Information security

Context

This policy uplifts information security maturity by applying consistent security practices to police information and supporting employees to uphold data security standards.

This policy includes:

- the security measures that authorised users need to consider when collecting, storing, recording and sharing information
- guidelines on unacceptable use of Victoria Police information and reporting responsibilities of authorised users
- information on adding a protective marking used to indicate the appropriate level of security measures to be applied
- information on the impact levels of the Business Impact Level table, designed to assess the value of Victoria Police information
- responsibilities of authorised users of Victoria Police information regarding clear desk principles
- instructions on the use and processing of Victoria Police information
- authorised user responsibilities for reporting security risks, events or incidents that breach or may breach the security controls.

This policy should be read in conjunction with **VPM Information and records management**, **VPM Personnel security**, **VPMP Physical security** and **VPMP Protective security incidents**, which provide more detail for specific components of information management and information security.

Contents

Definitions

Authorised user - a person who is authorised by Victoria Police to access:

- a corporate application and its information by the relevant System Owner (or their delegate) and/or
- information/records not stored in a corporate application, such as hardcopy documents or images, digital documents or audio/visual material whether stored on removable devices/media, personal drives or network drives by the relevant Information Owner (or their delegate).

Data - information that can be understood, analysed and reused to its full potential. Data can be incorporated into unique datasets saved in information and communications technology (ICT) applications, databases or spreadsheets.

Operational mobile technology device (e.g. IRIS device) – a Victoria Police digital asset that facilitates access to core policing platforms and applications (i.e., Computer-Aided Dispatch (CAD), LEAP) enabling members to securely access timely, accurate and relevant operational information in the field.

Health information - defined in s.3 of the *Health Records Act 2001* (HRA), as information or opinion about an individual's physical health, mental health, psychological health, disability or personal information collected to provide a health service.

Information asset - defined by the Office of the Victorian Information Commissioner (OVIC) as -

- a body of information, defined and practically managed so it can be understood, shared, protected and used to its full potential. Information assets support business processes and are stored across a variety of media and formats (i.e., both paper-based as well as electronic material)
- having a recognisable and manageable value, risk, content and lifecycle
- being a specific report, a collection of reports, a database, information contained in a database, information about a specific function, subject or process.

Information collection - creating, receiving or capturing information from internal or external sources becoming part of Victoria Police's records and managed in accordance with the *Public Records Act 1973* and PROV Standards.

Information lifecycle - the period covering creation or receipt of information through to lawful destruction at the end of the cycle unless the records are deemed permanent by the Public Record Office Victoria (PROV).

Information privacy - the protection of personal information handled by Victoria Police.

Information protection – measures and practices required to maintain the confidentiality, integrity and availability of official information throughout its lifecycle.

Information use – the way Victoria Police information is accessed, handled and applied by authorised personnel or systems during its lifecycle.

Information sharing – the authorised exchange of information with a third party on a systematic or ad hoc basis.

Original records - true and authentic information from a trusted primary source. Originals are paper or digital but not both.

Originator - anyone who creates or collects information for official purposes.

Personal information - information or opinion (including that forming part of a database) that is recorded in any form whether true or not, about an individual whose identity is apparent, or can be reasonably ascertained from the information or opinion but does not include health information. Personal information is only applicable to a natural person. It does not relate to a deceased person.

Portable computing device (PCD) - small, portable computing devices (such as laptops, tablets), mobile devices (e.g., phones, smartphones, etc) and portable storage devices (e.g., SD cards, USB sticks, etc.).

Product Manager - manages all resources required to maintain an application and to perform other duties tasked by the System Owner.

Sensitive information - defined in schedule 1 of the *Privacy and Data Protection Act 2014* (PDPA) as information or opinion about an individual's racial or ethnic origin, political opinions/membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record.

Security classification - A Security classification (OFFICIAL: Sensitive, PROTECTED, SECRET and TOP SECRET) is applied to information (or assets that hold information, such as laptops, approved portable storage devices) if it requires protection because of potential damage that would arise if the information's confidentiality were compromised.

Scope and application

This policy applies to all Victoria Police employees, Victoria Police approved third parties and Victoria Police contracted third parties.

Responsibilities and procedures

1. Information collection

Victoria Police information collection includes any information created, received or obtained from any source because of, or during the course of, a person's employment or engagement by Victoria Police.

1.1 *Overview*

Information collection should occur in line with the following:

- Victoria Police information must be managed lawfully and treated as an organisational resource
- Victoria Police information must be appropriately secured, fully auditable and transparent
- information must be collected, assessed and verified as close to the source as possible
- existing information sources must be used and updated wherever possible and

- Victoria Police information must not be falsified or fictitious; records created in accordance with the *Crimes (Assumed Identities) Act 2004* are exempt.

1.2 *Information ownership*

- Any information that is acquired, created, stored or used by a person in the course of their duties at Victoria Police is owned by the organisation, regardless of whether it is on personally owned equipment or Victoria Police owned equipment.
- Information owners, System Owners or Product Managers, work unit managers and originators have ongoing information ownership responsibilities.

1.3 *Tools*

- Information must be collected using Victoria Police equipment wherever possible.
- Any information collected on non-Victoria Police issued equipment during the course of work duties remains subject to the information handling, storage and disposal controls of this policy, **VPM Information and records management** and in accordance with the classification requirements of the information.
- If a portable recording device or a PCD, either owned by Victoria Police or personally owned, is used for Victoria Police information, then the requirements of **VPM Recording devices, CCTV and digital asset management** and **VPMG Portable computing devices** must be followed.

1.4 *Access to security classified information*

- In accordance with the handling requirements, recipients of security classified information must ensure that they:
  - need to know the information
  - hold the appropriate security clearance for the material and understand their responsibilities and obligations (see VPMG Security clearances)
  - will comply with any security controls, requirements or caveats for safeguarding the material
  - record receipt and dissemination of any security classified material.
- Refer to **Protective Security guide – G200 – Assessment and Secure Handling of Victoria Police Information** for further information on receiving security classified material.

2. Types of information

- All information developed, received or collected by or on behalf of Victoria Police must be assessed for confidentiality and security controls. Victoria Police information is designated as either:
  - Unofficial information or
  - Official information.

