

Victoria Police Manual – Policy Rules

IT equipment and software

Context

The primary legal source of Victoria Police's information security obligations is the **Standard for Law Enforcement Data Security (SLEDS)**. The 43 Standards developed by the Commissioner for Law Enforcement Data Security outline necessary controls for the secure management of law enforcement data systems and the information they contain. Law enforcement data systems include all relevant data repositories and are not limited to computer systems.

Victoria Police also has an obligation to comply with the **Australian Government protective security policy framework** and the **Information security manual** which describe the minimum standards for physical and information security for all Federal and State government agencies.

These policy rules on the purchase, use, maintenance and disposal of IT equipment and software support Victoria Police's compliance with the above manuals and standards.

The security of IT equipment and software plays an important role in maintaining the confidentiality, integrity and availability of Victoria Police information and authorised personnel must familiarise themselves with their responsibilities on this topic.

These Policy Rules provide personnel with the details of their responsibilities for the secure purchase, use, maintenance and disposal of IT equipment and software.

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 applies to all employees.

Rules and Responsibilities

1. Procurement requirements

- Any IT equipment and software purchased outright by Victoria Police Work Units must comply with Chapter 7.5, **Victoria Police Accounting Manual** and be obtained in accordance with **VPMG Obtaining IT equipment and services**.
- IT equipment owned by Victoria Police must be registered on the Assets Register or in the Portable and Attractive Items Register (PAIR) depending on its value, in accordance with **VPM 212-2 Managing equipment and assets**.
- IT equipment leased by Victoria Police must be registered by the outsourced IT Service Provider on their Assets Register easily accessible to Victoria Police employees authorised to view it.
- The physical security of all IT equipment and software equipment located in specific work units is the responsibility of the relevant Work Unit Manager.
- The acquisition and development of law enforcement data systems must comply with *SLEDs 25* and *26*.

2. Maintenance requirements

- Maintenance of IT equipment and software must be carried out onsite wherever possible.
- No maintenance may occur outside of Victoria Police premises unless prior contractual arrangements have been formalised with the Vendor or Service Provider which ensure that repairs are to be made:
 - under suitably secure conditions
 - by personnel authorised by Victoria Police.
- Only personnel who have:
 - the appropriate security clearance and
 - been authorised by the relevant System Sponsor(s)
 may undertake these duties unsupervised. All other maintenance personnel must be under the direct supervision of a Victoria Police employee or contractor nominated by the relevant System Sponsor(s). The removal of diagnostic data or the replacement of defective parts during a maintenance visit must be authorised by this supervising employee or contractor.
- All reasonable steps must be taken to prevent non-Victoria Police maintenance personnel:

- accessing information other than that required to carry out their task;
or
- taking action that may subvert the system's security safeguards.

3. Movement requirements

Where IT equipment (already connected to Victoria Police IT network and/or information systems) needs to be moved to another work area, prior consultation with the local IT Coordinator is required to ensure compliance with any conditions imposed by the System Sponsor for the ICT Infrastructure. If the equipment is not connected then the appropriate register must be updated to reflect the move.

4. Disposal requirements

- IT equipment that contains Victoria Police information or software must not be removed from Victoria Police premises for disposal unless all information and licensed software on the storage media has been overwritten and declassified, as required by *SLEDS 13* and *22*).
- All sensitive and/or security classified information stored on IT equipment must be sanitised and declassified (and, where applicable, disposed of) according to:
 - the highest classification of information ever contained on the storage media
 - the degree of risk associated with a breach of the confidentiality or security classification of the information.
- Prior to sanitisation, declassification and/or disposal, no official information contained on the storage media of IT equipment is to be deleted unless:
 - it is covered by an authorised disposal schedule issued by the Public Records Office of Victoria (refer to **VPMP Information review, retention and disposal**) or
 - a copy has been formally retained elsewhere.
- Before sanitising IT equipment or physically removing storage media from IT equipment personnel must contact one of the following areas for assistance and advice:
 - the local IT Coordinator
 - the relevant I&IT Business Engagement Manager, or
 - the IT Customer Service Centre.
- Failed IT equipment storage media that cannot be sanitised and any storage medium that has not been sanitised must be conveyed to I&IT Department by hand for controlled destruction.

5. Portable computing devices

5.1 General

Victoria Police portable computing devices (PCDs) are small, portable devices that can store and transport large amounts of electronic information or enable connection with the Victoria Police network. PCDs include USB memory sticks, digital cameras, laptops, personal digital assistants, smartphones (e.g. BlackBerry) and portable hard-drives.

In work areas where the use of PCDs is used the following conditions must be complied with:

- PCDs must only be connected either physically or via a wireless link to the Victoria Police network if they are:
 - an approved Victoria Police device
 - checked and certified virus-free by the authorised Victoria Police virus scanning software accessible on all Victoria Police computers for that purpose prior to use
 - only be used for authorised purposes
- Only authorised software is to be installed or used PCDs.
- For specific requirements relating to smart phones, see section 6.

