Information Incident Management Policy	
Office of the Chief Information Officer **Ministry of Citizens' Services**	**Draft/Version #1.0** **October 18, 2019**

TABLE OF CONTENTS

INTRODUCTION

Overview

The Province of British Columbia is the steward of a significant amount of confidential information, including the personal information of British Columbians. Government must protect citizens' personal information in accordance with the requirements set out in the *Freedom of Information and Protection of Privacy Act* (FOIPPA) and ensure that if an information incident occurs, it is managed in an appropriate manner. The Information Incident Management Policy is the Province's corporate policy for responding to and mitigating risks arising from actual or suspected information incidents, including privacy breaches.

The Information Management Investigations Unit (IMIU) within the Office of the Chief Information Officer's (OCIO) Corporate Information and Records Management Office provides ministries with expert advice, support and investigative services to assist them in navigating the information incident process. The IMIU partners with the OCIO's Security Investigations and Forensics Unit (SIFU) when suspected information incidents involve government information technology (IT) systems.

An **information incident** is a single or a series of events involving the collection, storage, access, use, disclosure, or disposal of government information that threaten privacy or information security and/or contravene law or policy.

A **privacy breach** is the theft or loss, or the access, collection, use or disclosure of personal information that is not authorized by Part 3 of FOIPPA. A privacy breach is a type of information incident.

Purpose

The purpose of this policy is to:

- Establish a comprehensive framework for managing information incidents.
- Provide clear direction and set out policy requirements.
- Clarify associated roles and responsibilities.

Application

This policy applies to all ministries, agencies, boards, and commissions subject to the Core Policy and Procedures Manual (referred to as ministries hereafter).

Authority

Core Policy and Procedures Manual Chapter 12

Legal

The Information Incident Management Policy does not replace or limit a ministry's legal obligations under the *Information Management Act* (IMA) or FOIPPA.

Advice on this Policy

For questions or comments regarding this policy, please contact:

Information Management Investigations Unit
Corporate Information and Records Management Office
Office of the Chief Information Officer
Ministry of Citizens' Services
Telephone: 250-356-0361

POLICY REQUIREMENTS

1. General Requirements

1.1 Supervisors must ensure that employees are made aware of their responsibilities under this policy:

a) At the commencement of their employment.
b) When a new or updated version of this policy is issued.
c) Annually for employees that have access to a significant amount of confidential information.

1.2 The IMIU must, in consultation with appropriate parties such as SIFU, review this policy regularly, update it as appropriate, and communicate any changes to ministries.

1.3 Ministries may establish ministry-specific policies and procedures, where necessary, to support this policy. All ministry-specific policies relating to information incident management must be submitted to the IMIU for review.

1.4 Ministries must assign a Ministry Incident Lead for each actual or suspected information incident. Please refer the Ministry Incident Lead Guideline[1] for information regarding the assignment of the Ministry Incident Lead.

2. Reporting

2.1 Employees must *immediately* report any actual or suspected information incidents to both

a) their supervisor; and
b) the IMIU by calling 250-387-7000 or toll-free 1-866-660-0811.

The requirement to report immediately includes actual or suspected information incidents discovered outside of normal working hours.

2.2 Employees must also report actual or suspected information incidents *within 24 hours* to the Risk Management Branch and Government Security Office by completing a General Incident or Loss Reporting Form,[2] in accordance with Procedure L[3] of the Core Policy and Procedures Manual.

2.3 The IMIU must maintain and monitor a means for ministries to report information incidents 24 hours per day, 365 days per year.

2.4 Where the incident is ongoing and related to government IT resources, the OCIO Security Incident Response Process[4] must be followed.

---

[1] Available at www.gov.bc.ca/privacy_breaches
[2] Available at gilr.gov.bc.ca
[3] Refer to https://www2.gov.bc.ca/gov/content/governments/policies-for-government/core-policy/procedures/loss-reporting
[4] Available at https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/cyber-security-incident-response-process

2.5 Where the IMIU determines that an incident is outside of its mandate and/or jurisdiction, and where the IMIU determines that the incident is within the mandate and/or jurisdiction of another investigative unit, the IMIU must provide notice of the incident to that investigative unit.

