Victoria Police Manual – Policy Rules

Information use, handling and storage

Context

Public confidence in the ability of the Victoria Police to manage all information effectively, including personal, sensitive and classified material, requires the application of the highest standards in information management practices which govern information confidentiality, integrity and availability.

The primary legal source of Victoria Police's *information management* obligations is the ***Public Records Office of Victoria (PROV) Standards*****.** The standards and supporting specifications developed by PROV apply to all Victoria Police information and detail requirements for the creation, maintenance and security of public records including the selection and disposal of public records not worthy of preservation. Records include all law enforcement data systems, corporate or other data repositories, archives and computer systems and the term is not limited to hardcopy records.

The primary legal source of Victoria Police's *information security* obligations is the Commissioner for Privacy and Data Protection (CPDP) ***Standards for law enforcement data security (2014)*****.** The Standards developed by CPDP 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 the term is not limited to computer systems.

This instrument provides the Victoria Police rules for the appropriate management of information, in line with the above requirements, the **Victoria Police Information Management Principles,** the **Australian Government Protective Security Policy Framework (PSPF)** and the **Australian Government Information security manual (ISM)**.

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 Authorised Users of Victoria Police information.

Rules and Responsibilities

1. Information Use

1.1 Principles

Victoria Police information use should occur in line with the Victoria Police information Management principles:

- Use of Victoria Police information supports business processes and functions and must only be used for official purposes.

- All Authorised Users are responsible for the security of Victoria Police information that they access or hold.

- Victoria Police information will be analysed and risk assessed for its accuracy, value and sensitivity. This analysis and assessment must:
  - determine actions
  - identify priorities
  - identify links with other Victoria Police information recorded elsewhere
  - identify any inherent risks.

1.2 Appropriate use of Victoria Police information

- In accordance with **VPMP Appropriate use of information**, Authorised Users:
  - must only access and use Victoria Police information where they have a demonstrable, legitimate business need which is directly related to the performance of their current duties with Victoria Police
  - are responsible for the security of Victoria Police information that they access or hold.

- Should material be considered for release into the public domain, it must be authorised in accordance with **VPMP Information sharing**.

1.3 Personnel considerations

- In line with **VPMP Information access**, pre-employment checks only provide clearance to access and handle UNCLASSIFIED Victoria Police information.

- Where an employee or other person will access or handle information security classified at PROTECTED or above, an appropriate security clearance must be obtained prior to providing access to the information. See **VPMP Personnel security** for policy rules on security clearances.

1.4 Physical and environmental considerations

- In accordance with **VPMP Information access**, Authorised Users must ensure that all non public domain information is physically protected from viewing, hearing or access by persons that do not have approval to access the information.

- Prior to the use of protectively marked Victoria Police information, Authorised Users are to critically assess their work area. This assessment must be based on the minimum security controls for the classification level of the information.

- The Authorised User should assess if the area is appropriate to:
  - protect Victoria Police information from oversight, or overhearing (audio secure) by other people
  - securely store Victoria Police information within the work area
  - securely store any information communication technology equipment on which Victoria Police information will be accessed and/or contained.

- As far as practicable within a facility, Work Unit Managers are to ensure that photocopiers, fax machines, shredders, and printers are located in areas where activity cannot be conducted unobserved.

1.5 Information communication technology (ICT) considerations

- In accordance with **VPMP Appropriate use of information**, Authorised Users must not take unacceptable risks in the transfer and storage of information.

- Victoria Police information must not be stored or transmitted using internet based systems or accounts unless specifically authorised by the Information Management Committee and/or VPM policy. Refer to the following guides for approved uses:
  - **VPMG Use of email**
  - **VPMG Use of internet**

- Authorised Users must not access Victoria Police information from public computers or other public ICT communication devices.

- Personally owned ICT devices may only be used to process UNCLASSIFIED Victoria Police information if all security and usage requirements are adhered to. Refer to:
  - **VPMG Portable recording devices**
  - **VPMG Portable computing devices**
  - **VPMG Home based work**

- Personally owned ICT devices may only be used to remotely access the Victoria Police network or store Victoria Police information:
  - when the device is able to segregate and protect Victoria Police information or used to remotely access the Victoria Police network through approved secure method (such as Connect. Police tokens or Good for Enterprise) **and**
  - all security and usage requirements for the application / connection are adhered to. Refer to the official procedure documents for the particular method for details.

