Document Version: 1.0
Last Reviewed: April 2023

# 1. Purpose

To define the deliverables, and their associated roles and responsibilities, needed to provide a structured approach to manage a cybersecurity incident.

This document provides detailed security specifications to support the IMIT 6.31 Cybersecurity Incident Management Standard. Both the standard requirements and these specifications MUST be followed.

# 2. Resources

| | |
|---|---|
| Defensible Security Framework | Critical security controls (assessment and tools). |
| IMIT 6.18 Information Security Classification Standard | Four levels of security classification applied to government information based on expected harm that could result from unauthorized disclosure. |
| IMIT 6.19 Information Security Standard | Framework that helps government organizations meet their goals to protect government information and technology assets. |
| IMIT 6.31 Cybersecurity Incident Management Standard | Corresponding standard for these specifications. |
| Information Incident Checklist | Employee checklist for actual or suspected information incidents, including a privacy breach or privacy complaint. |
| Information Incident Management Policy | Framework for managing information incidents, including associated roles and responsibilities. |
| Information Security Glossary | List of information security terms and definitions. |
| Process for Responding to Privacy Breaches | Defines privacy breach and the steps to take when a breach occurs. |

# 3. Specifications

3.1 Managing cybersecurity weaknesses, events, and incidents

3.2 Key cybersecurity incident response activities

**Note:** "You" refers to your role as defined in the Responsibility Assignment Matrix (RACI table) found in Section 4.

## 3.1 Managing cybersecurity weaknesses, events, and incidents

### 3.1.1 Incident management procedures

The Information Security Branch (ISB), Office of the Government Chief Information Officer, is the centre of expertise and an essential capability in cybersecurity incident protection, detection, response, and correction.

A cybersecurity incident:

- Is a violation (or a possible threat to violate) of security policies and standards.
- Potentially or actually jeopardizes the confidentiality, integrity, and availability of an information system (including information).

You MUST:

1. Document the cybersecurity incident management procedures.
2. Ensure the procedures include:
   a. Planning and preparing incident responses.
   b. Monitoring, detecting, analyzing, and reporting of cybersecurity incidents.
   c. Logging incident management activities.
   d. Handling different types of cybersecurity incidents, including immediate action for containment, response escalation, and contingency plans.
   e. Roles and responsibilities of employees who are involved.
   f. Documenting and collecting relevant evidence.
   g. Security and integrity of the collected evidence regardless of evidence format (that is, chain of custody).

   h. Identifying and documenting the incident cause.
   i. Communicating to relevant partners, and escalating the incident, as required.
   j. Properly logging all involved response activities for later analysis.
   k. Advising and including all appropriate partners in the incident.
   l. When and where appropriate, recommending remediation activities to the appropriate party regarding the identified cybersecurity weaknesses that were found to cause or contribute to the incident.
   m. Once the incident has been successfully dealt with, formally closing and recording the incident, which may include:
      i. A report on detailed problem analysis
      ii. Actions taken
      iii. Recommendations for corrective actions or improvements
      iv. Follow-up lessons learned
   n. Recommending improvements for security controls, security policies and standards, and user awareness (including training).
   o. Investigating and handling all reports securely and confidentially.
3. Ensure employees are aware of and trained on the cybersecurity policies.
4. Provide support to OCIO during a cybersecurity incident investigation.
5. Ensure the individual who reported the weakness is advised of the outcome when the investigation is complete.

### 3.1.2 Reporting

You MUST NOT:

1. Discuss, or make known, weaknesses except through approved reporting channels.
2. Test suspected or observed weaknesses.

You MUST:

1. Develop and maintain processes for reporting cybersecurity weaknesses.
2. Submit reports to the Ministry Information Security Officer (MISO) for review and follow up.

3. Train and counsel employees who commit errors that lead to cybersecurity incidents.
4. Include requirements for reporting events and incidents in contracts and service agreements.
5. Make employees aware of processes and contacts to report cybersecurity weaknesses, events, and incidents.
6. Complete the following, as required by the Information Incident Management Policy:
    a. Immediately report all suspected or actual information security events to their supervisor. The supervisor will ensure that senior managers and your Ministry Chief Information Officer are also informed.
    b. Immediately notify the Office of the Government Chief Information Officer by dialing the OCIO Service Desk at 250 387-7000 or toll-free at 1 866 660-0811 and selecting Option 3. Seek guidance from your supervisor, if needed.
    c. If it is a cybersecurity event, ask for a Security Investigation otherwise ask 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 the next steps.
7. Report potential types of cybersecurity incidents, including any infrastructure or technical systems breaches or potential incidents that may result from a degradation of confidentiality, integrity, and availability from such systems/infrastructure.
8. Consolidate the reporting and response processes for all cybersecurity weaknesses, threats, events, and incidents to avoid duplication and establish a consistent approach.

## 3.2 Key cybersecurity incident response activities

### 3.2.1 Evidence collection

You MUST:

1. Ensure employees with responsibilities for cybersecurity investigations (investigating officers) are aware of processes for securing potential evidence,

such as technology assets, audit logs, audit trails, voice mail, and email accounts for analysis and as potential evidence in legal proceedings. Such employees MUST have the appropriate training relevant to their role.

