Table of Contents

I  Introduction, Scope, Background .................................................................3
II  Glossary, Terms and definitions, List of commonly used references .......................3
1  Information Security Incident Management ................................................................4
   1.1 Management of information security incidents and improvements.........................4
I Introduction, Scope, Background

This standard is designed to be read in conjunction with the Information Security Standard (version 2.0) as it is a sub-section or sub-standard of the Information Security Standard (version 2.0) (published here: IM/IT Standards).

II Glossary, Terms and definitions, List of commonly used references

To avoid repetition of content, please check the “Glossary”, “Terms and definitions” and “List of commonly used references” sections of the Information Security Standard (version 2.0) (published here: IM/IT Standards) for the terms and definitions used in this standard.
1 Information Security Incident Management

This chapter establishes requirements for reporting a possible breach of information security as quickly as possible. This includes establishing procedures and processes so that employees understand their roles in reporting and mitigating security events.

Information security incident management policies identify mechanisms to detect and report when information security events occur and the directives for the consistent management of such events. The information collected about the events can be analyzed to identify trends and to direct efforts to continually improve and strengthen the information security infrastructure of the Province.

1.1 Management of information security incidents and improvements

1.1.1 Incident management responsibilities and procedures must be established to ensure a quick, effective and orderly response to information security incidents.

a) Information security incident management

Purpose: To enable quick and orderly management of information security incidents.

1.1.1 a) Information security incident management

Information Owners and Information Custodians must adopt the Information Security Incident Management Process and ensure that those responsible for information security incident management understand the priorities for handling information security incidents.

Ministries must follow the established Information Incident Management Process for reporting, managing, responding to and recovering from information security incidents. The process must include:

- Procedures for incident response planning and preparation;
- Procedures for monitoring, detecting, analyzing and reporting of information security incidents;
- Procedures for logging incident management activities; and,
- Procedures for handling different types of information security incidents, including immediate action for containment, response escalation and contingency plans.

Employees with security incident management responsibilities must be appropriately trained and deemed qualified (e.g., in forensics and investigations), and their authorization for access to live systems and data must be delineated formally. Incident response processes must be documented, tested and rehearsed regularly to evaluate their effectiveness.

In case of an information security incident, the Investigations and Forensics Unit of the Office of the Chief Information Officer must be provided access to all and any relevant primary data stores in a quick, effective and expedient manner to ensure an orderly response to incidents.

The Information Incident Management Process includes the following documents:

- Information Incident Management Process document;
- Information Incident Report Form;
- Easy Guide for Responding to Information Incidents;

Ministry of Citizens Services,

Province of British Columbia
• Process for Responding to Privacy Breaches; and,
• Information Incident Checklist.

Guidelines:
Potential types of security incidents to be reported include:
• Suspected or actual breaches of privacy and/or confidentiality;
• Denial of service;
• Detection of network probing;
• Detection of malicious code (e.g., virus, worm, Trojan horse);
• Errors due to incomplete or inaccurate data;
• Outgoing network traffic not associated with typical business processing;
• Repeated attempts of unauthorized access;
• Inappropriate use of government information resources;
• Repeated attempts to e-mail unknown internal accounts;
• System activity not related to typical business processing;
• System failures and loss of service;
• Privacy breaches of personal information;
• Responses to phishing attacks;
• Threatening or harassing communication; and,
• Sharing of user credentials.

Employees who regularly ignore information security and privacy policies should be subject to a
disciplinary process that includes notification of their Supervisor and suspension of privileges for
repeated offences.

Recommended Tests:
Note: 1.1.1 is reported on as part of the annual information security review.
• Demonstrate that employees are made aware of the Information Security Incident Management
  Process.
• Demonstrate that employees follow the Information Security Incident Management Process for
  reporting and responding to information security incidents.

<table>
<thead>
<tr>
<th>1.1.2</th>
<th>Information security events must be reported immediately.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Reporting information security events</td>
<td></td>
</tr>
<tr>
<td>b) Information security event logging</td>
<td></td>
</tr>
</tbody>
</table>

Purpose: To enable prompt response to information security events and identify government wide
trends.

