

September 2011

Information Incident Management Process

Office of the Government Chief Information Officer



Ministry of Labour, Citizens' Services
and Open Government

Table of Contents

Policy Overview	3
Objectives	3
Scope	3
Supporting Documents:	4
Section 1: Information Incidents	5
Section 2: Appendices	16

Information Incident Management Process

Policy Overview

This policy was developed to provide policy direction to guide employees and business owners (including supervisors and contract service providers) in responding to incidents that threaten information privacy or security.

Policy direction is offered through the following sections:

- Section 1 – Information Incidents
- Section 2 – Appendices
 - A. Key Definitions
 - B. Process Flow Chart
 - C. Information Management/Information Technology (IM/IT) Guiding Principles

For questions or comments regarding this policy and other Information Management/Information Technology policy, please contact:

Information Security Branch
Office of the Government Chief Information Officer
Ministry of Citizens' Services
Telephone: 250 387-7572

Objectives

The objectives of this policy are to:

1. Provide a policy framework for responding to information incidents in accordance with legislative and policy requirements;
2. Consolidate policy by function (information incident management) rather than by business area (security, privacy, records management, etc.);
3. Assist employees and business owners (including supervisors and service providers) in understanding their responsibilities in addressing information incidents.

Scope

This policy applies to employees and business owners (including supervisors and contract service providers) or any person handling information managed (e.g., collected, accessed, used, shared, stored, disclosed, disposed of, or archived) by the government of British Columbia.

Supporting Documents:

The following documents and tools support the application of this policy:

1. [Freedom of Information and Protection of Privacy Act \(FOIPPA\)](#)
2. [Process for Responding to Privacy Breaches](#)
3. [Information Security Policy](#)
4. [General Incident and Loss Report \(GILR\)](#)
5. [Information Incident Checklist](#)
6. [Easy Guide for Information Incidents](#)

Section 1: Information Incidents

This section defines the steps that must occur in response to an information incident, including the roles and responsibilities of the stakeholders.

An **information incident** is a single or a series of unwanted or unexpected events that threaten privacy or information security. Information incidents include the collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that is not authorized by the business owner of that information.

Information incidents include **privacy breaches**, which are 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* (see Appendix A – *Key Definitions* for other terms.)

Policy

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 supervisor and to the Government Chief Information Officer using the Information Incident Management Process (below).
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. The only exception may occur under the Whistle Blower provision within Section 30.3 of the FOIPP Act which allows for information sharing with the Commissioner by an employee acting in good faith.
4. Deputy Ministry's will be responsible for decisions relating to notifications when a decision must be made to not notify individual(s) based on a balance of harms.

Process

Event Reporting and Triage Phase

1. Any employee, service provider or other person who discovers a suspected or actual information incident (including privacy breaches) must immediately report it to their supervisor or designated management contact (if one has been appointed).
2. The supervisor or management contact, must also immediately report the information incident to the Office of the Government Chief Information Officer by:
 - a. 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
 - b. Selecting Option 3 and stating they require an **“Information Incident Investigation”**.

In circumstances where the supervisor or management contact is not immediately available (in person or by phone), the employee, service provider or other person must immediately report the information incident as indicated above.

The service desk will take contact information and create a ticket for the incident report. The ticket will be delivered to the Government Chief Information Officer's Investigations Unit, the Chief Information Security Officer, and the Privacy Investigations Unit.

3. Whoever reported the incident to 387-7000 in step 2 above must also report it to their [Ministry Chief Information Officer](#).

Where appropriate, the Ministry Chief Information Officer also notifies the ministry executive (deputy minister / assistant deputy minister).

The business owner or employee reports the information incident to the Risk Management Branch through a General Incident Loss Report (GILR) within 24 hours of its discovery.

4. The Investigations Unit contacts the information incident reporter to:
 - Assess and document the information incident including, if applicable, the nature, sensitivity, volume, impact and type of incident (physical and/or information);
 - Assist with resolving the incident and containing the information incident (if applicable) if it is still ongoing; and
 - Provide the information incident reporter with instructions explaining the incident response process and priorities (e.g., contain the loss, prevent a recurrence, and determine next steps).
5. The Investigations Unit reports to the Standing Response Team. The Standing Response Team assesses the incident, assigns the Incident Lead who establishes the Incident Action Team that includes the business owner and, depending on the nature of the information incident, may include the Ministry Information Security Officer, and delegates from the BC Public Service Agency.