2.1 *Unofficial information*

- Unofficial information is information for personal use only and not related to Victoria Police activities (e.g. personal email).
- Use of Victoria Police resources for unofficial information is only permitted in accordance with **VPM Professional and ethical standards, VPMP Appropriate use of information** and **VPMP Information use, handling and storage.**

- If authorised users are unsure which category applies to their information, seek advice from Security, Information and Privacy Division (SIPD), Digital Services and Security Department (DSSD) or **Protective Security guide – G200 – Assessment and handling of Victoria Police Information.**

2.2 *Official information*

- Official information is all information created, sent and received as part of Victoria Police's work. It is an official record and it provides evidence of what the organisation has done and why.
- Official information also includes:
  - public domain information - police information that has been authorised for unlimited public release
  - personal and/or health related information managed or disclosed in accordance with relevant legislation, including the PDPA and the HRA. See **VPM Information privacy** and the Information Sharing Guide for more information
  - sensitive information (e.g., information on a person's racial or ethnic origin, religious beliefs or affiliations or criminal record)
  - security classified information.
- There are four security classifications:
  - OFFICIAL: Sensitive
  - PROTECTED
  - SECRET
  - TOP SECRET.
- All other information is not security classified, and is either:
  - OFFICIAL – all other Victoria Police information
  - UNOFFICIAL - information that does not form part of Victoria Police activities; see section 5 of this policy for more information.
- The Australian Government may share security classified information with Victoria Police regarding national security or the national interest. When sharing security classified information under the associated Memorandum of Understanding (MOU) between the Commonwealth, States and Territories and Victoria Police, Victoria Police is required to apply the relevant Commonwealth Protective Security Policy Framework protective security measures to that information. Refer to section 5 of this policy for security classified information.

2.3 *Security requirements for information and information systems*

- Victoria Police information and information systems must facilitate confidentiality, integrity and availability.
- All employees and Victoria Police contracted third parties must assess, protect and manage information in line with this policy, **VPM Information and records management** and the **Protective Security Guide - 200- Assessment and secure handling of Victoria Police information**, at all stages of the information lifecycle.

2.4 *Information security risk management*

- To protect Victoria Police information, authorised users must follow the Information System Security Risk Management process using the following steps:
  - identify the Victoria Police information assets

  - assess the value or sensitivity of information assets using BILs to complete an Information Value Assessment
  - conduct a security risk assessment (SRA) and implement operational controls for information assets proportional to their value, importance and sensitivity.

- To determine the security classification, the originator must:
  - assess the value, importance or sensitivity of official information by considering the potential consequences of unacceptable use of information, using the Victoria Police Business Impact Level (BIL) table; see section 4 of this policy for information
  - set the security classification at the appropriate level
  - mark the information with the appropriate protective marking (PM); see section 5 of this policy for further guidance
  - protect the information when used, stored, carried and travelled with, as per the handling instructions relevant to the PM.
  - protect the information during transfer and transmission by means that deter and detect compromise and that meet the minimum protection requirements as per the handling instructions relevant to the PM.

3. Information assets

- Employees must identify and monitor all significant information assets within their control or management. Significant information assets are determined by their value and risk assessment.
- Examples of significant information assets are enterprise ICT systems such as LEAP, Interpose, Neo, Station Books, HR Assist, Oracle and RecFind/RMS. Other significant information assets are databases and spreadsheets.
- Victoria Police must maintain an Information Asset Register (IAR) that aligns with PROV requirements, OVIC and is underpinned by the Victorian Protective Data Security Standards (VPDSS) to protect public sector information.
- The IAR includes descriptions, purpose, owners, value, risks and how the assets are used until they are no longer fit for purpose or are decommissioned.
- Information collected through the DSSD End to End Delivery Framework feeds into the IAR and product owners are responsible for updating the data. Refer to the Information Asset register on the DSSD intranet page to view current information assets. Refer to the End to End Delivery Framework on the DSSD intranet page.
- Information, Communication and Digital Technology, DSSD also maintains a system diagram for all systems with an Approval to Operate certificate that shows what and how data is shared.

4. Business Impact Level

4.1 *Overview*

- The BIL table has been designed to assess the value of Victoria Police information based on the impacts and consequences of unauthorised disclosure or unacceptable use of official information. The five levels are as follows:

Business Impact Levels					
0	1	2	3	4	5
NONE	**MINOR**	**LIMITED**	**MAJOR**	**SERIOUS**	**EXCEPTIONAL**
No business impact	Minor harm / damage to operations, the organisation or individuals	Limited harm / damage to operations, the organisation or individuals	Major harm / damage to operations, the organisation or individuals	Serious harm / damage to operations, the organisation or individuals	Exceptionally grave damage to the national interest

- As part of the information recording process, all information must be assessed according to the impacts and consequence of compromise using the BIL table to determine the PM.
- For more information see **Protective Security guide – G200 – Assessment and handling of Victoria Police Information**.

5. Protective markings

5.1 *Application of protective markings*

- All official information created must be individually valued and where possible to do so, must be labelled with a visible PM to indicate the appropriate level of security measures to be applied.

Protective Markings relative to Business Impact Levels						
Business Impact Level						
0	**1**	**2**	As applicable to the information product	**3**	**4**	**5**
NONE	MINOR	LIMITED		MAJOR	SERIOUS	EXCEPTIONAL
Protective markings, their Categories & Application						
Unofficial	OFFICIAL	OFFICIAL: Sensitive	Cabinet-in-Confidence	PROTECTED	SECRET	TOP SECRET
Non-Sensitive	**Non-Sensitive**	**Security Classified**	**Cabinet**	**Security Classified**	**Security Classified**	**Security Classified**

Non-work related material	Routine business information that, when appropriately authorised, may be released to the public	Bulk of Victoria Police's official information including personal information	Documents prepared for and responding to Cabinet	Most of Victoria Police's higher risk information	Majority of national security information received or created	The most sensitive national security information

- The PM chosen must reflect the highest value of information contained within the document, file or asset.
- When assessing which PM to apply to a document or asset, employees should refer to **Protective Security Guide - G231 – Selecting an Appropriate Protective Marking**, which provides a flowchart.
- A work area or employee who creates and protectively marks Victoria Police information is considered the originator of the material; that is, creates or collects information for official purposes.
- Where a PM is applied, the originator must:
  - obtain relevant authorisation for applying a PM, if required (see section 9.7 of this policy)
  - establish timelines for the review of the security classification (if applicable) and
  - ensure appropriate storage, distribution and any other special handling requirements are available.
- PMs must be visible, communicated or otherwise made available.
- Where technology or services are unable to provide PM selection, the value of the asset is to be clearly communicated to the user and ongoing endeavours made to ensure the information is handled appropriately.
- When completing forms owned by an external organisation or prescribed by legislation such as court forms, Victoria Police PMs may be removed if required.
- Information must be managed in line with the applicable information handling requirements for the PM.
- Refer to the **Protective Security Guide – G231 – Selecting an appropriate Protective Marking** for information on how to select an appropriate PM.