1.1.2 a) Reporting information security events
As required by the Information Incident Management Process, employees must immediately report all
suspected or actual information security events as quickly as possible to their Supervisor. Your
Supervisor will ensure that senior managers and your Ministry Chief Information Officer are also
informed. You or your Supervisor must also immediately notify the Office of the Government Chief
Information Officer by dialling the OCIO Helpdesk at 250 387-7000 or toll-free at 1-866 660-0811 and
selecting Option 3 and asking for an Information Incident Investigation. You will be contacted shortly by
the Government Chief Information Officer’s Investigations Unit, which will seek further details and may give advice on next steps.

All employees must be aware of:
- Procedures for reporting information security events; and,
- Points of contact for reporting.

Requirements for reporting events must be included in contracts and service agreements.

Situations to be considered for information security event reporting include:
- Ineffective security controls;
- Breach of information integrity, confidentiality or availability expectations;
- Breach of personal privacy;
- Human errors;
- Non-compliance with policies or guidelines;
- Breaches of physical security arrangements;
- Uncontrolled system changes;
- Malfunctions of software or hardware; and,
- Access violations.

1.1.2 b) Information security event logging

Information security event logs are logs that could be used in security investigations, auditing or monitoring and could give rise to a security incident. Security events may be any activities that can potentially impact the confidentiality, integrity or availability of government information in both paper and electronic format.

Information security event logs are notification or alert that a device or software may be technically capable of producing, and are related to its status (e.g., configurations changes, log-on or log-off events), or its function and activities (e.g., data, traffic or sessions routed, transmitted, blocked, permitted). Information security event logging must always be enabled to provide context and data to support security investigation, audit, and monitoring.

Information security event logging is not limited to security devices, but is applicable to any and all devices, systems, software or applications that can produce logs that can be used to validate the confidentiality, integrity or availability of government information whether in security investigations, auditing or ongoing monitoring. Examples of devices, systems, software or applications that can produce information security logs include, but are not limited to, routers, switches, content filtering, network traffic flow, network firewalls, Intrusion Prevention/Detection Systems, servers, applications, databases, operating systems, application firewalls, authentication services, directory services, DHCP, DNS, and hardware platforms.

All devices, systems, software or applications that have logging capabilities must be configured to produce logs to enable the detection of security events and intrusions that otherwise would go undetected without such logging.

If the logging that the device or software is technically capable of producing is disabled or only partially configured, then this decision must be documented and include the rationale for deactivating or only
partially implementing the logging. The corresponding Security Threat and Risk Assessment must be updated to reflect this decision and must assess whether the risk introduced by the lack of logging is acceptable.

**Guidelines:**
The Information Incident Management Process should be part of the Ministry Business Continuity Program. The awareness program should build trust with employees and stress that “to err is human”. Positive reinforcement of good computing and reporting practices will help employees understand their responsibilities. Employees who commit errors that lead to security incidents should receive appropriate training and counselling.

**Recommended Tests:**
*Note: 1.1.2 is reported on as part of the annual information security review.*
- Demonstrate employees are made aware of the Information Incident Management Process.

### 1.1.3 Employees using the organization’s information systems must note and report any observed or suspected security weaknesses in those systems.

#### a) Reporting security weaknesses

**Purpose:** To assist in maintaining the security of information systems.

**1.1.3 a) Reporting information security weaknesses**
All employees must report as quickly as possible any observed or suspected security weaknesses in information systems. Ministries must follow the Information Incident Management Process for responding to suspected or actual security weaknesses which includes:

- Reporting to the Ministry Chief Information Officer, Risk Management Branch and Government Security Office, and the Office of the Government Chief Information Officer as appropriate. The response process must:
  - ensure all reports are investigated and handled in a secure, confidential manner, and,
  - ensure the individual who reported the weakness is advised of the outcome when the investigation is complete; and,
- A user awareness program on information security advising employees that:
  - they have a responsibility to report observed or suspected weaknesses to the Ministry point-of-contact,
  - suspected or observed weaknesses must not be tried or tested, and,
  - weaknesses should not be discussed, or made known, except through approved reporting channels.