The Incident Action Team also decides if additional information should be gathered to determine the response strategy and to define work assignments according to relevant factors, including:

- Type of information incident (physical and/or information);
 - Nature and sensitivity of the incident;
 - Volume; and
 - Impact and implications of unauthorized disclosure or asset loss.
6. The Incident Lead determines whether the information incident is major or minor, based on relevant factors that include:
 - The incident involves multiple ministries;

- The incident involves personal or sensitive information;
- Whether there is, or could have been, a reasonable expectation of harm to any individuals as a result of the incident;
- Whether individuals will be, or have been, notified that their personal information was breached;
- Whether the incident will be, or has been, reported to the independent offices of the Legislative Assembly, including the Office of the Information and Privacy Commissioner and the Office of the Auditor General; or
- Whether the incident has a serious or potentially serious public impact.

a) Minor information incidents:

- The Incident Lead will be the main point of contact for the breach.
- The Incident Lead will refer all minor information incidents to the Ministry Chief Information Officer for follow-up and resolution in collaboration with the business owner.
- If the minor incident is a privacy breach, the Privacy Investigations Unit in the Information Security Branch gives operational support and assistance as needed.
- If the minor breach is not a privacy breach, the Investigation Unit in the Information Security Branch gives operational support and assistance as needed.
- When requested by the Office of the Chief Information Officer, the business owner provides a final report to the Ministry Chief Information Officer, the Chief Information Security Officer, and the Incident Lead. The Chief Information Security Officer or the Incident Lead will provide periodic updates to the Government Chief Information Officer as appropriate and as needed.

b) Major information incidents:

- The Incident Lead coordinates an incident management and investigation process in order to conduct an assessment and gather evidence (see Appendix B for the process flow).
- Status reports are sent to the Chief Information Security Officer and/the Director, Privacy Investigations Unit (for incidents involving personal information), who provide periodic updates to the Government Chief Information Officer as appropriate and as needed.

Note: Privacy breaches are resolved in accordance with government's [Process for Responding to Privacy Breaches](#).

7. Executive Notifications:

- The Chief Information Security Officer or (for privacy breaches) Director of the Privacy Investigations Unit informs the Government Chief Information Officer, Ministry Chief Information Officer, Government Communications and Public Engagement, and other Standing Response Team members.
- The Government Chief Information Officer informs the Deputy Minister of Citizens' Services, who will inform the Minister of Citizens' Services where appropriate.

- The Ministry Chief Information Officer informs that ministry’s executive, including its deputy minister.
- An executive steering group may be created to coordinate government communications.
- The Government Chief Information Officer will liaise with the Information and Privacy Commissioner in accordance with government’s [Process for Responding to Privacy Breaches](#).
- In situations requiring the involvement of law enforcement, the Incident Lead notifies the Assistant Deputy Minister, Police Services Division, Ministry of Public Safety and Solicitor General. Where this involves a public servant, the Incident Lead must also notify the Public Service Agency.
- Additionally, when the Public Service Agency becomes aware that a public servant is subject to criminal investigation, they must:
 - i. Call the Shared Services BC Service Desk at 250 387-7000 or toll-free at 1-866 660-0811 (available 24 hours a day); and
 - ii. Select Option 3 and state that they require a “**Security Investigation**”.

Investigation and Resolution Phase for Major Information Incidents

8. The Incident Lead leads the investigation and management of the incident. The Privacy Investigations Unit takes the lead for privacy breaches; the Investigations Unit takes the lead for other information incidents. During the investigation:
 - The Incident Lead will work with the affected ministry, so the ministry can notify affected parties and take other required actions as appropriate. Notification for privacy breaches is in accordance with government’s [Process for Responding to Privacy Breaches](#).
 - The Incident Lead will provide status reports to the Chief Information Security Officer, the Director of the Privacy Investigations Unit (for incidents involving personal information), the Ministry Chief Information Officer, and the business owner.
 - The Chief Information Security Officer or the Director, Privacy Investigations Unit (for incidents involving personal information) will provide status reports to the Government Chief Information Officer. Where necessary, the Government Chief Information Officer liaises with the responsible ministry’s executive (deputy minister / assistant deputy minister) and the Office of the Information and Privacy Commissioner.