5.2 *Unmarked information*

- Unmarked information is deemed to have the PM of OFFICIAL information until assessment is made and a suitable PM is applied or, if for public release, labelled as 'Released into the public domain by [authoriser] for [purpose] on [date]'.

5.3 *Optional marking and caveats*

- Add-on markings (e.g. information management markers) and caveats may be used alongside PMs to provide context and/or specify limitations regarding information sharing.
- The different optional markers, roles and applications are detailed in the **Protective Security guide – G200 – Assessment and Secure Handling of Victoria Police Information**.

5.4 *Legacy marked information*

- Victoria Police information that has been protectively marked under the former scheme is now referred to as legacy marked information.
- If legacy marked information is actively used, an SRA must be conducted against the Victoria Police BIL table to determine the current PM for the information.
- The relationship between the current markings and previous PMs are detailed within the **Protective Security guide – G200 – Assessment and Secure Handling of Victoria Police Information.**
- Inactive legacy marked information does not require reassessment.

5.5 *Review of protective markings*

- PMs (especially security classifications) should be reviewed regularly by the relevant work area if the sensitivity of information changes during its lifecycle.
- Any adjustments to the PM must be made by the originator or in consultation with the originator or originating work area. Adjustments to the PM must be recorded.
- If the originator cannot be located or is no longer the information owner, the department head who is currently responsible for the function or activity related to the information, is responsible for approval of the revised PM.

5.6 *Security classification authorisation*

- Work areas may stipulate that security classified information created within the area is approved by managers at specified levels. It is recommended that approval levels align with section 9.7 of this policy.

5.7 *Inappropriate protective markings*

- Inappropriate allocation of PMs, such as incorrect security classifications, can impact information sharing and unnecessarily increase or reduce the necessary protections; this may result in integrity concerns and additional expenses. Refer to **VPM Professional and ethical standards** to inform decision-making and for further guidance regarding Victoria Police values and obligations.

5.8 *Labelling and format of protectively marked information*

- Protectively marked information must be clearly labelled. Refer to **Protective Security guide – G200 – Assessment and Secure Handling of Victoria Police Information** for guidance when required.
- Information requiring a PM, held on information and communications technology (ICT) systems or portable storage devices, is to be identified in the same way as information held on other mediums and given an appropriate level of protection.
- Digital files containing protectively marked information are to include the PM in the file name. This allows users to identify handling requirements without opening the file. Refer to **Protective Security Factsheet – 245 – Secure information handling: OFFICIAL to PROTECTED**.

6. Information handling

- Authorised users must comply with any PMs (including security classifications, caveats and dissemination limiting markers (DLMs)) to ensure material is handled in accordance with minimum security controls for the information.
- 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.
- Authorised users receiving information from other agencies that is marked as 'Accountable Material' must contact SIPD, DSSD for advice on specific handling instructions.

6.1 *Information handling control variations*

- **Protective security guide – G200 – Assessment and Secure Handling of Victoria Police Information** sets out standard information handling controls. Variations to the controls may be required if:
  - risks **are identified** – in this instance, refer to **Protective Security Factsheet – 245 – Secure Information Handling: OFFICIAL to PROTECTED** for stronger controls to mitigate risks associated with higher PM levels. Additional controls may derive from local circumstances, e.g. local business practices
  - **controls cannot be implemented** – in these circumstances, the risk of not adhering to the standard control is to be assessed and documented by SIPD and approved and recorded (including reasons) on the work area or systems risk register by the appropriate work area manager or regarding systems, the appropriate owner.
- Authorised users must contact SIPD for advice if either of the above scenarios apply.

6.2 *Classified Document Register*

- The purpose of a Classified Document Register (CDR) is to support the control, handling and auditing of hard copy security classified information with a protective marking of PROTECTED or above.
- A CDR must be used to record details associated with the creation, location, movement and disposal of security classified material produced or received by Victoria Police.
- CDRs are numbered registers that are tracked by SIPD, DSSD. To obtain a hardcopy CDR template contact SIPD or obtain an electronic CDR template via the Information Security intranet page.

6.3 *Movement of information*

- Information that is PROTECTED or above has requirements around its movement and 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) and
  - media type on which the information resides.
- All authorised users of Victoria Police information must ensure transfer methods (physical or digital) are appropriate for the information and any associated PMs. Refer to **Protective Security guide – G200 – Assessment and handling of Victoria Police Information, Protective Security Factsheet – F480 – Security Containers** and **Protective Security Guide – G350 – Physical Security Guide** for further details about transfer of Security Classified information.

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

6.4 *Accessing information while working from home*

- Authorised users should not remove police information from Victoria Police premises unless pre-approved by a manager (inspector or VPS-5 and above). This applies to information contained on Victoria Police issued electronic devices/laptops and hard copy information including Force Files.
- Removing physical police information from the workplace is a temporary arrangement and must be returned to the workplace at the first opportunity.
- Refer to **VPM Workplace flexibility**, **Protective Security Practice Guide – G810 – Working from home securely** and **Working remotely – G812 - Quick Reference Guide** on the approval process, safe handling and the returning of information to the office.

6.5 *Removing security classified information from Victoria Police premises*

- The removal of information classified as OFFICIAL: Sensitive or above from Victoria Police premises requires:
  - the authorised user complete a SRA (contact SIPD if assistance is required)
  - management authorises the removal and
  - the authorised user, who is to remove the information, is aware of the risks involved and accepts responsibility for the safe custody of the information.
- Access or use of Victoria Police information classified as OFFICIAL: Sensitive or above overseas requires:
  - the work unit manager, in conjunction with SIPD, conduct a SRA, to ensure there is a justifiable need to remove the material from the Victoria Police site
  - management subsequently authorise the removal
  - SIPD records the assessment and authority for accountability purposes and
  - the employee, who is to remove the information, is aware of the risks involved and accepts 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 Secure Handling of Victoria Police Information**.

6.6 *Receipts*

- A receipt provides a valuable means of tracing the movement of information classified as PROTECTED or above and provides a level of assurance that the recipient will be responsible for the protection of the material.
- Receipts must be used when transferring hardcopy security classified information externally. For further information on when receipts should be used and when recording in a Classified Document Register is required, contact SIPD, DSSD.

6.7 *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 ICT

system to which the device is connected to. The general Victoria Police ICT network is only able to process and store information up to and including OFFICIAL: Sensitive without additional security controls being applied.

- 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.