1.6 Misuse of Victoria Police information

- The accidental or deliberate failure to observe requirements around the handling of official resources (including Victoria Police information) is identified as a security incident.

- Refer to **VPMP Protective security incident reporting and management** for more information on the categories of security incidents, as well as reporting procedures.

2. Information Handling

2.1 Personal and health information

All personal and health information held by Victoria Police, whether or not it is also in the public domain, must be managed in accordance with the Information Privacy and Health Information Privacy Principles. Refer to **VPMG Information privacy** for further information.

2.2 Protectively marked information

- Authorised Users must comply with any protective markings (including security classifications, caveats and dissemination limiting markers (DLMs)) on the material to ensure it is handled in accordance with minimum security controls of the information.

- Refer to **Protective Security guide – G200 – Assessment and handling of Victoria Police Information** for clarification on particular handling requirements for individual security classifications and protective markings.

2.3 Legacy security classified information

- Victoria Police information that has been protectively marked under the former Protective Security Manual (PSM) scheme is now referred to as 'legacy' classified information.

- In accordance with **VPMP Information categorisation, collection and recording**, legacy classified information that is being actively used, should be reclassified against the new classification scheme (which aligns to the PSPF) and marked appropriately.

- Inactive legacy classified information does not need to be reassessed.

- There is not a direct correlation between legacy markings and current markings. Within Victoria Police, the approved minimum handling requirements to be used for inactive information or information equipment for legacy classified information are:

Legacy classification / marking	Use handling requirements for (in accordance with the PSPF classification scheme)
X-IN-CONFIDENCE (excluding Cabinet-in-confidence)	Dissemination Limiting Markers (DLM)
RESTRICTED	PROTECTED
HIGHLY PROTECTED	SECRET
CABINET-IN-CONFIDENCE	PROTECTED Sensitive: Cabinet

2.4 Information from other areas

- Information received from other internal work units or external agencies must be provided the same and no less protection as that given by the originating work unit or agency. This includes taking care to identify and comply with any instructions, protective markings and additional requirements.

- Authorised Users receiving information from other agencies that is marked as 'Accountable Material' must contact the Information Security Manager, Protective Security for advice on specific handling instructions.

2.5 Securing information

- All Victoria Police information must be secured appropriately when unattended. Refer to **VPMG Clear desk principles** for guidance.

- Protectively marked information must be secured in a container appropriate to the protective marking when not in use. Refer to **Protective Security Factsheet – F230 – Physical and digital storage requirements** for details on appropriate physical storage containers.

- ICT equipment and media that have been used to process or store protectively marked and security classified information must be protected to the same degree as paper-based security classified information.

2.6 Movement of information

- Protectively marked information has specific requirements around its movement and in particular approved methods of transfer.

- The appropriate method of transfer is dependent on the:
  - security classification of the material
  - format that the information is in (i.e. digital or hardcopy)
  - media type on which the information resides.

- All Authorised Users of Victoria Police information must ensure transfer methods (physical or electronic) are appropriate for the information and any associated protective markings. Refer to **Protective Security Factsheets – F230 Physical and digital storage requirements** and **F180 Protective barriers for transfer of Security Classified information** for further details.

- Refer to **Protective Security guide – G200 – Assessment and handling of Victoria Police Information** for specific instructions on the requirements for the transfer of different categories of protectively marked information.

2.7 Removing security classified information from Victoria Police premises

- The removal of security classified information from Victoria Police premises requires:
  - a security risk assessment to be conducted by the Work Unit Manager to ensure there is a justifiable need to remove the material from the Victoria Police site
  - subsequent authorisation provided by management for the removal
  - a record of the assessment and authority for accountability purposes
  - the Authorised User who is to remove the information to be aware of the risks involved, and accept responsibility for the safe custody of the information.

- For further information on handling requirements for protectively marked and security classified information refer to **Protective Security guide – G200 – Assessment and handling of Victoria Police Information**.

