third party.

8. **Sensitive Information:** Information which is confidential or of high value, and which if compromised could result in serious consequences, is considered to be sensitive information.

9. **Standing Response Team** – consists of the Chief Information Security Officer, the Executive Director of the Privacy and Legislation Branch and delegates from their offices. Depending on the nature of the information incident, the team may also include the business owner, Ministry Information Security Officer, and delegates from the BC Public Service Agency.

Acronyms

BCPSA – British Columbia Public Service Agency

BCPS – British Columbia Public Servant

GCIO – Government Chief Information Officer

MCIO – Ministry Chief Information Officer

MISO – Ministry Information Security Officer

MSO – Ministry Security Officer

OCIO – Office of the Chief Information Officer

OIPC – Office of the Information and Privacy Commissioner

RDC - Remote Desktop Connection

VPN - Virtual Private Network

Links Related to Policies and Procedures

B.C. Privacy and Access Helpline: For public bodies and private sector organizations with inquiries specific to privacy matters in general please contact us through the BC Privacy and Access Helpline.

Phone: 250-356-1851 **Email:** *privacy.helpline@gov.bc.ca*
Or via Enquiry BC:
1-800-663-7867

Core Policy and Procedures Manual, Chapter 12: Information Management and Information Technology Management
http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm

Freedom of Information and Protection of Privacy Act (FOIPPA) Policy and Procedures Manual.
http://www.cio.gov.bc.ca/cio/priv_leg/manual/index.page?

Handle an Information Incident the Right Way. Information incident overview on the @ Work website (internal) *https://gww.gov.bc.ca/sites/default/files/broadcast/handle-information-incident-right- way.htm?bemail=privacy*

Home Technology Assessment Guide. A self-assessment guide in the Working Outside the Workplace policy that describes the readiness of the home technology environment for government employees who need to work on confidential and/or personal information**.**
http://www.cio.gov.bc.ca/local/cio/working_outside_workplace/home_technology_assessment. pdf

Information Access Operations. Corporate website for FOI requests and records management.
http://www.gov.bc.ca/citz/iao/

Information Incident Management Process. The complete process and support documents
http://www.cio.gov.bc.ca/local/cio/information_incident/information_incident_management_process.pdf

Information Security Branch. The branch within the Office of the Chief Information Officer (OCIO) that is responsible for the security of government's electronic information and developing the policies, *standards* and programs that protect sensitive and personal information.
http://www.cio.gov.bc.ca/cio/informationsecurity/index.page?

Information Security Classification Framework. An information security classification system assists in determining the value and sensitivity of information as well as the protective measures to be applied
http://www.cio.gov.bc.ca/cio/informationsecurity/classification/information_security_classification_framework.page?

Information Sharing Agreements Guidelines. Information Sharing Agreements document the terms and conditions of the exchange of personal information in compliance with the provisions of

the Act and any other applicable legislation.
http://www.cio.gov.bc.ca/local/cio/priv_leg/documents/foippa/guidelines_isa.pdf

Ministry Chief Information Officer (MCIO's) Role
http://www.cio.gov.bc.ca/cio/about/governance/role_cio/ministry_cio.page

Ministry Chief Information Officers' and their Ministries
http://www.cio.gov.bc.ca/local/cio/about/documents/mcio_contact.pdf

Ministry Information Security Officer (MISO's) Role
http://www.cio.gov.bc.ca/cio/informationsecurity/MISO/MISORole.page

Office of the Information and Privacy Commissioner for British Columbia
www.oipc.bc.ca

Privacy and Legislation Branch. The branch within the Office of the Chief Information Officer (OCIO) that is responsible for privacy protection and developing the policies, standards and programs that protect individuals' personal information. *http://www.cio.gov.bc.ca/cio/priv_leg/lpp.page*

Process for Responding to Privacy Breaches
http://www.cio.gov.bc.ca/cio/information_incident/index.page
To report an information incident in Victoria, including a Privacy Breach, notify the Shared Services BC Service Desk at 250-387-7000 and Select Option 3. Elsewhere in the Province dial **Toll-free:** 1-866-660-0811 and Select Option 3.

Visit the **Office of the Chief Information Officer** (OCIO) website to view the policy and online resources *http://www.cio.gov.bc.ca/*

Provincial Legislation and Strategic Privacy Practices
The Office of the Chief Information Officer (OCIO) is responsible for the *Freedom of Information and Protection of Privacy Act* (FOIPPA), the *Personal Information Protection Act* (PIPA), the *Document Disposal Act* and the *Electronic Transactions Act*, and all policy, standards and directives that flow from them. This website provides more information on the legist ration, regulations, policies, guidelines, information access requests, forms and reports.
http://www.cio.gov.bc.ca/cio/priv_leg/index.page

Recorded Information Management Manual. The Recorded Information Management (RIM) manual is the central agency manual on government records management.
http://www.gov.bc.ca/citz/iao/records_mgmt/policy_standards/rim_manual/index.html

Schedule E Privacy Protection – General Services Agreement (GSA)
http://www.cio.gov.bc.ca/cio/priv_leg/foippa/contracting/ppsindex.page

Working Outside the Workplace Policy. This policy document provides direction on how to safeguard confidential and/or personal information when working outside the workplace
http://www.cio.gov.bc.ca/local/cio/working_outside_workplace/Working%20outside%20the%20workplace%20policy.pdf