7. Information storage

7.1 *Storage of Victoria Police information*

- All Victoria Police information must be secured appropriately when unattended.
- All authorised users:
  - must secure protectively marked information in a container appropriate to the PM when not in use - refer to **Protective Security Factsheet – F480 – Security Containers** for details on appropriate physical storage containers
  - must ensure Victoria Police information is kept secure from theft, damage, loss and unauthorised access. Where loss or damage has occurred as a result of a breach of security, refer to **VPM Security incident management** for reporting obligations
  - must store digital based information/data (including all information relevant to work area such as briefs or correspondence):
    - in Victoria Police shared network folder or on a Victoria Police issued device or
    - on non-rewritable DVD/CDs and securely stored/filed on Victoria Police premises.
  - must identify risks in a risk register to be reviewed and inspected annually by the officer in charge or equivalent
  - must ensure, in accordance with **VPM Information and records management**, that all inactive information is identified through regular reviews and appropriately archived
  - must comply with storage caveats on information
  - use **Protective Security checklist - C090 - Local Documentation Information Security Checklist** to identify and address issues.
- Refer to Protective Security guide – G200 – Assessment and Secure Handling of Victoria Police Information for more information on specific requirements for different levels of protectively marked or security classified material.
- System Owners or Product Managers must:
  - contact the Security, Cyber and Risk Unit, SIPD, DSSD via the INFORMATION SECURITY-MGR PBEA to:
    - advise of any updates to existing information assets recorded on the information asset register (e.g., enhancements, decommissions and change of ownership) and
    - conduct an SRA for all new, and for changes to, information assets.

- Work unit managers:
  - must ensure that all active official information is stored in their workplaces in accordance with the following conditions:
    - in facilities that are commensurate with the level of security protection required
    - secure from public and unauthorised access
    - 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 ICT network and
    - security classified information must not be archived in personal drives, emails or in personal storage containers and
  - must consider information security related risks within workplace management risk registers, which are inspected annually.

7.2 *Clear desk principles*

- Victoria Police enforces a clear desk policy. This includes:
  - keyboard locking computers
  - closing files and turning documents face down during short absences and
  - logging off and locking security classified files/documents into suitable drawers/filing cabinets during longer absences.
- Lockable containers minimise risk and can provide evidence of tampering. An alternative to a lockable container is to lock the room or office.
- At the end of each day, authorised users must:
  - log off all systems and networks
  - lock away all sensitive information, particularly security classified information
  - ensure all security containers and safes are locked and
  - secure keys for security containers.
- To comply with a clear desk policy outside of the office, authorised users must:
  - package and carry the information appropriately
  - protect information from unauthorised viewing in public places, including on devices being used in public places
  - ensure the security of hardcopy information and laptop computers and
  - control access to information in the home or external environments.

8. Acceptable use of information

- All Victoria Police information (including information received from external sources) in any format must be secured, including during storage and transfer, as indicated by the PM. Only authorised users should access and use information in accordance with the business need.
- Victoria Police employees and former employees have a duty to only access, use or disclose police information for which they have a demonstrable and legitimate need, and which arises from and is directly related to the performance of their duties or functions. Service providers are also subject to compliance obligations. The **Protective Security guide – G200 – Assessment and Secure Handling of Victoria Police Information** and its accompanying guides and factsheets must be referred to for details regarding the controls on how to use, transfer, store and destroy Victoria Police information according to its PM.

- 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, PMs, and any other specific requirements.
- 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 should critically assess their work area. This assessment must be based on the minimum security controls for the classification level of the information.
- As far as practicable within a facility or work location, work unit managers must ensure that photocopiers, fax machines, shredders, and printers are located in areas where the use of the equipment can be observed.

8.1 *Personal use*

- Authorised users must not let private interests interfere with their responsibilities as authorised users of Victoria Police information and information systems.
- Authorised users must not use Victoria Police information systems to access or use law enforcement data or other official information, directly or indirectly, for unofficial reasons or personal interest.
- Any personal information created, stored and/or transmitted on Victoria Police information systems is treated as Victoria Police information, and as such Victoria Police reserves the right to:
  - access, copy, and/or delete all such information for any purpose and
  - disclose that information to any party deemed appropriate by the system or information owner.

8.2 *Unacceptable use*

- Unacceptable use of official information, technology or services is regarded as serious and may lead to disciplinary consequences, including termination of appointment or charges under sections 227, 228 and 229 of the *Victoria Police Act*. Refer to **VPM Professional and ethical standards** to inform decision-making and guidance on Victoria Police values and obligations.
- All authorised users must report unacceptable use of Victoria Police information or information systems to the appropriate work unit manager and/or as a security incident.

9. Information sharing

9.1 *General requirements*

- Effective policing relies on Victoria Police to communicate and share information internally and with a wide range of external partners.
- Information sharing, within and outside the organisation, should occur in line with the following:
  - policing requires information to be shared within Victoria Police, with partner agencies or organisations and with the public
  - establishing a policing purpose and a legal avenue as the basis for sharing police information

  - sharing of information must occur via official police systems (i.e., ICT applications and infrastructure and/or transfer processes) commensurate with the classification, sensitivity and risk profile of the information and
  - Victoria Police should actively seek to share unclassified non-personal information with the community.
- Authorised users are only given authority to share Victoria Police information by:
  - relevant legislation
  - policies and procedures.
- Authorised users must only share information under this authority if:
  - the information is within their area of responsibility and
  - the recipient has a legitimate official need for the information and
  - the recipient meets the protective security requirements for the information (if applicable).
- Where information sharing is also governed by a formal agreement, such as a MOU or Interagency Protocol, authorised users must follow its requirements, in addition to legislation and policy. Refer to **VPM Formal arrangements with external organisations** for further guidance on the creation and governance of MOUs.
- Written requests for Victoria Police information should provide justification that the information sought is reasonably necessary for a particular purpose and state what legislation or agreement facilitates the release.
- In all circumstances of release of information outside the organisation, the authorised user releasing the information is to advise the recipient that they:
  - are responsible for the security of the information
  - must provide the same level of security protection assigned by Victoria Police and
  - must manage the information securely and not release it to any other individual or organisation without prior approval from Victoria Police.
- Refer to **Protective Security Guide – G200 – Assessment and Secure Handling of Victoria Police Information** for instructions on approved methods of transfer for protectively marked or security classified information and use of DLMs and caveats.

9.2 *Personal information*

- Information relating to individuals (including Victoria Police employees) must only be accessed, used or disclosed in accordance with the PDPA and HRA. Refer to **VPM Information privacy** for further guidance.