2. Provide integrated digital forensics services, including artifact and forensic evidence analysis.

### 3.2.2 Cybersecurity event logs

You MUST:

1. Ensure that security logs are available from devices, applications, systems, and hardware.

### 3.2.3 Cybersecurity event or incident assessment

You MUST:

1. When criminal activity is suspected, follow established ministry and government procedures. Before contacting law enforcement authorities, consult with the Risk Management and Government Security Office, and the Office of the Government Chief Information Officer. Seek guidance from your supervisor, if needed.
2. Continuously improve incident response processes through various activities, including:
    a. Identifying trends and patterns, and escalating the findings to appropriate partners for awareness or further action.
    b. Using incident reports and trends to promote continuous improvement of security policies, standards, and processes; security awareness and training programs; and business continuity and disaster recovery plans.
    c. Advising Information Owners, Information Custodians, and Ministry Information Security Officers (MISO) of evolving security exposures and mitigation strategies.
    d. Evaluating the effectiveness of incident management processes, tools, response, and reporting.
3. Provide monthly updates on cybersecurity incident remediation status until completed.

## 4. Roles and responsibilities of the standard

The RACI table summarizes measurable deliverables. The role information after the table provides additional guidance.

**Responsibility Assignment Matrix (RACI)**

CISO = Chief Information Security Officer
DIR = Executive Director/Director/Manager/ Supervisor
E = Employee/Contractor
GCIO = Government Chief Information Officer

IC = Information Custodian
IO = Information Owner
MCIO = Ministry Chief Information Officer
MISO = Ministry Information Security Officer
V = Vendor

**RACI: R** = Responsible; **A** = Accountable; **C** = Consult; **I** = Inform

| | Roles | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **IMIT 6.31 Cybersecurity Incident Management Deliverables** | **CISO** | **DIR** | **E** | **GCIO** | **IC** | **IO** | **MCIO** | **MISO** | **V** |
| **Managing cybersecurity weaknesses, events, and incidents** | | | | | | | | | |
| 1. Documented incident management procedures (including regular reviews and exercises) for the government. (Section 3.1 and 3.2) | **AR** | | | | | | | | |
| 2. Documented and approved cybersecurity incident management procedures. (Section 3.1.1) | **A** | | **I** | | **R** | **R** | **I** | **C** | |
| 3. Business area cybersecurity incident management procedures. (Section 3.1.1) | | | | | **R** | **R** | **A** | **I** | |

| | Roles | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **IMIT 6.31 Cybersecurity Incident Management Deliverables** | **CISO** | **DIR** | **E** | **GCIO** | **IC** | **IO** | **MCIO** | **MISO** | **V** |
| 4. Ministry cybersecurity incident management procedures. (Section 3.1.1) | | | | | | **I** | **A** | **R** | |
| 5. Cybersecurity policies awareness and training. (Section 3.1.1 [3]) | | | **R** | | | | **A** | **R** | **R** |
| **Key cybersecurity incident response activities** | | | | | | | | | |
| 6. Collected and preserved incident evidence. (Section 3.2.1) | **AR** | | | | | | | | |
| 7. Integrated digital forensics services, including artifact and forensic evidence analysis. (Section 3.2.1 [2]) | **AR** | | | | | | | | |
| 8. Security logs from devices, applications, systems, and hardware. (Section 3.2.2 [1]). | | | | | **R** | **R** | **A** | **R** | |
| 9. Development and maintenance of relevant incident response tools and processes. (Section 3.2.3 [2]) | **AR** | | | | | | | | |
| 10. Monthly updates on cybersecurity incident remediation status until completed. (Section 3.2.3 [3]) | **I** | | **R** | | **R** | **R** | **A** | **R** | **R** |

## 4.1 Information Owner

**Responsible for**

1. Implementing OCIO-recommended incident remediation actions in a timely manner.
2. Ensuring that personnel are aware of the government's information security policies.
3. Ensuring that cybersecurity event and incident reporting requirements are in contracts.
4. Ensuring requirements for cybersecurity event and incident reporting are in contracts.
5. Reporting cybersecurity events to the MISO.

## 4.2 Information Custodian

**Responsible for**

1. Implementing remediation recommendations under the direction of the MISO, or Information Owner.
2. Reporting cybersecurity events to the MISO.

## 4.3 Ministry Chief Information Officer (MCIO)

**Accountable for**

1. Ensuring support to OCIO during a cybersecurity incident investigation.
2. Ensuring cybersecurity incident remediation recommendations are implemented.
3. Ensuring ministry post-incident reviews are conducted.

## 4.4 Ministry Information Security Officer (MISO)

**Responsible for**

1. Requesting that the Information Owner implement the OCIO recommendations from the cybersecurity incident.
2. Being the central ministry contact for employees to report cybersecurity weaknesses, events, and incidents.
3. Reporting cybersecurity events and incidents to the OCIO.

## 4.5 OCIO's Information Security Branch

**Responsible for**

1. Reviewing and analyzing reported cybersecurity events and cybersecurity incidents.
2. Providing artifact and forensic evidence analysis including, but not limited to, event logs, file system artifacts, malware samples, memory images, packet captures, network artifacts.
3. Providing remediation recommendations to the ministry.
4. Conducting post-incident reviews for significant incidents (for example, broad in scope/nature).
5. For any inappropriate use of information and technology resources, contacting the following within 48 hours:
   a. In the case of an employee, the individual's excluded supervisor, and the BC Public Service Agency (BCPSA), Labour Relations.
   b. In the case of a contractor or business partner, the contract manager or relationship manager.

# 5. Revision history

| Version | Revision Date | Author | Description of Revisions |
|---|---|---|---|
| 1.0 | March 2023 | Kristina Petrosyan | Document creation |

# 6. Contacts

For questions regarding these specifications, contact:

Information Security Branch, Office of the Chief Information Officer
Ministry of Citizens' Services
Email: InfoSecAdvisoryServices@gov.bc.ca