9. Notification of 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. The Incident Lead will work with the affected ministry, so the ministry can notify affected parties and take other required actions as appropriate. Notification for privacy breaches is in accordance with government’s [Process for Responding to Privacy Breaches](#).

- 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
 - A risk of physical harm
 - A risk of hurt, humiliation or damage to reputation 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.

Notification is determined based on the balance of harms. Under this principle, an individual(s) who could potentially face harm as a result of an information incident may not be notified if it is determined that the harm that would result from conducting notification would outweigh the benefit to be gained from the notification.

Important: Where an information incident involves the potential for significant harm to an individual(s), the decision to not notify individual(s) is based on the balance of harms and must be approved by the Deputy Minister of the responsible ministry.

If it is determined that notification of individuals is appropriate:

- Notification should occur as soon as possible following the breach and
 - Affected individuals should be notified directly, whenever possible.
10. When closing an information incident file, the Incident Lead notifies the Chief Information Security Officer, the Director, Privacy Investigations Unit (for incidents involving personal information), the Ministry Chief Information Officer, and the business owner. In some cases the Incident Lead writes a final report, including recommendations, and submits it to required stakeholders. There are two types of recommendations included in final reports:
- mandatory recommendations (directives), which must be implemented; and
 - advisory recommendations, which the ministry decides whether to implement (the Ministry Chief Information Officer informs the Office of the Government Chief Information Officer of the decision).

Compliance

11. Government, the ministry, or the business owner is, as applicable, responsible for implementing the final report's mandatory recommendations and reporting their status and results to the Ministry Chief Information Officer, Chief Information Security Officer and

the Director of the Privacy Investigations Unit (for incidents involving personal information).

12. The Chief Information Security Officer and the Director of the Privacy Investigations Unit (for incidents involving personal information) review the report and, if necessary, forward implementation results to the Government Chief Information Officer.
13. The Chief Information Security Officer may perform compliance reviews or may audit the implementation of the recommendations and its effectiveness. The CISO reports the review or audit results to Government Chief Information Officer. (For privacy issues, the Director of the Privacy Investigations Unit will also participate in the audit/review process).

Responsibilities

Employee

- In the case of the actual or suspected incident, the employee's responsibilities are to:
 - **Report** – the information incident immediately to their supervisor, the Government Chief Information Officer (by calling the Shared Services BC Service Desk at 250 387-7000 or toll-free at 1-866 660-0811 and selecting Option 3), and the Ministry Chief Information Officer.
 - **Recover** – the confidential or personal information if possible, or otherwise contain the incident to lessen the impacts and implications for government and individuals. (Note: If the incident involves information technology, seek the direction of the Investigations Unit before taking any containment steps).
 - **Remediate** – the information incident by working collaboratively with the Investigation Unit, Standing Response Team, the Government Chief Information Officer's staff or others to determine the specifics of the incident and resolve it.
 - **Prevent** – information incidents by being diligent in the handling of confidential or personal information, and being an active participant in developing the culture of prudent information management.

Supervisor

- In the case of the actual or suspected incident supervisor's responsibilities are to:
 - **Report** – receive the report about the information incident from the employee and provide direction on assessing the incident and ensuring it is reported centrally (to the Office of the Government Chief Information Officer by calling the Shared Services BC Service Desk at 250 387-7000 or toll-free at 1-866 660-0811 and selecting Option 3) and locally (notifying senior managers, the Ministry Chief Information Officer) within the workplace.
 - **Recover** – determine if the confidential or personal information can be recovered, or if the loss/disclosure can otherwise be contained. (Note: If the incident involves information technology, seek the direction of the Investigations Unit before taking any containment steps).