9.3 *Sharing information from personnel records with third parties*

Information from personnel records (including employment history, statements of earnings and leave records) can only be granted to third parties in accordance with the PDPA and HRA in the following circumstances:

- with the written consent of the employee
- in accordance with disclosure obligations in criminal and civil proceedings - refer to **VPM Disclosure in criminal proceedings**
- where a subpoena is issued for the production of records; details are to be provided in accordance with the conditions prescribed within the subpoena and/or as prescribed by the court

- to solicitors, executors or estate administrators working on behalf of the estate of a deceased former employee
- to representatives of Police Veterans Victoria and Victoria Police Legacy as part of their support services for former employees and their families
- to representatives of external agencies where an employee or former employee has submitted a claim for benefits/compensation, such as the Transport Accident Commission, Victims of Crime Victoria and superannuation companies
- to the Ombudsman in accordance with s.18, *Ombudsman's Act 1973*
- to the Victorian Public Sector Commission in accordance with s.63(1), *Public Administration Act 2004*
- to the Independent Broad-based Anti-corruption Commission (IBAC) in accordance with s.15(7)(a), *Independent Broad-based Anti-corruption Commission Act 2011*
- to the Office of the Director of Public Prosecutions (DPP), normally with a DPP representative examining the appropriate records, accompanied by an authorised employee; any records identified as being relevant to the prosecution of the DPP case will only be released upon production of a subpoena or search warrant
- to defence counsel, under identical provisions applying to the DPP; the only exception to this is cases where employees may access and copy documents from their own personnel files to assist in their defence
- to the Chairperson of the Police Registration and Services Board Police Appeals Board in connection with appeals or reviews in accordance with Part 8 of the *Victoria Police Act*
- where legal representatives acting on behalf of the Chief Commissioner request access to personnel files in connection with formal legal proceedings. In these cases access will be on Victoria Police premises and supervised by a payroll practitioner.

Before sharing this information externally, employees must consider whether they hold relevant authority to release this information; refer to section 10 of this policy for further guidance.

Where personnel information is released to a third party, appropriate records are to be retained of:

- written consent from the employee or the reason consent was not required
- details of the information provided.

For further information about the management of personnel records, refer to **VPM Information and records management**.

9.4 *Artificial intelligence tools*

- The use of artificial intelligence (AI) and generative AI (GenAI) can create risk to Victoria Police through potential sensitive data loss, reliance on inaccurate information and the inability to confirm analysis or decision-making processes.
- Entering Victoria Police information into external AI tools uploads the information to the internet, which is an uncontrolled environment and potentially exposes that information to unauthorised access.
- Employees, Victoria Police approved third parties and Victoria Police contracted third parties must not install or develop AI tools on Victoria Police devices. They

must only enter Victoria Police information into, or access or use, publicly available or commercial AI tools for business purposes when approved via the following process:

- employees must complete and submit a Request to use Artificial Intelligence Products form via the DSSD intranet page for approval
- applications must include:
  - the legitimate business need to use AI and
  - completed information security, privacy and architecture assessments, as indicated by the form and in compliance with the DSSD End to End Delivery Framework
- depending on the type of AI tool and proposed use, applications may be:
  - approved by a superintendent/VPSG-6 or above via the employee's chain of command (as indicated via the form) or
  - subject to review and endorsement by the AI Ethics Committee (AIEC), which may also request further assessments such as human rights and legal advice
- approval must only be provided where:
  - a legitimate business need has been identified and
  - a Request for use of AI Products has been submitted and the use is endorsed by the AIEC
- employees should consider the need for any additional endorsement that may be required, for example where funding is required.

- Only public domain information may be entered into publicly available AI tools, including GenAI tools such as ChatGPT and AI-enhanced search tools (e.g. Microsoft Co-Pilot for web (Bing), Google AI Overview). The use of Victoria Police approved GenAI tools is preferred over publicly available GenAI tools.
- Application of the Victoria Police AI Ethics Framework, available on the intranet, ensures Victoria Police applies relevant legal and ethical frameworks to any use of AI.
- The information that can be used in a Victoria Police approved AI tool is established by the permitted information classification, which is documented in the use endorsed by the AIEC.
- Any police information entered into a Victoria Police approved AI tool must not exceed the protective security level applicable to the endorsed use for that tool.
- All AI usage is monitored and users who attempt to access external AI tools, including GenAI, will be presented with a warning banner. Refer to DSSD's intranet page for more information about the AIEC, the AI Register and general advice.

9.5 *Microsoft Teams*

- Microsoft Office 365 (Office 365) is the standard operating environment used at Victoria Police that supports SharePoint Online and Microsoft (MS) Teams. MS Teams is not a compliant records management system and is intended to be used as a chat-based collaboration platform, which also facilitates document sharing, file storage, online meetings/telephony, video calling, screen sharing, and dedicated channels for work teams.

- Only copies of information (not records or evidence) should be shared in MS Teams with a protective security marking up to and including OFFICIAL: Sensitive for MS Office file types, including the following:
  - Word documents
  - Excel
  - PowerPoint
  - Email
  - OneNote (digital diary)
  - images
  - video
  - PDF.
- Documents should be saved in SharePoint Online and MS Planner. Recordings should be saved in OneDrive/SharePoint Online.
- Prior to using the recording function in MS Teams, the facilitator must inform all participants that the conversation will be recorded and provide participants sufficient time to object to recording or leave the meeting if they do not consent.
- Data associated with MS Teams is retained and discoverable for compliance purposes, (e.g., Subpoenas, Freedom of Information (FOI) requests, Notice to Produce, Court, Royal Commissions).
- Any content classified as PROTECTED and above must not be stored in MS Teams.

9.6 *Use in Victoria Police training*

- Victoria Police information may be used to facilitate operational training, either in the workplace or through formal courses. The use of Victoria Police information for training purposes must comply with section 9 of this policy and where applicable, **VPM Recording devices, CCTV and digital asset management** and **VPM Body worn cameras**.
- Audio/visual recordings of interviews or events may be viewed by participants but should not be available for download. A record of audio-visual recordings shown to participants must be maintained.
- Consideration must be given to the privacy of any person depicted in audio/visual recordings used in training by, for example, obtaining consent for the use of the recordings or pixelating the person's image.
- Excluding workplace integrated learning programs managed by People Development Command, any event details or scenarios based on real incidents or investigations must be from finalised cases. Live data/systems, not including those specifically designed for training purposes, must not be used for systems training or demonstrations.