5.2 Work Unit Manager responsibilities

Work Unit Managers must assign a Victoria Police employee as the custodian to all PCDs in their Work Unit to be responsible for the protection of the PCD and the Victoria Police information it contains, as follows:

- keep the device secure at all times and if it contains sensitive and/or security classified information that this is protected, in accordance with **VPMP Information use, handling and storage** and as required by Chapter 10 of the *SLEDS*. The required level of security must be provided irrespective of whether the PCD is in use, in transit, or in storage
- not allow the device to be transferred to another authorised person without first erasing or sanitising the information stored on the PCDs storage media that the recipient is not authorised to access, as required by *SLEDS 22*
- before any maintenance occurs on the device storing:
 - Victoria Police information, the information is backed up (and securely stored) and
 - sensitive and/or security classified and unencrypted, the storage media is sanitised, or physically removed from the PCD, as required by *SLEDS 28*.

- ensure that, where sensitive and/or security classified information is likely to be created or stored on the device a security safeguard is installed that a user is required to use a password before access is granted to the information stored on the device and ensures all sensitive and/or security classified information stored is fully encrypted, as required by *SLEDS 18* and *23*
- adequate physical security measures must be established, as required by *SLEDS 15*.

5.3 ***Custodian responsibilities***

Nominated custodians must ensure that:

- PCDs with a market value at or above the asset threshold as defined in the *Victoria Police Accounting Manual*, Chapter 10: Physical and Intangible Assets, section 3 under Policy/Procedure) are recorded on the Assets Register
- PCDs with a market value less than the asset threshold (excluding GST) are either recorded:
 - in the local Portable & Attractive Items Register (PAIR) for accountability and audit purposes or
 - in a Register for the specific management of PCDs so that details of who used the PCD and the dates it was signed-out and returned can be monitored.

Either of these options provides a convenient means of tracking Victoria Police PCDs for audit purposes, and assists when PCDs are reported lost or missing.

5.4 ***Lost or stolen PCD***

Lost or stolen PCDs must be reported through the Work Unit Manager to the Security Incident Manager, Protective Security, I&IT Department as soon as practicable after the incident, as required by *SLEDS 32*.

For best practice guidelines on the secure management of PCDs, Work Unit Managers and Custodians should have regard to **VPMG Managing portable computing devices**.

6. Smartphones

6.1 ***Eligibility***

- Authorised smartphones (e.g. BlackBerry) provide mobile access to Victoria Police networks. Approval to obtain a smartphone must be obtained from a Department Head.
- To be eligible to apply for a smartphone, employees must be either:

- an Inspector or above, VPSG-7 or above, and
 - able to demonstrate that they require the portable functionality provided by the device to complete their duties effectively
- or
- an Emergency Response Co-ordinator (see **VPMP Emergency Management Response**)
- Contractors are only eligible to apply for a smartphone in exceptional circumstances.
 - Department Heads must approve any allocation of smartphones. Approval must only be given if the Department Head is satisfied that the employee has a demonstrable need for portable access to the Victoria Police network and alternatives (e.g. Telstra NextG cards and laptops) are impracticable.
 - Members who are allocated smartphones must also have regard to **VPMP Operational duties and responsibilities** when undertaking patrol duties.

6.2 *Accessing allowances*

Employees approved to use smartphones are only eligible for availability (police members) or standby (VPS employees) allowances where they have been rostered or directed to be available for work in accordance with applicable workplace agreements (cl. 13.5, **Victoria Police Workplace Agreement 2007** and cl. 30.5, **2009 Extended and Varied Version Victorian Public Service Agreement 2006**).

6.3 *Ordering and maintenance*

- Smartphones must be:
 - purchased in accordance with the IT Catalogue, see **VPMG Managing portable computing devices** for approval process
 - funded by the employee's Work Unit.

For guidance on purchasing these devices refer to **VPMG Managing portable computing devices**.

- Only corporate SIM cards can be used.
- Employees approved to carry a smartphone must also have regard to **VPMG Managing portable computing devices** in relation to the ongoing maintenance of these devices.

Quick Links

- *SLEDS:*
 - Release (Std 13)*
 - Physical Security (Stds 15, 18)*
 - Electronic Data Storage Devices (Std 22)*
 - Cryptographic Controls (Std 23)*
 - Data Systems Acquisition and Development (Stds 25, 26)*
 - Security Classified Law Enforcement Data (Std 28)*
 - Security Incident Management (Std 32)*
- VPMP ICT security
- VPMG Managing portable computing devices
- VPMG Obtaining IT equipment and services
- VPM 212-2 Managing equipment and assets
- Standards for Victoria Police Law Enforcement Data Security

Further Advice and Information

For further advice and assistance regarding these Policy Rules, contact your local IT Co-ordinator or your supervisor.

Update history

Date of first issue	22/02/10	
Date updated	Summary of change	Force File number
06/12/10	Inclusion of references to specific CLEDS Standards that apply to this policy and name changes to the Commonwealth protective security manual to Australian Government protective security policy framework and Information and communication technology security manual to Information security manual.	061979/10
04/01/11	Replacement of exact value of asset threshold in Section 5 with a reference to Chapter 10, Section 3 of the <i>Accounting Manual</i> for current value	064270/10
07/11/11	Inclusion of instruction relating to smartphones (section 6) and amendment at section 5 to reinforce guideline requirements.	059316/09
18/11/13	References to redundant instruments following IMSSD review have been updated with corresponding new instruments.	069562/11

07/12/15	Legislative reference update to <i>Privacy and Data Protection Act 2014</i> .	FF-096355
25/03/19	Administrative amendments to update IMSSD to Protective Security.	FF-139207