Protective security incident reporting and containment

Source Policy

These Procedures and Guidelines support and must be read in conjunction with the following:

- VPMP Protective security incidents
- VPMP Cyber security incident management
- VPMP Physical Security

Application

Procedures and Guidelines are provided to support the interpretation and application of rules and responsibilities. They include recommended good practices and assessment tools to help employees make lawful, ethical and professional decisions. Employees should use the **Professional and ethical standards** to inform the decisions they make to support interpretation of Procedures and Guidelines.

Procedures and Guidelines are not mandatory requirements on their own. However, where rules and responsibilities state that employees must have regard to Procedures and Guidelines, the Procedures and Guidelines must be used to help make decisions in support of the rules.

Procedures and Guidelines

1. Overview

Reporting of protective security incidents enables mitigation and remedial actions to be taken, identification of trends and promotion of ongoing awareness of security issues. When a protective security incident is identified, the correct response will ensure that the nature of the incident can, where ever possible, be isolated from other impacts and controlled.

1.1 Protective security incident reporting

Every protective security incident must be reported to the Security Incident Registry (SIR), Information Systems and Security Command.

Protective security incidents include, but are not limited to:

- Unauthorised access to Victoria Police facilities or facilities in control of Victoria Police (ie redundancy sites for business continuity purposes).
- Loss or theft of, unauthorised access to, or disclosure of, Victoria Police information or security equipment (including access cards and combination/keys to security containers). This includes:
  - access attempts by unauthorised users (whether successful or unsuccessful);
  - attempts to access information for any unauthorised purpose by an authorised user (whether successful or unsuccessful); or,
  - unauthorised use of information by authorised users.
- Unauthorised access to, loss or damage of, and/or use of, Victoria Police information communications and technology equipment or systems – including either directly or through malicious software.
- Loss or theft of, unauthorised access to and/or use of, Victoria Police radio equipment or systems.
- Inappropriate handling, storage or disposal of Victoria Police information – Including destruction without appropriate approval or inability to locate official records (after all appropriate avenues of inquiry are exhausted).
- Unsolicited encounters with people or organisations that seek to obtain Victoria Police information through unauthorised means.
- Espionage or sabotage affecting the service delivery of Victoria Police.
- IT related events deemed to be a security incident by the IT Security Advisor.

1.2 Employee and contractor responsibilities

In accordance with **VPMP Protective security incidents** all employees, contractors and service providers must, as soon as possible, notify their line manager and the SIR of any identified protective security incident whether deemed intentional, accidental, human error, IT or system related.

2. Initial action – Work Unit Managers

Work Unit Managers must ensure that:

- all security incidents are reported by employees and contractors to the SIR as soon as possible.
- isolation, containment and remediation occur at a local level as soon as possible for all security incidents:

- the aim of isolation is to quarantine the event leading to the incident so that it represents the nature of the occurrence at the time it occurred.
- the aim of containment is to keep the incident under control and to prevent the issue spreading or escalating.

- an assessment of the known facts to determine the urgency of reporting and the most appropriate actions in response to the protective security incident is conducted. This assessment and subsequent actions are not a substitute for reporting a protective security incident.

3. Methods of reporting

3.1 Reporting a protective security incident

- The method of reporting a protective security incident will vary depending on the nature of the incident and the perceived urgency of investigative or remedial actions.

- Protective security incidents urgent in nature should be initially reported by telephone to the SIR.

- All reports of protective security incidents to the SIR must be formally reported in writing by using the - **Security Incident Report Form**. (Available on the SIR intranet page).

- Security Incident Registry can be contacted:
  - Email – SECURITY INCIDENT-PROTECTIVE SECURITY- MGR
  - Phone - 03 9628 7335 or 03 9628 7282 (Business hours)
  - For urgent matters contact Police Communications D24 Police Shift Manager Phone - 03 9247 3222

- Incidents involving police radios and communications – contact Police Communications (D24) for directions in accordance with **VPMP Managing equipment and assets** and **VPMP Operational safety and equipment**. D24 will notify the SIR or Professional Standards Command (PSC) when appropriate.

- Incidents involving criminal activity or where an employee is, or has been, engaged in any:
  - misconduct
  - corruption
  - detrimental action against a person making a protected disclosure or internal source

  report to PSC or other appropriate area in accordance with **VPMP Complaints and discipline**. The SIR will be notified by PSC or other appropriate area when appropriate.

- Incidents involving ICT equipment or services – Including malicious software and intrusion attempts contact the IT service provider helpdesk. The helpdesk will notify the IT Security Services when appropriate.

3.2 Post reporting actions

After reporting of security incidents to SIR the following actions will be undertaken:

- An incident assessment will be conducted by SIR. This will determine the reporting timeframes and requirements.
- SIR will co-ordinate with the local Work Unit Manager to ensure all containment activities and reporting requirements are fulfilled.
- For further details on SIR post reporting responsibilities refer to **VPMG Protective security incident management.**

Further Advice and Information

For further advice and assistance regarding these Procedures and Guidelines, contact the Security Incident Registry, Information, Systems and Security Command

Update history

Date of first issue	30/03/15	FF-088999
Date updated	**Summary of change**	**Force File number**
26/03/18	Administrative- phone number updated	FF-124154
25/03/19	Administrative amendment to reflect name change from IMSSD to Protective Security.	FF-139207