9.7 *Issues to be considered when authorising information release*

Victoria Police employees authorising the release of Victoria Police information should consider the following issues:

- **Compromise** – Authorised users must not share information if there is a possibility of compromising a current investigation or prosecution. Consideration is also to be given to Public Interest indemnity and immunity. Authorised users should consider whether the release will divulge police methodology, capability, future focus or identify the source of information. Legal advice should be obtained, as required.

- **Authority** – Whether the employee has the ability to authorise the release; refer to section 10 of this policy for guidance regarding relevant authority
- **Relevance** – The relevance of the information, the intent of the information sharing and the intended recipient
- **Ownership** – Information obtained from another organisation is not to be disclosed unless authorised by the originating organisation.

  For example, CAD data (Refer **VPMG Release of corporate statistics**).
- **Sensitivity** – It is paramount that authorised users always consider the sensitivity and any legislative requirements for the information.

  For example, information regarding victims of sexual assault or information regarding children, reporters or caregivers under the *Children, Youth and Families Act 2005*.
- **De-identify/check/redact** – Ensure any non-relevant information is removed from information that is to be released, e.g., victim, co-offender or witness names or other defined personal or health information related to another person that may appear in a summary or in audio. Refer to **VPM Information privacy**.
- **Notifications** - When releasing personal or health information to a statutory body (e.g. Australian Health Practitioner Regulation Agency) for the purposes of their specific law enforcement function, it is recommended that police inform the victim or witness of the intended disclosure, preferably prior to disclosure.

9.8 *Authorisation required to release information*

- Security classified information (i.e., information classified as OFFICIAL: Sensitive or above) must only be shared in accordance with all applicable handling restrictions or caveats, and with appropriate authorisation as detailed in the following table.

Marking	Authorisation for internal sharing	Authorisation for external sharing
Public Domain	Not security classified information No additional authorisation required	
UNOFFICIAL	Not security classified information No additional authorisation required	
OFFICIAL	The originating work area may authorise the release of material in accordance with this policy	
OFFICIAL: Sensitive The following Information Management Markers (IMMs) are recommended for use with information marked as OFFICIAL: Sensitive and above • Legal privilege	The originator work area may authorise the release of material marked at this level in accordance with this policy	

• Legislative secrecy • Personal privacy		
PROTECTED and/or Cabinet-in-Confidence	An inspector or VPSG-5 from the originating workplace Regarding information relevant to their work unit/line control, a sergeant or VPSG-4 and above from Counter Terrorism Command (CTC)	Regarding information relevant to their work unit/line control, a senior sergeant or VPSG-5 and above from CTC
SECRET and/or TOP SECRET	Where permitted by the originating organisation, a superintendent or VPSG-6 between those who hold the appropriate security clearance. Regarding information relevant to their work unit/line control, all CTC senior sergeants and VPSG-5 or above between those who hold the appropriate security clearance. If disseminating via electronic means, dissemination must occur via the Australian Secret Network for SECRET information	

- For classifications PROTECTED and above, an employee of a lower level may be authorised, by the positions listed in the table above, to release security classified information provided this authority is in writing and specifies the employee's work unit, the reason for the authority and the scope of the authority including the security classification levels for which the authorisation applies.

9.9 *Requests for information*

- Providing information to external parties increases the risk to Victoria Police.
- Guidance on providing specific types of information is contained in the below policies and guidelines:

Topic	Relevant guidance
Individuals or organisations regarding a reported traffic or industrial accident	**VPMG Release of accident and property records**
Media organisations	**VPMG Release of information to the media**
Individuals or organisations regarding a civil matter	**VPMG Civil proceedings**
Research requests	**VPMG Research**

Insurance agency interviews	**VPMG Release of accident and property records**
Employers or regulatory authorities	**VPM Notification of offences** **VPM Information privacy**
Release or comment on corporate statistics	**VPMG Release of corporate statistics**
Media	**VPMG Release of information to the media**
Disclosure in criminal proceedings	**VPM Disclosure in criminal proceedings**

9.10 *Sharing information with other emergency services*

- Where police and other emergency services are in attendance at operational incidents, information relating to that incident may be exchanged.
- Personal and health information gained from emergency services must not be passed onto third parties except where necessary for law enforcement or as specifically provided for in the HRA or other relevant legislation.
- In accordance with **VPM Operational duties and responsibilities**, incidents requiring information sharing with other emergency services are to be recorded.

9.11 *Sharing information with other government agencies or statutory authorities*

- Details of what information can be shared with other government agencies or statutory authorities and appropriate approval is included in relevant policies and guidelines:

Topic	Relevant guidance
Personal or health information	**VPM Information privacy** and the Information Sharing guides available on the DSSD intranet page
Traffic incident details	**VPMG Release of accident and property records**
Reporting to medical authorities	**VPM Notification of offences**
Release to RSPCA inspectors	**VPM Animals**
Release of sex offender information	**VPM Registered sex offender management**
Release of criminal histories	**VPMG Release of police records**
Reporting of child in need of protection	**VPM Family violence and child information sharing** and **VPM Protecting children**
Reporting personal details of nominees for bravery awards	**VPM Honours and awards**

9.12 *Information privacy*

- All personal information and health records held by Victoria Police, whether or not this information is also in the public domain, must be managed securely in accordance with the information privacy principles of the PDPA and health privacy principles of the HRA. Refer to **VPM Information privacy** for further details about compliance requirements and exemptions.

9.13 *Release of information into the public domain*

- Victoria Police may, and in some cases must, release information into the public domain as authorised by the Information Owner, Product Manager or OIC of their work unit for the purposes of:
  - public interest and/or
  - FOI.
- Such release must be documented.

9.14 *Public interest*

- Victoria Police may release information of public interest into the public domain to:
  - inform and reassure the public about the integrity and performance of Victoria Police's practices and systems and/or
  - comply with the Victorian Government's DataVic Access Policy (DVAP), which enables the use of Victorian Government data by the public.
- The DVAP supports open and accountable government by allowing the public access to Victorian Government information so that it can be used and reused by the community and businesses.
- While a significant amount of information held by Victoria Police is not suitable for public release, information owners should identify datasets or other information that may be suitable for public access.
- Victoria Police must release data suitable to be used and reused by the community and businesses in accordance with the DVAP guidelines as approved by the Assistant Treasurer of Victoria.
- The Director, Media, Communications and Engagement Department should be engaged prior to the unlimited public release of information.
- Unclassified and non-personal information should be considered for release unless access is restricted for reasons of privacy, public safety, security and law enforcement, public health, and compliance with the law.
- Data release in accordance with DVAP must be in line with DVAP guidelines.
- All datasets proposed for release under DVAP must be recorded on the IAR.