- **Remediate** – work collaboratively with the Business Owner, the Standing Response Team, the Government Chief Information Officer’s staff, or others to determine the specifics of the information incident and to implement the steps needed to resolve it.
- **Prevent** – information incidents by
 - ✓ Implementing recommendations from the Incident Report and ensuring that employees know and understand how to apply changes in the handling of confidential or personal information.
 - ✓ Participating in the development of a culture for the prudent management of information, including by providing training.
 - ✓ Ensuring employees understand their responsibility in reporting all actual and suspected information incidents, including containing the loss and/or recovering the information.

Business Owner and Contract Manager

- In the case of the actual or suspected information incident, the business owner’s and government Contract Managers responsibilities are to:
 - **Report** – ensure the information incident is reported immediately to the Office of the Government Chief Information Officer (by calling the Shared Services BC Service Desk at 250 387-7000 or toll-free at 1-866 660-0811 and selecting Option 3), senior managers, and the Ministry Chief Information Officer.
 - **Recover** – the confidential or personal information if possible, or otherwise contain the incident to lessen the impacts and implications for government and individuals. (Note: If the incident involves information technology, seek the direction of the Investigations Unit before taking any containment steps).
 - **Remediate** – the information incident:
 - ✓ As incident owner and as appropriate as government contract manager on behalf of a contracted service provider
 - ✓ By working collaboratively with the Investigation Unit
 - ✓ By supporting the investigation and the Standing Response Team, the Government Chief Information Officer’s staff, or others to determine the specifics of the information incident and resolve it
 - ✓ By notifying individuals or parties affected by the incident, where directed
 - **Prevent** – information incidents 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 Report Process and reporting the results the Chief Information Security Officer and the Director of the Privacy Investigations Unit, Information Security Branch.
 - ✓ Developing a culture for the prudent management of information, including by providing training.
 - ✓ Ensuring employees understand their responsibility in reporting information incidents, including containing the loss and/or recovering the information.
 - ✓ Ensuring Contractors and Service Providers understand their responsibilities under the Information Incident Report Process and working with them to ensure timely and accurate reporting.

- ✓ Supporting the audit activities of the Office of the Government Chief Information Officer.

Contractor or Service Provider

- In the case of an actual or suspected information incident, the contractor's responsibilities are to:
 - **Report** – Contractors will ensure that any of their employees, service providers, or other persons who discovers a suspected or actual information incident (including privacy breaches) immediately notify their supervisor or manager and report it to their Government contract manager.
 - The government contract manager is then required to immediately report the information incident to the Office of the Government 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 stating they are reporting an information incident.

In circumstances where the contractor's employee, service provider or other person is unable to immediately inform their supervisor or manager, they are required to immediately report the information incident to their Government contract manager.

In circumstances where the employee, supervisor or manager is unable to immediately inform the government contract manager, they are required to immediately report the information incident as outlined above by calling the Shared Services BC Service Desk and following up as soon possible thereafter with the government contract manager.

- **Recover** – the confidential or personal information if possible, or otherwise contain the incident to lessen the impacts and implications for government and individuals. (Note: If the incident involves government information technology, seek the direction of the Contract Manager to seek the assistance of the Investigations Unit before taking any containment steps).
- **Remediate** – the information incident:
 - ✓ With the government Contract Manager as the incident owner
 - ✓ By working collaboratively with the Contract Manager and the Investigation Unit
 - ✓ By supporting the investigation and the Standing Response Team, the Government Chief Information Officer's staff, or others to determine the specifics of the information incident and resolve it
 - ✓ By notifying individuals or parties affected by the incident, where and as directed by the Incident Action Team and the government contract manager.
- **Prevent** – information incidents 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 Report Process and reporting the results the Chief Information Security Officer and the Director of the Privacy Investigations Unit, Information Security Branch.
- ✓ Developing a culture for the prudent management of information, including by providing training.
- ✓ Ensuring employees understand their responsibility in reporting information incidents, including containing the loss and/or recovering the information.