3. Preliminary Assessment

3.1 The IMIU must conduct a preliminary assessment of reported information incidents that includes, but is not limited to, the following:

a) Whether the incident falls within the IMIU's mandate.
b) Whether the incident is within the IMIU's jurisdiction.
c) The type of information involved, including whether personal information is involved.
d) The potential severity of the incident.
e) The likelihood that an actual information incident has occurred.

3.2 The IMIU may provide notice of information incidents to the Ministry Chief Information Officer of the responsible ministry.

3.3 The IMIU may provide notice, in accordance with the Joint Investigations Protocol[5], of information incidents to other investigative units within government.

4. Containment and Recovery

4.1 In the event of an information incident, ministries must take appropriate steps to contain the incident and, wherever possible, recover any information that has been lost or otherwise exposed.

These steps will vary depending on the nature of the incident, but could include:

a) Isolating or suspending the activity that led to the incident.
b) Correcting weaknesses in physical or technical security.
c) Recovering or seeking the disposal of any information or IT equipment that was lost, stolen, or otherwise exposed.
d) Determining if any copies of confidential information were made or shared with third parties and attempting to recover them where possible.
e) Requesting that individuals involved provide written attestations confirming that they have returned and/or destroyed any records they received without authorization, and whether they sent them to others and, if so, to whom.

5. Information Access Suspensions and Restrictions

5.1 Ministries may temporarily suspend or restrict access to information to contain an information incident at any time. Before suspending or restricting access to information, ministries must take the following into consideration:

a) Whether there is reason to conclude that the actual or suspected information incident may potentially cause moderate or serious risk of harm to a member of the public, the ministry, an employee, a service provider, or any other person/entity.
b) Whether there is reason to believe that the person acted with malice or ill intent, intentionally and knowingly initiating or facilitating a privacy breach.

[5] Available at https://www2.gov.bc.ca/assets/gov/careers/managers-supervisors/managing-employee-labour-relations/investigation_protocol.pdf

c) Whether suspension of access will prevent further harm.
d) Whether there is reason to believe that not suspending or restricting the person's access will result in further breach activity and potential harm to individuals.
e) The impact of the suspension on the person whose access is being suspended and other parties.
f) Whether there is reliable, credible and relevant evidence available on which to base a decision regarding the suspension or restriction of access to information. Information access suspensions/restrictions should not be based purely on conjecture that an information incident has occurred.
g) The business context for which the information was being used and the information access arrangements for the person concerned.
h) Mitigation strategies that reduce the impact to the person whose access is being suspended including, restricting the person's access, creating a new account or provisional suspension until further evidence is identified.

5.2 The decision to suspend or restrict access to information must be documented in writing and be made by the Ministry Incident Lead, unless this responsibility has been otherwise assigned within a ministry.

5.3 The decision to temporarily suspend or restrict access should be periodically reviewed to ensure that the suspension is still justified. If it is found that the basis for the suspension is no longer valid, access to information must be reinstated immediately.

5.4 If information access is temporarily suspended or restricted, ministries must notify the individual subject to the suspension/restriction. Notification must include:
a) The reason why access has been suspended or restricted.
b) The length of time that access is expected to be suspended or restricted.
c) Who to contact for further information.

5.5 At the conclusion of the investigation, the ministry must notify the person if the final decision is to suspend or restrict access to information permanently and provide an opportunity for the person to respond. The ministry must provide the person with:
a) a written summary of the reasons and evidentiary basis for the decision; and
b) a reasonable opportunity to respond in writing or in-person.

6. Privacy Breach Harm Assessment and Notification

6.1 In consultation with the IMIU, ministries must ensure that a harm assessment is completed for all privacy breaches in order to determine the risk of harm to affected individuals as a result of the incident.

Harm assessments must consider informational and situational risk factors, in addition to the circumstances of the incident. This includes, but is not limited to:
a) Which and how many individuals are impacted.
b) The sensitivity, context, and volume of the personal information involved.
c) The ability to quickly contain the incident and the potential likelihood of further dissemination of the information involved.

d) The relationship between the party in receipt of personal information and the person the information is about.
e) Whether any affected individuals could face a risk of:
    i. identity theft or identity fraud;
    ii. physical harm;
    iii. financial, business, or employment loss;
    iv. hurt, humiliation or damage to reputation; and/or
    v. loss of trust.
f) Whether legal or contractual obligations require notification.