9.15 *Freedom of Information*

- The Victorian Government requires the release of some government data and information through the *Freedom of Information Act 1982* (FOI Act) and the DVAP.
- FOI provides the public with a right to access information held by Victoria Police and to request the correction or amendment of any personal information where it is inaccurate, incomplete, out of date, or where it would give a misleading impression.
- The presence or absence of protective markings (in the form of Disseminating Limiting Markers or security classifications) does not affect a document's status under the FOI Act.
- On receipt of a request from the FOI office, employees must make a diligent search and supply all documents or information requested within the required timeframe.
- Information must not be edited before being given to the FOI office. It is the responsibility of the FOI office to apply the various exemption provisions within the FOI Act.

- The legislated timeframe for processing standard FOI requests is 30 days. Requests for documents will be sent electronically to employees and their work unit manager for actioning. The responding employee must:
  - ensure a response is provided within four calendar days from the date the request was sent, or the work unit manager must advise where an employee is not available within this time frame and the expected return of the employee
  - send the response, including required documents and a completed copy of the provided FOI 47 checklist, electronically to PBEA: FOI-DOCUMENTS-MGR, or if the requested records cannot be located, a confirmation email must be sent to the FOI Unit detailing the searches undertaken and reasons why the document/s cannot be located and
  - contact the FOI Unit for advice where materials cannot be provided within the required timeframe (e.g., where the file cannot be sent electronically or due to rostering constraints or issues with retrieving the documents).
- If the requested information has been destroyed the employee is to provide a copy of the destruction authorisation in accordance with **VPM Information and records management**.
- If the requested information existed but is unable to be located, a security incident should be reported in accordance with **VPMP Protective security incident reporting and management**.
- Former employees may request access to police information e.g., diaries, daybooks, notebooks through the FOI process. All former employees must refer all such requests to FOI.
- Further guidance on the FOI process for Victoria Police is provided on the FOI intranet page.

9.16 *Documenting release*

- Work unit managers must ensure that the requests for, and external release of any Victoria Police information is formally documented.
- The documentation is to capture sufficient information that identifies the:
  - details, content and PM of the information to be authorised for release
  - details of the organisation to which the information was released
  - details of who authorised the release of the relevant data/information
  - time, date, format in which the release was made and the mechanism for release.
  - Any information relating to court processes that has been released without a written request must have a follow up record outlining the decision to release the material.

9.17 *Information not specifically covered by legislation or policy*

- Information sharing that is not specifically governed by relevant legislation, and/or Victoria Police policies and procedures may be considered for release if it is:
  - not personal or health information
  - not security classified or protectively marked and
  - for legitimate community safety reasons or law enforcement purposes.
- The release of the information must be recorded and authorised. The other party must be informed that the information is not in the public domain and the information must be secured against unauthorised access.

10. Security

- Appropriate and successful security of information relies on many factors including sound understanding and use of classification systems, information handling processes, physical security, personnel security as well as education and auditing/deterrence activities.
- Work unit managers are responsible for maintaining the security of employees, information, assets and resources under their control through appropriate security practices and procedures for their workplace, as determined by the nature of the workplace and the type of information or resources it holds. Clear desk and clear screen procedures must be followed.
- All department heads and work unit managers must ensure compliance with the appropriate controls to ensure security of police information. See **VPMP Physical security**, **VPMP Personnel security**, **VPM Protective security** and **VP Cyber Security Standards**.

10.1 *System audits*

- All Victoria Police information and information systems are subject to audit logging and monitoring. Refer to the **Cyber Standard – Logging and Monitoring** on the DSSD intranet page.
- Information system owners must develop a Site Security Plan. This plan must address the requirements of **Cyber Security Standard – Infrastructure, Cloud and Network Security** and **Cyber Security Standard – Logging and Monitoring**. The results of audits conducted must be recorded and reported in accordance with the approved plan.
- Personnel authorised by Victoria Police to audit system use are entitled to view any information that users store in, or transmit across, Victoria Police information systems. Authorised users undertaking these roles must have appropriate security clearances relative to the information subject to the audit. Refer to **VPMP Personnel Security**, **VPMG Security Clearances** and **VPM Service provider and external personnel security requirements**.
- All employees and any other individuals authorised to use Victoria Police information and information systems, must cooperate with requests for information about their use of information systems from Professional Standards personnel, Internal Audit, System Managers and protective security personnel. Should there be any doubt regarding a request for information, the Victoria Police Chief Information Security Officer should be consulted via the INFORMATION SECURITY-MGR PBEA.

10.2 *Reporting security risks, events or incidents*

- All incidents that breach or may breach the security controls (personnel, physical, system or information management) must be reported to the Security Incident Registrar (SECURITY-INCIDENTS-MGR PBEA). Incidents that must be reported are reflected in **VPMP Physical security** and **VPMP Protective security incidents**.
- Any Victoria Police personnel and/or contracted third parties who become aware of known or suspected unacceptable use of security classified information must report the details, either directly or through a work unit manager.
- Victoria Police uses security incident reporting and investigation to record and evaluate the type, volume and costs of security incidents to inform Victoria Police risk management.

11. Information security governance

- Victoria Police's information security obligations are primarily from the Office of the Victorian Information Commissioner's (OVIC's) Victorian Protective Data Security Standards (VPDSS). The VPDSS developed by OVIC 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 is not limited to computer systems.
- All Victoria Police employees and contracted third parties are responsible for managing and protecting Victoria Police information in accordance with Victoria Police policies. The following positions and groups have specific responsibilities for information management and security.

Role	Responsibilities
Chief Commissioner of Police (CCP)	– Strategic leadership of Victoria Police – Overall accountable officer for information management and security – CCP or their delegate represents Victoria Police on all relevant State and National governing bodies providing oversight and direction for the development and enhancement of national and state law enforcement systems and information sharing initiatives
Security Executive	– Ensures development and oversight of Victoria Police information management and security policy, compliance, strategy and work programs as well as the ongoing development of Victoria Police protective security policy and the oversight of protective security matters
Digital Transformation Committee	– Approves digital innovation, technology project delivery and operations, information management and cyber security strategies – Monitors and supports the implementation of the Strategy to Digitally Transform Victoria Police by leading cultural change and providing advice to Executive Command regarding strategic directions and digital investment priorities
Chief Information Security Officer	– Provides cyber security leadership and guidance on all information security matters, including and advice on personnel, physical and information and operational technology security measures which need to be implemented across Victoria Police

11.1 *Work area information security review*

- All work unit managers can assess their work unit's information management and information security (IM&IS) compliance using the Protective Security Template C090 Work Area Information Security Review (WAISR) Template available on the Protective Security intranet site.
- The WAISR provides a valuable tool to help work unit managers to identify and mitigate gaps in the work unit's IM&IS processes and procedures.