Ministry Chief Information Officer (MCIO)

- Ministry point of contact for:
 - receiving reports about the management of the incident from the supervisor, employee, or business owner (including service providers);
 - communicating advice and information to / from the Incident Lead and the Standing Response Team; and
 - receiving status reports and the final investigation report from the Information Incident Lead, and distributing them as necessary.
- For minor information incidents, the MCIO is the Incident Lead's main point of contact for follow-up and resolution in collaboration with the business owner.
- Ensures information incidents are reported within 24 hours to the Risk Management Branch via the General Incident and Loss Report.
- Coordinates information incident communication and updates internally (including with ministry executive).
- Responsible within the ministry for delegation of roles and responsibilities under this information incident process.
- Supports the information incident investigation process.
- Liaises with other ministry chief information officers in multi-ministry incidents.
- Ensures that the business owner (including service providers) reports the result of the information incident resolution to the Chief Information Security Officer and the Director of the Privacy Investigations Unit (for incidents involving personal information).
- Reviews the information incident investigation reports and conveys results to the responsible ministry executives as appropriate.
- Assists program areas in reviewing and rectifying existing procedures, where necessary.
- Ensures that the business owner implements the recommendations of the final report and reports the implementation results to the Chief Information Security Officer and the Director of the Privacy Investigations Unit (for incidents involving personal information).
- Ensures that the audit activities of the Office of the Government Chief Information Officer are supported by the ministry.
- Receives, follows up and resolves minor incidents in collaboration with the business owner.

Ministry Executives (DMs, ADMs)

- Receives reports on information incidents from Ministry Chief Information Officer and others, as applicable.
- Ensures that details about the information incident are conveyed as necessary to senior levels of government.
- Supports the information incident investigation.
- Ensures that the recommendations of the final report are appropriately implemented.

Chief Information Security Officer (CISO)

- Member of the Standing Response Team.
- Reports information incidents (except privacy breaches) to the Government Chief Information Officer, where appropriate.
- Follows established protocols for criminal offenses or other law enforcement matters.
- Reviews ministries reports on how they resolved information incidents.
- Reviews investigation reports.
- Provides reports on information incident investigations, except for privacy breaches, to the Government Chief Information Officer.
- Reviews reports on the implementation of recommendations.
- Initiates audits on the implementation of recommendations, where necessary.

Director of the Privacy Investigations Unit, Information Security Branch

- Member of the Standing Response Team.
- Reports privacy breaches to the Government Chief Information Officer, where appropriate.
- Reviews ministries reports on how they resolved privacy breaches.
- Provides reports on privacy breach investigations to the Government Chief Information Officer.
- Reviews reports on the implementation of recommendations concerning privacy breaches.
- Recommends audits to the CISO on the implementation of recommendations, where necessary.
- Participates in audits and reviews, where necessary.
- Upon the direction of the Government Chief Information Officer, liaises with the Office of the Information and Privacy Commissioner on privacy breaches.

Director of the Investigations and Forensics Unit, Information Security Branch

- Member of the Standing Response Team.
- Reports security incidents to the Government Chief Information Officer, where appropriate.
- Reviews ministries reports on how they resolved security incidents.
- Provides reports on security investigations to the Government Chief Information Officer.
- Reviews reports on the implementation of recommendations concerning security incidents.
- Recommends audits to the CISO on the implementation of recommendations, where necessary.
- Participates in audits and reviews, where necessary.

Privacy Investigations Unit, Information Security Branch

- Subject matter experts in privacy breach management.
- The Incident Action Lead for privacy breaches.
- Provides privacy breach management advice to business owner and Ministry Chief Information Officer.
- Provides privacy breach investigation status reports and final report with recommendations to the Chief Information Security Officer and Director of the Privacy Investigations Unit, Information Security Branch.
- Provides immediate incident management (including containment) advice to the Business owner.

- Provides privacy expertise.
- Recommends to the business owner that the affected people be notified of the information incident.
- Participates in audits on the implementation of the recommendations, where necessary.

Investigations and Forensics Unit, Information Security Branch

- Subject matter experts in non-privacy breach management and information incident investigations.
- The Incident Action Lead for security incidents.
- Provides immediate incident management (including containment) advice to the Business owner.
- Follows established protocols for criminal offenses or other law enforcement matters.
- Provides non-privacy breach information incident investigation status reports and the final report with recommendations to the Chief Information Security Officer.
- Provides non-privacy breach management advice to business owner and MCIO.
- Provides investigations expertise.
- Performs audits on the implementation of the recommendations, where necessary.