6.2 In determining the risk of harm to an impacted individual, the weight applied to each factor should be determined according to the circumstances of the incident.

6.3 Notifications must be based on a balance of a harms assessment. Under this principle, the risk of harm to an impacted individual as a result of the breach must be weighed against the risk that notification would cause further harm to an individual. Ministries should notify the impacted individual(s) if the risk of harm, as a result of the breach, outweighs the risk of further harm to an individual, if notification occurs.

6.4 Notifications should occur without unreasonable delay, be direct wherever possible, and should include the following information:
a) The date of the privacy breach.
b) A description of the privacy breach.
c) The personal information involved.
d) The risk to the individual and the steps taken to mitigate the potential for harm.
e) Steps the individual can take to further mitigate any potential harm they face.
f) Measures that have been, or will be, taken to prevent similar incidents from occurring in the future.
g) The contact information of an individual within the responsible ministry who can answer questions or provide further information.
h) The right of complaint to the Office of the Information and Privacy Commissioner (OIPC) or notice that the OIPC is aware of the breach and contact information for the OIPC.

7. Investigations

7.1 Ministries may initiate an investigation to determine the nature, extent, and/or cause of an information incident.

7.2 Ministries may request the support of the IMIU in conducting investigations into information incidents. If a ministry requests the IMIU's support, the IMIU takes on responsibility for 7.4 below.

7.3 Ministries must ensure that information incident investigations are conducted in accordance with principles of administrative fairness. This includes, but is not limited to:
a) The terms of reference established in writing, including purpose and scope.
b) Objective, documented standards are used to measure the event or issue being investigated.
c) Investigations are conducted with an open mind and consider all reasonably available evidence.

d) Individuals with allegations made against them are given an appropriate opportunity to respond to the allegations and provided with notice of the allegations in advance of any interview.
e) Individuals are treated with respect throughout the interview process.
f) Findings are based on a reasonable assessment of the available evidence.

7.4 Ministries must ensure that information incident investigators are sufficiently trained in:
a) The subject-matter of information incident investigations.
b) How to gather, review, assess, document, and weigh evidence.
c) How to conduct an investigative interview.
d) Administrative fairness.
e) When and how to report potential crimes and/or share information with law enforcement agencies.

8. Prevention

8.1 Ministries must have appropriate measures in place to prevent information incidents from occurring. These measures will vary depending on the ministry and the type of information they hold, but may include the following:
a) Regular training and awareness activities for employees.
b) Adequate policies, procedures, and/or guidelines for staff to follow.
c) Tools and resources to assist staff in performing their duties without risking an information incident.
d) Appropriate physical and technical security controls and processes to ensure confidential information is protected against such risks as unauthorized access, use, disclosure, or disposal.

8.2 In response to an information incident, ministries must, in consultation with appropriate parties such as the IMIU and SIFU, assess, implement and document preventative measures to mitigate the risk of a similar incident occurring.

8.3 The IMIU may request that ministries provide documentation of the preventative measures implemented to mitigate the risk of a similar incident happening.

9. Documentation

9.1. Evidence of the information incident must be preserved, and the circumstances of the information incident must be documented, including:
a) The IMIU file number.
b) The OIPC file number (where applicable).
c) What happened and when.
d) How and when the incident was discovered.
e) Any personal information involved and the scope of any privacy breach.
f) Steps taken to contain the incident and their effectiveness.
g) The number and type of impacted individuals and the assessment of harm.
h) Any decision to notify the impacted individual(s) and the steps taken to notify (in the case of a privacy breach).

i) The decision and the circumstances around any suspension/restriction of access to information.
j) Prevention measures undertaken in response to the incident.
k) Any IMIU recommendations (if applicable).

10. Roles & Responsibilities

Information Management Investigations Unit (IMIU)

The IMIU of the OCIO's Corporate Information and Records Management Office has the responsibility to:

- coordinate, investigate, and/or resolve actual or suspected information incidents, including privacy breaches;
- provide expert advice, recommendations and investigative services throughout incident response and investigative processes, including on the containment and recovery of information, the suspension of access to information, harm assessment and privacy breach notification, and preventative measures;
- act as government's liaison with the OIPC with regard to information incidents, including privacy breaches;
- maintain and monitor a means for ministries to report information incidents;
- provide notice of incidents to Ministry Chief Information Officers (MCIOs), the SIFU, program areas, and other stakeholders, as appropriate;
- ensure its investigation procedures and practices are administratively fair;
- provide sufficient training to its investigators;
- track and retain information about government's response to an information incident; and
- report on information incidents on behalf of government.