11.2 *Business continuity planning*

- In accordance with **VPM Business Continuity Management** department heads are responsible for ensuring appropriate business continuity strategies and plans are in place.
- All business continuity strategies and plans must specifically address the information management (including records management) and information security considerations for all information and information systems managed by the department.
- The business continuity strategies and plans must consider and address the information assets under their control based on their risk profile (including natural disasters, accidents, equipment failures or deliberate actions) and the importance of the information to the organisation.

11.3 *Compliance, monitoring and reporting*

- Where appropriate, audits and reviews of Victoria Police functions and activities should include an assessment of compliance with the information management and information security policies and guidelines.
- Information management and information security risk areas are included as part of the Victoria Police Strategic Internal Audit plan, as approved by the Victoria Police Audit & Risk Committee (VPARC). The areas or topics to be audited will be identified through the Victoria Police risk profile or to address emerging issues as requested by Victoria Police management. All audit results will be reported to VPARC, Executive Command and other senior management as relevant and Victoria Police management.
- SIPD, DSSD must provide adequate training and education of individuals to ensure proficiency in information security.
- Department heads must:
  - ensure departmental procedures and processes comply with information management and information security policy and guidelines and
  - include information management and information security compliance auditing as part of internal auditing processes.
- Work unit managers must:
  - include compliance with information management and information security policies as part of their workplace inspections. The minimum issues to be inspected are in the WAISR - C090 checklist. Each work unit manager must assess what other compliance inspections should be undertaken, based on the information holdings and activities of the area
  - ensure new personnel under their management are given adequate training in information security and their responsibilities under this policy
  - ensure that workplace inspections include adequate monitoring to identify potential instances where policy rules are not being followed
  - ensure they (or their nominated delegate) only authorise access or variations to access, to the information created, used and stored in the work unit or in the network folders/directories under their responsibility
  - conduct audits of access to their physical location and network folders/directories they are responsible for, to ensure only authorised users with a current business need have access to information stored there

- ensure that the controls used to maintain the security of information are commensurate with the sensitivity and any official information that requires a higher degree of security and an increased level of protection is security classified.
- System Owners and Product Managers must:
  ensure compliance, monitoring and reporting requirements of their SRAs are conducted and official records of these activities are maintained.

- Authorised users must:
  - through education and training, be competent in all aspects of information security, including protection against unauthorised access, use and disclosure and
  - complete any mandatory information security training and refresher training in accordance with mandatory training obligations.

12. Solution development and acquisition governance requirements

- The development or acquisition of a solution that will support any part of the information management lifecycle must comply with security policies, standards, architecture and the DSSD End to End Framework This is regardless of whether the solution is a process, procedure, ICT system, application or hardware.
- Where the solution does not comply with the above, this must be documented. Notice of solutions to be developed that will not comply must be forwarded to the Chief Information Security Officer, SIPD, DSSD via the INFORMATION SECURITY-MGR PBEA.
- Solutions that involve ICT systems, applications or hardware must also comply with the **Cyber Standard – Secure System Development** available on the DSSD Cyber Standards intranet page.
- Solutions must be supported by:
  - documented business cases (appropriate to the level of the proposed development) for all proposed solution developments
  - documented and comprehensive business requirements that address:
    - business activity processes
    - information management and information security requirements
    - audit requirements and
    - technology and infrastructure requirements
  - approval of the solution development from the system owner for minor developments or DTC for major developments and
  - appropriate application of Victoria Police project management processes including status reporting of the project to the project sponsor.
- ICT solutions are subject to organisational governance processes such as the DSSD End to End Framework and supporting standards. Refer to the DSSD End to End Framework on the DSSD intranet and to Cyber Standards Secure System Development and System Security.

12.1 *Information and communications technology change management*

- All ICT changes must be properly planned, managed, reviewed, authorised and implemented to minimise the security risks associated with changes to systems and the information that they process, store and communicate. For more information and appropriate contacts, refer to the Service Integration and Management (SIAM), DSSD intranet page.

- All proposed ICT changes with potential security risks and impacts must be security assessed prior to implementation. This security assessment includes consideration of existing controls which may mitigate the risk of the change or appropriate treatment if risk exceeds an acceptable level. Contact SIPD for assistance.
- Relevant Victoria Police Business Owners and/or Product Managers approve ICT changes and the Change Advisory Board reviews and authorises ICT changes for implementation. For further information refer to the SIAM, DSSD intranet page.
- For minor ICT changes, Product Managers and the Change Advisory Board (CAB) may engage SIPD to determine if a security assessment is required.
- Change notifications received from or potentially impacting third-party agencies which interface with Victoria Police systems and network may be included in an ICT impact assessment, where appropriate.

12.2 *Procurement*

- Victoria Police investment management and procurement must have formal processes that integrate compliance with the Victoria Police information records management principles, DSSD's End-to-End Delivery Framework and Cyber Standard – Secure System Development and Cyber Standard – System Security.
- Victoria Police Procurement and Legal Services Departments must ensure that all new or extended contracts involving management or use of Victoria Police information by non-employees:
  - require compliance by all individuals to Victoria Police information management and information security policies for all Victoria Police information created, collected, managed or used under the contract and
  - allow Victoria Police to direct the removal of individuals deemed by the Contract Principal to be unsuitable for access to Victoria Police information.

Related documents

- VPM Information and records management
- VPM Information privacy
- VPMG Mobile / smart phones
- VPMG IM and IS responsibilities
- CCI 10/17 Mobile device deployment
- VPMG Information and information equipment disposal
- Protective Security guide – G200 – Assessment and handling of Victoria Police Information
- Protective Security Guide - G231 – Selecting an Appropriate Protective Marking
- C090 Work area information security review

Further advice and information

For further advice and assistance regarding this policy, contact SIPD, DSSD via the INFORMATION SECURITY-MGR PBEA.

Update history

DATE UPDATED	SUMMARY OF CHANGE	FORCE FILE NUMBER
28/01/2026	This policy consolidates and replaces VPM Information categorisation, collection and recording, VPMP Information use, handling and storage, VPMP Information sharing, VPMP Information management and information security framework, VPMP Appropriate use of information, Information management and information security organisational policy statement, VPMG Information management and information security roles and responsibilities, VPMG Clear desk principles.	FF-215906