Government Chief Information Officer

- Responsible for the coordination, investigation, and resolution of all information incidents, including privacy breaches.
- Receives and reviews status reports and, where applicable, final information incident investigation reports and reports on implementation of recommendations.
- Ensures that the recommended controls of the final report are appropriately implemented through audits.
- Reports information incidents to the Deputy Minister of Citizens' Services.
- Contacts responsible ministry executives to ensure appropriate communication, recommendation, and collaboration, where appropriate.
- Liaises with the Office of the Information and Privacy Commissioner on privacy breaches, where appropriate.

Deputy Minister, Ministry of Labour, Citizens' Services and Open Government (CITZ DM)

- Receives information incident and investigation reports, where necessary.
- Ensures that details about the incident are conveyed as necessary to senior levels of government.

Section 2: Appendices

- A. Key Definitions
- B. Process Flow Chart
- C. Simplified Flow Chart
- D. Information Management/Information Technology (IM/IT) Guiding Principles

Appendix A – Key Definitions

Business Owner – the operational unit (such as a branch or a service provider) in which the information incident occurred.

Contract Manager – the person(s) responsible for the oversight of a Contractor or Service Provider. It should be noted that this could also include government personnel responsible for less formal information sharing arrangements.

Contract Service Provider – a person or organization retained under a contract to perform services for a public body.

Incident Action Team – the team pulled together to take action and respond to the incident. The team includes the Incident Lead and the business owner at a minimum. The team may involve, depending on the nature of the information incident, the Ministry Information Security Officer, and delegates from the BC Public Service Agency.

Incident Lead – the OCIO member assigned by the Standing Response Team as the investigative lead for managing the incident.

Information Incident – a single or a series of unwanted or unexpected events that threaten information security or privacy.

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;
- 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;
- anyone else's views or opinions about an individual and the individual's personal views or opinions unless they are about someone else.

Privacy Breach – a type of information incident where there is a collection of, use of, disclosure of, access to, disposal of, or storage of personal information, whether accidental or deliberate, that is not authorized by the *Freedom of Information and Protection of Privacy Act*.

Record – includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means, whether graphic, electronic, mechanical or otherwise.

Standing Response Team – consists of the Chief Information Security Officer, the Directors of the Privacy Investigations and Investigations & Forensics Units, Information Security Branch and delegates from their offices.