**Guidelines:**
The reporting and response processes for all security weaknesses, threats, events and incidents should be consolidated to avoid duplication and establish a consistent approach.

**Recommended Tests:**
*Note: 1.1.3 is reported on as part of the annual information security review.*
- Demonstrate employees are made aware of the Information Incident Management Process as a mechanism for reporting security weaknesses.
1.1.4 Information security events must be assessed to determine if an information security incident has occurred.
   
a) Assessment of and decision on information security events

Purpose: To help assess and classify events to identify if they are information security incidents.

1.1.4 a) Assessment of and decision on information security events

The Chief Information Security Officer must assess each information security event using the agreed upon information security event and incident classification scale and decide whether the event should be classified as an information security incident. 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.

Results of assessments and decisions should be recorded in detail and provided to the Office of the Government Chief Information Officer.

Recommended Tests:

Note: 1.1.4 is reported on as part of the annual information security review.

- Demonstrate documentation identifying an information security event investigation escalation process.
- Demonstrate a formal review of an incident complete with recommendations.

1.1.5 Information security incidents must be responded to in accordance with the documented procedures.
   
a) Response to information security incidents

Purpose: To identify in advance of an information security incident, the authority to respond in a controlled manner.

1.1.5 a) Response to information security incidents

Information security incidents must be responded to by the Chief Information Security Officer and other relevant employees of the organization or external parties.

The response should include the following:

- Collecting evidence as soon as possible after the occurrence;
- Conducting information security forensics analysis, as required;
- Escalation, as required;
- Ensuring that all involved response activities are properly logged for later analysis;
- Communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations with a need-to-know;
- Dealing with information security weaknesses found to cause or contribute to the incident; and,
- Once the incident has been successfully dealt with, formally closing and recording it.

The goals of incident response are to resume ‘normal security level’ and to initiate the necessary recovery. Post-incident analysis should take place, as necessary, to identify the source of the incident.
Recommended Tests:

Note: 1.1.5 is reported on as part of the annual information security review.

- Demonstrate post incident analysis includes recommended corrective measures.

1.1.6 Knowledge gained from analyzing and resolving information security incidents must be used to reduce the likelihood or impact of future incidents.

a) Learning from information security incidents

**Purpose:** To identify and use information security incident trends to update the Information Security Policy, standards and supporting security processes.

1.1.6 a) Learning from information security incidents

The Chief Information Security Officer is responsible for monitoring and evaluating information security incidents by:

- Using statistical analysis of incident frequency, type and location to identify trends;
- Ensuring incident reports and trends are used to promote continuous improvement of security policies and processes, security awareness and training programs, and business continuity and disaster recovery plans;
- Advising Information Owners and Information Custodians and Ministry Information Security Officers of evolving security exposures and mitigation strategies;
- Evaluating the effectiveness of incident management, response and reporting; and,
- Evaluating the effectiveness of information security technologies.


The Information Security Branch, Office of the Government Chief Information Officer, is the centre of expertise and an essential capability in security incident protection, detection, response and correction where employees assigned responsibility for information incident management receive special training in managing crises across the spectrum of potential incidents.

The Information Security Branch must provide incident analysis to the Office of the Government Chief Information Officer and Risk Management Branch and Government Security Office as the focus of security incident reporting, management and improvement within government. Information sharing with stakeholder and partner organizations, other provincial security incident response centres and national incident response centres should also be fostered. Information security incident response must be integrated within the broader requirements for business continuity and disaster recovery. Integration will simplify processes, maintain consistency and eliminate duplication.

Continuous improvement of security incident management processes includes:

- Monitoring incidents using statistical analysis of frequency, types and locations of security incidents;
- Analysis of incidents, responses and successful containment;
- Determining requirements for user awareness and training;
- Improving the security of information systems through monitoring and reporting; and,
• Integrating automated alarms and other security incident detection technology with user reporting, checking logs and auditing systems.