2.8 Movement outside Australia

- Special care must be given to protectively marked and security classified information when taken overseas.

- Authorised Users are to contact the Information Security Manager, Protective Security to obtain advice on the most appropriate method of despatch and handling requirements.

2.9 Receipts

- A receipt provides a valuable means of tracing the movement of a package and provides a level of assurance that the recipient will be responsible for the protection of the material contained within it.

- Receipts must be used when transferring security classified information externally. For further information on when receipts should be used and when recording in a Classified Document Register is required, refer to **Protective Security guide – G200 – Assessment and handling of Victoria Police Information**.

2.10 Copying security classified information

- Prior to the reproduction of protectively marked and security classified information, authorisation must be granted from the originator.

- ICT equipment used to reproduce security classified material (photocopiers, fax machines etc) must not be used to copy information classified higher than the IT system to which the device is connected to. The general Victoria Police IT network is only able to process and store information below PROTECTED.

- For information on producing copies of protectively marked or security classified information, refer to **Protective Security guide – G200 – Assessment and handling of Victoria Police Information**.

- Accountable material, i.e from an external source, once disseminated is not to be copied or reproduced in any form. If additional copies are required they are to be requested from the original source.

3. Storage

- Authorised Users are to ensure that all Victoria Police information is kept secure from theft, damage, loss and unauthorised access.

- Work Unit Managers must ensure that all active official information must be stored in their workplaces in accordance with the following conditions:
  - is stored in facilities that are commensurate with the level of security protection required - refer to **Protective Security Factsheet – F230 – Physical and digital storage requirements** for suitable types of containers
  - is secure from public and unauthorised access
  - is protected as far as practical from disaster and destruction
  - only electronic information that is regularly required, either as a reference or is currently being worked on is to be stored on the shared or personal directories of the IT network

  - is security classified information must not be archived in H drives, emails or in personal storage containers.

- All Authorised Users must ensure that all official digital based information/data (including all information relevant to your work area such as briefs or correspondence) is saved to either:
  - a Victoria Police Network shared drive folder
  - non-rewritable DVD/CDs and securely stored/filed on Victoria Police premises
  - a Victoria Police application or system that is security classified at or above the rating of the information.

- In accordance with **VPMP Information review, retention and disposal**, Work Unit Managers must ensure that all inactive information is identified through regular reviews and appropriately archived.

- Storage caveats on information must be complied with.

- Information should only be stored on a portable flash device (USB, external hard drive, etc.) as a temporary measure and should not be used as a permanent storage option. Refer to **Protective Security Factsheets F020 – Victoria Police approved USB devices**; **F021 – Choosing a USB Flash device** and **F022 – How to select an appropriate USB flash device** for more information.

- Work Unit Managers should use **Protective Security checklist - C090 - Local Documentation Information Security Checklist** to assist with ensuring that all issues are addressed.

- Refer to **Protective Security guide – G200 – Assessment and handling of Victoria Police Information** for more information on specific requirements for different levels of protectively marked or security classified material.

Personal drives

- Personal drives (H:\drives) are limited to 500MB capacity. All Authorised Users must ensure that information stored in personal drives on the Victoria Police Network is limited to:
  - personal / personal administrative / personal reference material or information
  - temporary storage of transient information eg. VP form data that is subsequently submitted via email or other system.

Quick Links

- PROV Standards
- CPDP Standards
- VPMP Information access
- VPMP Appropriate use of information
- VPMP Information use, storage and handling
- VPMP Information sharing
- VPMP Information review, retention and disposal
- VPMG Information privacy
- VPMG Portable recording devices
- VPMG Portable computing devices
- VPMG Digital asset management
- VPMG Use of email

Further Advice and Information

For further advice and assistance regarding these Policy Rules, contact Protective Security.

Update history

Date of first issue	15/10/13	
Date updated	**Summary of change**	**Force File number**
06/07/15	Use of personal drives/location of saving official information clarified; updated references to IMSSD factsheets.	FF-087743
25/03/19	Administrative amendments to reflect name change from IMSSD to Protective Security.	FF-139207