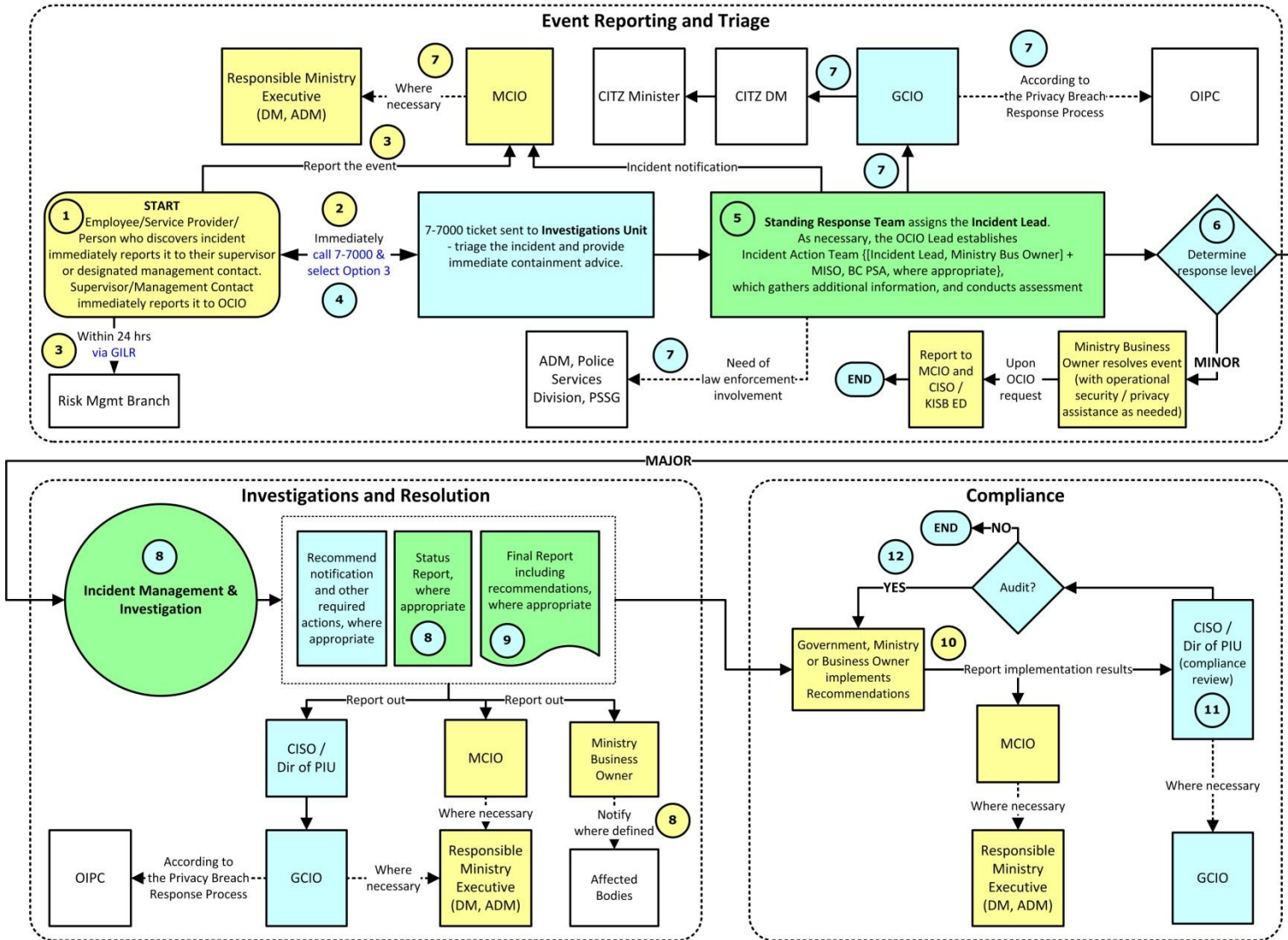
Appendix B – Process Flow Chart

Information Incident Management Process Flow

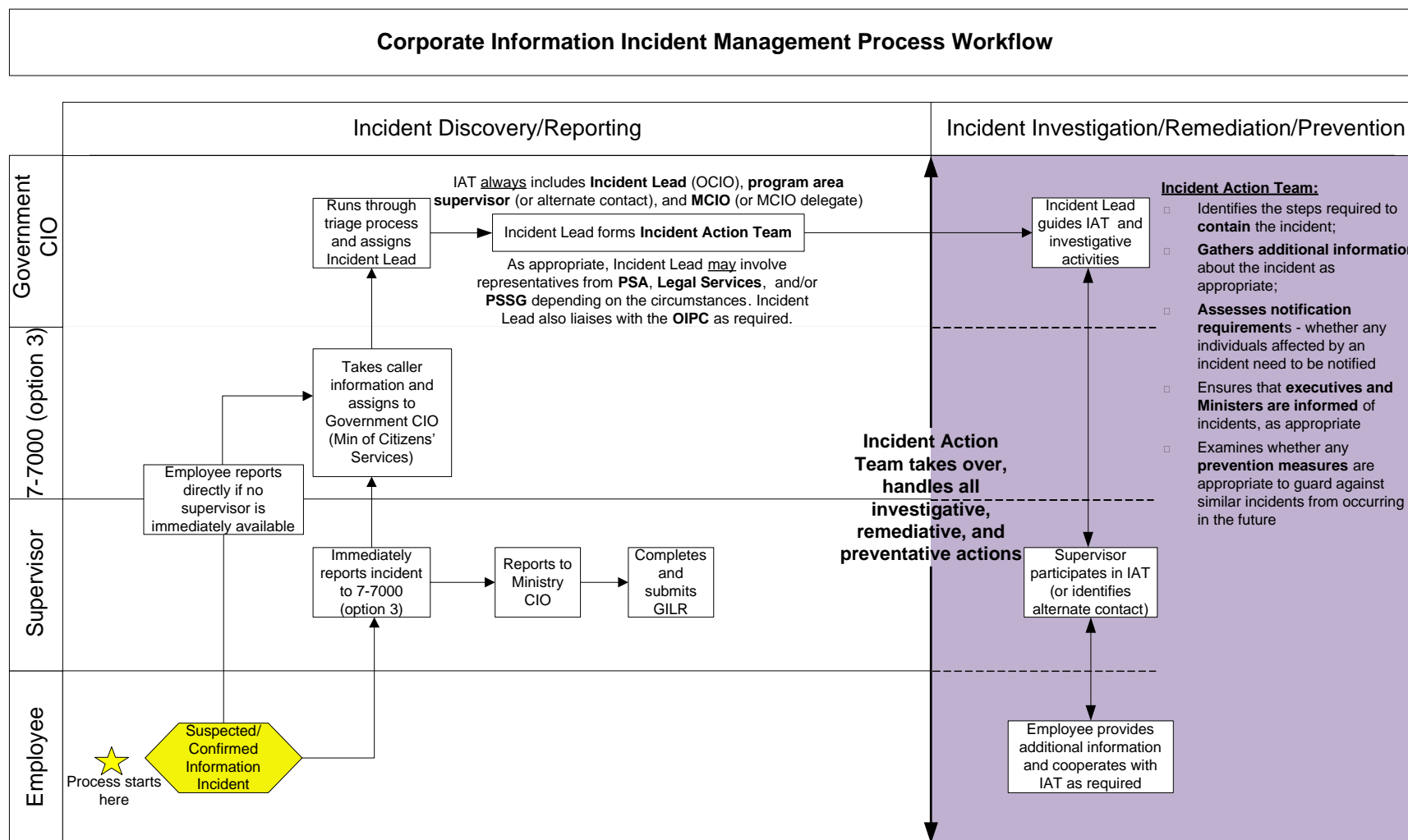
Participation Legend



The colour in the numbered circles represents the accountable party for the task. (OGCIO and Ministry)



Appendix C – Simplified Flow Chart



Appendix D – Information Management/Information Technology (IM/IT) Guiding Principles

Information Management/Information Technology Principles for Use of Information

Information Management/Information Technology (IM/IT) Principles outlines the principles that guide government employees as they work with, handle and manage government information.

Introduction:

The Government of British Columbia is rich in information – an asset that can help transform government services, develop evidence informed policy and programs, and achieve better outcomes for British Columbians. Applying the following strategies and guiding principles in every day work will help government achieve its overall goals and ensure information is used and managed in a way that recognizes its value.

Guiding Principles

Definition:

Information is data that conveys meaning. It is created, received, and acquired for or by the B.C. government and enables the provision of services. Information includes and is not limited to: personal data; population data (economic, cultural and demographic data); and program and operational data (performance measures and data used in policy and program development and operations).

Strategies:

Information is an *asset* that is shared, where appropriate, to optimize its value to government and British Columbians.

Information, as a managed strategic government-wide resource, is *leveraged* with the appropriate policies, priority and security, resulting in:

- Integration and coordination of service delivery of government programs and services;
- Collaboration, innovation and transformation of service delivery to better meet the needs of citizens; and
- Evidence-informed decision-making and program and policy development.

Right Information

Information meets the needs of its users, and the quality of information is appropriate for its purpose in terms of accuracy, relevancy, reliability, consistency, and comprehensiveness.

Right Person

Information is available and accessible as appropriate.

Right Purpose

Information is integral to the business of government, and is shared as appropriate for pursuing an identified purpose or to support achievement of government policy and/or service goals and business needs.

Right Time

Information is available in a timely way, when needed, to support business and program goals, needs and decisions.

Right Way

Information is handled in a way that respects and protects the privacy of individuals regarding their personal information held by government and the confidentiality of government and private sector information.