1. Purpose

To provide a structured approach to identify and quickly report information or cybersecurity activities related to managing a cybersecurity incident.

This standard includes establishing procedures and processes so employees know their role in reporting and mitigating cybersecurity events. Information collected about events can be analyzed to identify trends and to direct efforts to continually improve and strengthen the Province's information security infrastructure.

The IMIT 6.31 Cybersecurity Incident Management Specifications document provides detailed specifications for this standard. Both this standard and the specifications MUST be followed. This standard supplements the IMIT 6.19 Information Security Standard.

2. Scope

This IMIT 6.31 Cybersecurity Incident Management Standard applies to:

- All government organizations (ministries, public agencies, boards, and commissions) who are subject to Information Security Policy, Core Policy and Procedures Manual, and legislation.
- Contracted service providers conducting business on behalf of the B.C. government (or the contracted service providers must demonstrate compliance with ISO 27002:2022). Contracted service providers must also comply with other IM/IT standards as shown in Section 6.

Temporary exemptions to the standard can be requested from the Office of the Chief Information Officer.

3. Requirements

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

3.1 Managing cybersecurity weaknesses, events, and incidents

Ministries MUST have established and maintained processes to manage cybersecurity weaknesses, events, and incidents. The OCIO Information Security Branch leads all government-wide cybersecurity incident investigations. The Ministry Information Security Officer (MISO) is the central liaison contact with the OCIO and provides support as required throughout the incident. The MISO also provides interim remediation status updates to the OCIO until the remediation activities have been completed.

3.1.1 Incident management procedures

You MUST:

- Adopt and follow the established Information Incident Management Policy to report, manage, respond to, and recover from cybersecurity incidents. The processes are outlined in the specifications for this standard.
- Document incident response procedures before cybersecurity events and incidents occur. The incident response procedures must include:
    - Roles, responsibilities, authorities, and escalation processes to respond to an incident in a controlled manner.
    - Activities to contain and stop further harms from occurring, to remove the threat from the environment, and to recover normal business operations.
- Define and document employees' authorization for access to live systems and data.
- Train employees who have security incident management responsibilities. Ensure they understand the priorities for handling security incidents.
- Assess and classify cybersecurity events to determine if a cybersecurity incident has occurred.
- When a cybersecurity incident occurs, quickly and effectively provide access to all relevant primary data stores to the Security Investigations and Incident

Response Team (SIIRT) within the Office of the Chief Information Officer to ensure an orderly response to incidents.

- Conduct post-incident reviews after the incident has been resolved to determine possible process improvements.
- Document and regularly test and rehearse incident response processes to evaluate their effectiveness.

3.1.2 Reporting

You MUST:

- Immediately report cybersecurity weaknesses (such as information system misconfigurations or implemented system changes that provide unexpected results) to the Ministry Information Security Officer (MISO) for review and follow-up actions to limit further potential harm.
- Immediately report cybersecurity events and incidents to enable prompt response and identify government wide trends.
- Report cybersecurity events and incidents to the Office of the Chief Information Officer and the Risk Management and Government Security Office as appropriate for assessment.
- Submit the report on the cybersecurity incident findings to Information Owners, Information Custodians, senior management, Office of the Chief Information Officer, Risk Management and Government Security Office, and the Office of the Comptroller General, as appropriate.

3.2 Key cybersecurity incident response activities

3.2.1 Evidence collection

Evidence MUST be collected only by individuals authorized by the Chief Information Security Officer (CISO) to maintain confidentiality, privacy, and proper chain of custody. At the start of a cybersecurity investigation, it may not be known if legal or disciplinary actions will result and what evidence will be required. Evidence can occur

in many forms: physical or electronic (including security event logs, malicious code, or digital forensic artifacts).

You MUST:

- During cybersecurity incident investigations, ensure evidence is identified, collected, preserved, retained, and presented according to rules for collecting evidence. Following the rules preserves the integrity of evidence that may be required for legal or disciplinary action.
- Ensure the evidence collection procedures and processes are written and follow the rules of evidence to ensure relevance, admissibility, and materiality.
- Immediately contact the Chief Information Security Officer when you receive a legal order to produce electronic evidence.

3.2.2 Cybersecurity event logs

Cybersecurity event logs record the status of a device/software/application or system (for example, configuration changes) and the functions or activities attempted or performed (for example, network traffic that is blocked or routed) at a given time.

You MUST:

- Configure cybersecurity event logging on all devices, systems, software, or applications that have logging capabilities. The logs enable the detection of security events and intrusions that could otherwise go undetected without logging. Cybersecurity event logs may reveal an event or a pattern that could create a security incident. The logs provide context and data to support security investigations, audits, and monitoring (See IMIT 6.27 Operations Security Standard for logging requirements.)

3.2.3 Cybersecurity event or incident assessment

You MUST:

- Assess each cybersecurity event using the approved incident classification scale to decide whether the event should be classified as a cybersecurity incident.
- Record assessment and decision results in detail.
- Provide the assessment and decision results to the Office of the Chief Information Officer (OCIO).

4. Supporting documents

Cyber Security Incident Response Process

IMIT 6.18 Information Security Classification Standard

IMIT 6.31 Cybersecurity Incident Management Specifications

Information Incident Management Policy

5. Definitions

Information Security Glossary

6. Authority

Core Policy & Procedures Manual (CPPM)

IMIT 6.19 Information Security Standard

Information Security Policy

7. Revision history

Version	Revision Date	Author	Description of Revisions
2.0	March 2023	Kristina Petrosyan	Content improvement
	March 2022	Sarah Browning	New template, formatting

8. Contacts

For questions regarding this standard, contact:

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