Recommended Tests:

Note: 1.1.6 is reported on as part of the annual information security review.

• Demonstrate Information Owners, Information Custodians and Ministry Information Security Officers are made aware of security issues and an action plan is formulated to mitigate further risks of exposure.

• Demonstrate that information incident trends are analyzed to inform decision-making.

1.1.7 Investigations into information security incidents must ensure evidence is identified, collected, preserved, retained and presented in conformance with the rules for collection of evidence.

a) Information security incident investigation

b) Collection of evidence

Purpose: To ensure investigation processes preserve the integrity of evidence that may be required for legal or disciplinary action.

1.1.7 a) Information security incident investigation

Information security incident investigation must be formalized and practiced in accordance with standard investigation techniques:

• Information security incident investigation processes include:
  o identification of the incident cause,
  o planning of corrective action,
  o implementation of corrective action to prevent recurrence, and,
  o reporting action taken;

• Employees with responsibilities for information security investigations (investigating officers) must be aware of processes for securing potential evidence such as technology assets, audit logs, audit trails, voice mail and e-mail accounts for analysis and as potential evidence in legal proceedings;

• Inappropriate use of information and technology resources requires that within 48 hours the investigating officer contact:
  o in the case of an employee the individual’s excluded Supervisor and BC Public Service Agency (BCPSA) Labour Relations; and,
  o in the case of a contractor or business partner the contract manager or relationship manager;

• When criminal activity is suspected, the investigating officer must ensure that the appropriate law enforcement authorities are contacted. Before contacting law enforcement authorities, the Risk Management Branch and Government Security Office and the Office of the Government Chief Information Officer must be consulted;

• On resolution of an information security incident or weakness, the investigating officer must prepare a report that includes a detailed problem analysis, actions taken, and recommendations for corrective action or improvements; and,

• Information security incident reports must be submitted to Information Owners, Information Custodians, senior management, Office of the Government Chief Information Officer and Risk Management Branch and Government Security Office as part of security program management.
In order to enable quick, effective and immediate response to information security incidents and breaches, employees with responsibilities for security investigations (investigating officers) must be able to access security log data and security log data processing and reporting facilities immediately. This access will be for the purposes of evidence collection as well as security log parsing, searching, and reporting to enable identification, root cause analysis, and resolution of breaches and incidents. Access will be configured and enabled for on-line, real-time access to the GUI (Graphical User Interfaces)/Consoles/Interfaces of:

- The systems that generate and produce security log data and feature an interface that has reporting, parsing or searching functions with relation to the security log data it generates;
- The centralized log management system, service or facilities; and,
- The centralized monitoring system, service or facilities.

If the specific technology does not have a GUI/Console/Interface available, and instead relies on raw log data generation, equivalent functionality that permits the timely and effective searching of the security logs produced must be implemented.

1.1.7 b) Collection of evidence
At the outset of an information security investigation it may not be known if legal or disciplinary actions will result and what evidence will be required. To ensure proper procedures, confidentiality and information privacy, evidence must only be collected by individuals authorized by the Chief Information Security Officer.

- Evidence collection procedures must be documented by the Chief Information Security Officer;
- Investigative processes must follow the rules of evidence to ensure relevance, admissibility and materiality; and,
- Information Owners and Information Custodians in receipt of a legal order to produce electronic evidence must immediately contact the Chief Information Security Officer.

Guidelines:
In general, procedures for evidence collection should include identification, collection, acquisition and preservation of evidence in accordance with different types of media, devices and the status of devices (e.g., powered on or off). The procedures should take account of:

- Chain of custody;
- Safety of evidence;
- Safety of employees;
- Roles and responsibilities of employees involved;
- Competency of employees;
- Documentation; and,
- Briefing.

Recommended Tests:
Note: 1.1.7 is reported on as part of the annual information security review.

- Demonstrate that in instances that collection of evidence was required, that it was done under the direction of the Chief Information Security Officer.