Cyber security incident management

Context

This document outlines Victoria Police requirements for the management and reporting of cyber security incidents and ensures that Victoria Police's approach is consistent with overall State and Federal Government security policy and the Commissioner for Privacy and Data Protection and Law Enforcement Data Security standards.

This policy must be read in conjunction with **VPMP Protective security incidents. Cyber security incident management standard** supports these policies by setting the requirements for our Business and Technology Owners and IT Service Providers.

Application

Policy Rules are mandatory and provide the minimum standards that employees must apply.

Non-compliance with or a departure from a Policy Rule may be subject to management or disciplinary action. Employees must use the Professional and Ethical Standards to inform the decisions they make to support compliance with Policy Rules.

These Policy Rules apply to every authorised user of Victoria Police information.

Rules and Responsibilities

1. Overview

Cyber security incident management enables timely containment, mitigation and recovery from incidents. It also reduces the impact on Victoria Police's service delivery, community safety and public confidence and those of its partner agencies.

A Cyber security incident is defined as:

a single or a series of unwanted or unexpected cyber security events that have a significant probability of compromising Victoria Police operations and objectives and threatening information security. As an example, this could be receipt of an email with suspicious links or attachments, unusual or unexpected activity following Internet browsing, inability to access files, pop-up notices and unusual or unexpected activity following use of a removable media device such as a USB stick.

A *cyber security event* is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

2. Accountabilities

2.1 Cyber security incident management

- The IT Security Adviser (ITSA), Information, Systems, and Security Command (ISSC) is accountable for cyber security incident management.
- The responsibility for cyber security incident management and response oversight is delegated to the IT Security Incident Manager (ITSIM).
- Victoria Police's approach to cyber security incident management and the obligations of Business and Technology Owners and IT Service Providers are documented in **Cyber security incident management standard.**

2.2 Detection and recording

- Business owners are accountable for configuring critical information systems to monitor and record information security events where the system functionality is available. Where system functionality is not available, a remediation plan must be developed and a security risk must be escalated to the ITSA for formal acceptance by the Security Executive and CIO.
- Victoria Police IT and its IT Service Providers are accountable for the provision, configuration and maintenance of system logging functionality, tools and procedures to detect and record cyber security events. This ensures the provision of timely reports of security events and incidents to the ITSA and ITSIM.
- Where an IT system, function or service is outsourced, the Service Provider must report all suspected or actual cyber security incidents to the ITSIM.

3. Reporting and response

3.1 Employees, IT Service Providers and other third party service providers

- As soon as possible after any cyber security incident is identified, employees, including IT Service Providers and other third-party service providers and their employees and partner agencies, must report all cyber security incidents to:
  - a Line Manager
  - the IT Service Provider Helpdesk (Tel: 1300 307 082 or email: VP IT Helpdesk-MGR)
- Where a cyber security incident is found to have occurred, Victoria Police IT Service Providers and their employees and partner agencies are required to report all confirmed cyber security incidents to the ITSIM or via email to IT-SECURITY INCIDENTS-MGR.

- Where an IT system, function or service is outsourced, the IT Service Provider must report all suspected or actual cyber security incidents to the ITSIM as soon as possible after an incident is discovered.

- Victoria Police's approach to cyber security incident management and the obligations of IT Service Providers are documented in **Cyber security incident management standard.**

3.2 Work Unit Managers

- All Victoria Police, IT Service Provider and partner agency Work Unit Managers must ensure that all cyber security incidents are reported by employees, IT Service Providers and partner agencies to the Victoria Police IT Service Provider Helpdesk as soon as possible.

- Reporting of cyber security incidents to the Victoria Police IT Helpdesk does not remove the obligation of employees, IT Service Providers and other third-party service providers and Work Unit Managers to complete any other reporting or actions required by their position with respect to operational activities, policy or instructions.

- Work Unit Managers must assist the ITSIM and the Cyber Security Incident Response Team (VP-CSIRT) in the remediation of all cyber security incidents.

3.3 IT Security Adviser

The ITSA is accountable for reporting cyber security incidents to the Agency Security Advisor (ASA), the Security Executive and CIO and, as directed by the ASA and CIO, to Victoria Police Media and the Chief of Staff.

3.4 IT Security Incident Manager

The ITSIM is responsible for:

- oversighting the response to cyber security incidents
- engaging the VP-CSIRT and the CERT where specialist services are required, including but not limited to, forensic analysis and reverse engineering of security incidents
- reporting all confirmed cyber security incidents to the ITSA, the ASA, the Security Executive, the CIO and the Security Incident Registry (SIR).
- conducting post-incident reviews and reporting.

4. External reporting of cyber security incidents

- The ITSA is responsible for:
  - external reporting of cyber security incidents in compliance with the Commissioner for Privacy and Data Protection and Law Enforcement Data

Security standards, the Australian Government Protective Security Policy Framework (PSPF) and the Information Security Manual
- reporting cyber security incidents to the Australian Signals Directorate, following approval by the CIO or nominated delegate.

- Work Unit Managers or Victoria Police IT Service Providers are not to report cyber security incidents externally or to other investigative authorities unless required by law, policy or other agreement.

Quick Links

- **Victoria Police Standard - Cyber security incident management**

Further Advice and Information

For further advice and assistance regarding these Policy Rules, contact the ITSA, Protective Security, your Work Unit Manager or your direct supervisor.

Update history

Date of first issue	26/10/15	FF-090855
Date updated	**Summary of change**	**Force File number**
25/03/19	Administrative amendment to reflect name change from IMSSD to Protective Security.	FF-139207