Deputy Ministers (or equivalent positions)

Deputy Ministers (or equivalent positions) have the responsibility to ensure that:

- ministry-specific policies to support this policy are developed as appropriate;
- information incident investigations are conducted in accordance with administrative fairness;
- information incident investigations are conducted by investigators with sufficient training and expertise;
- adequate resources are assigned to support information incident investigations;
- a process is in place to receive notifications of privacy breaches as per section 30.5 of FOIPPA;
- an appropriate Ministry Incident Lead has been identified; and
- preventative measures are developed, where appropriate, to prevent the recurrence of information incidents.

Ministry Chief Information Officers

Ministry Chief Information Officers have the responsibility to:

- lead the development of ministry-specific policies as appropriate;
- identify parties within the ministry who should be notified of information incidents;
- collect and retain summary information about information incidents for the ministry;

- act as a liaison and point of contact for issues within the ministry that may arise during an information incident investigation;
- liaise between investigative teams and other stakeholders within the ministry, as needed;
- ensure that information incidents are reported to ministry executives with responsibility for information management, including the head of the public body for the purposes of FOIPPA; and
- facilitate the implementation of preventative measures.

Ministry Incident Leads

Ministry Incident Leads have the responsibility to:

- act as the primary decision-maker for incident response and investigative processes, including approving preliminary assessments, Terms of Reference/Workplans, and decisions to conduct investigative interviews;
- where necessary, and in consultation with the IMIU wherever possible, direct employees and supervisors to take immediate action to contain an incident and recover any information exposed;
- consult and coordinate with the IMIU throughout the incident response and investigation processes, including assigning appropriate resources to facilitate an effective response and ensuring the IMIU is provided with sufficient information to formulate appropriate recommendations in a timely manner;
- approve notifications of privacy breaches to impacted individuals, including withholding notification on the basis of a balance of harms test;
- make decisions to suspend or restrict access to information, unless these decisions have been assigned to another party by the ministry;
- receive and accept the IMIU's investigative reporting materials; and
- ensure that the ministry's response to an information incident is adequately documented.

Employees

Employees have the responsibility to:

- be aware of their responsibilities under this policy;
- report any actual or suspected information incident in accordance with this policy; and
- take appropriate steps to contain an incident and recover any information as directed by the IMIU and/or the Ministry Incident Lead, as appropriate.

Service Providers

Service Providers have the responsibility to:

- report suspected information incidents in accordance with the terms of their contracts or service agreements; and
- be aware that, if their contracts or service agreements do not include privacy protection or security schedules that address information incidents, service providers are considered employees under this policy.

Supervisors

Supervisors have responsibility to:

- ensure employees are made aware of their responsibilities under this policy as per 1.1 of this policy;
- ensure that all actual or suspected information incidents reported to them are also reported to the IMIU in accordance with this policy; and
- take appropriate steps to contain an incident and recover any information exposed, as directed by the IMIU and/or the Ministry Incident Lead, as appropriate.

DEFINITIONS

Confidential information: a category of **Government Information** (as defined under the *Information Management Act*) with confidentiality requirements. Confidential information includes, but is not limited to:

- Cabinet confidences (for example, a briefing note to Cabinet).
- Government economic or financial information (for example, information about a proposed administrative plan that has not yet been implemented or made public).
- Information harmful to intergovernmental relations (for example, information received in confidence from another government).
- Third-party business information, where its disclosure could harm the third party.
- Personal Information.
- Legal advice or law enforcement information.

Employee: an individual working for, or on behalf of, a ministry, agency, board or commission subject to the Core Policy and Procedures Manual.

Personal Information: recorded information about an identifiable individual other than (business) contact information.

Service Provider: a person retained under a contract or service agreement to perform services for a ministry, agency, board or commission subject to the Core Policy and Procedures Manual.

Supervisor: a person to whom an **Employee** directly reports or a person who manages a **Service Provider** contract or service agreement.

REVISION HISTORY

Version	Date	Notes
1.0	October 18, 2019	CRO/GCIO-approved version posted online