

Information Management and Information Security

Context

Information¹ is a fundamental and critical component for the provision of law enforcement and emergency response services. In order to effectively and efficiently deliver these services, information must be handled consistently and securely as a priority throughout its lifecycle. Public confidence in the ability of the Victoria Police to collect and manage all information, (including personal, sensitive and classified material) effectively and in line with our legal obligations, requires the application of the highest standards in information management practices. These standards govern information confidentiality, integrity and availability.

This Information Management and Information Security Organisational Policy Statement provides a clear mandate for Victoria Police to work towards achieving effective, accurate and secure systems and processes (human and technical) for the benefit of the State. It sets a clear expectation for Victoria Police to work towards achieving best practices, productivity gains and improved business outcomes through improved information management.

Policy

1. Organisational Commitment

Victoria Police will continuously improve the way we manage information. To achieve this we aspire to:

- establish and maintain effective governance of our information assets;
- consider and embed information management principles into all aspects of our business activities;
- manage all information, regardless of format and media, securely and appropriately throughout the entire information management lifecycle; and,
- fully comply with Standard for Law Enforcement Data Security (SLEDs), Public Records of Victoria (PROV) standards, privacy principles and other legislative requirements.

¹ "Information" includes, but is not limited to, data, documents, email, images, video & audio - before and after they have been deemed public records or law enforcement data – regardless of media or format.

2. Organisational Outcomes

Victoria Police information and information systems must facilitate:

- **confidentiality** – to ensure privacy of the information and that it is only used by, and disclosed to, those authorised to do so for legitimate business purposes;
- **integrity** – to ensure that changes to information and information systems are authorised and auditable;
- **availability** – to ensure that information and information systems are accessible and useable when required.

The confidentiality, integrity and availability of our information and information systems is integral to the secure delivery of the right information to the right people at the right time in the right format.

Victoria Police is committed to continuously improve our information management and information security practices. This will ensure that Victoria Police:

- establishes and maintains an information management strategy and implementation plan;
- undertakes regular information management planning;
- creates, collects, and maintains information that is relevant, accurate, and complete to meet organisational, policy, and accountability requirements;
- manages all information as an organisation-wide resource. We will:
 - handle, store and transmit information in accordance with security classification controls and privacy considerations;
 - share information without the restriction of unwarranted personal ownership;
 - continually review and correct to maximise the quality of existing information; and,
 - comply with relevant legislation, requirements and appropriate standards, including recordkeeping, privacy, security, accessibility and freedom of information;
- protects information from unauthorised access, disclosure, destruction and from interruptions to availability. This will ensure the continuity of key law enforcement services and business processes;
- optimises the value of information by enabling business processes and systems to securely share, re-use and reduce duplicate information;
- leverages the knowledge of our police members and employees; connecting people with people and people with information;
- undertakes focused ongoing activities to establish and build information management and information security as an important part of the organisational culture;
- provides relevant training and education to all police members and employees.
- understands the value of, and enables effective information exchange with, community members;
- holds information in an accessible format so that it can be shared and made available, where appropriate, on a state/national basis and to meet obligations to other criminal justice agencies, emergency service organisations and partner agencies;

- implements governance and accountability structures for investment in, and the management of, information solutions to support optimal business outcomes;
- considers information management, recordkeeping and security requirements and best practice when designing and acquiring new information services and systems; and,
- has appropriate risk management plans in place for all significant information assets.

Responsibility

All Victoria Police Employees, Members and Contractors are responsible for managing and protecting Victoria Police information in accordance with Victoria Police policies. This includes only accessing information specific to their duties, in a secure way. The following positions and groups have specific responsibilities for Information Management and/or Information Security.

Chief Commissioner of Police

The Chief Commissioner of Police (CCP) is responsible for the strategic leadership of Victoria Police. The CCP is the overall accountable officer for the activities and performance of the organisation, including information management and information security. The CCP 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

The Victoria Police Security Executive is responsible for ensuring development and oversight of Victoria Police information management and security policy, compliance, strategy and work programs.

Information Management and Information Security Committee (IMISC)

The IMISC (chaired by the Security Executive) is responsible for:

- setting the strategic direction for Victoria Police Information Management and Information Security;
- driving cultural change for information management and information security;
- leading the delivery of policies, procedures and improvement initiatives;
- overseeing responses to recommendations from relevant regulatory bodies and monitors overall compliance; and,
- ensuring that the requirements of this policy are integrated into, and implemented through, organisational governance processes, policies and procedures, business processes, systems and training.

Director, Protective Security

Director Protective Security is responsible for the development and implementation of the Information Management and Information Security Strategic Plans, including shaping key policies and procedures, driving compliance, leading information improvement initiatives and mitigation of risks. The Director Protective Security is the primary contact for external agencies for Information Management and Information Security.

Operational policy references

The Organisational Policy Statement is implemented through the following Policy Rules and Procedure and Guidelines:

- VPMP Information Management & Information Security; and,
- All subordinate policy rules & guidelines.

Further advice and information

For further advice and assistance regarding this Organisational Policy Statement, contact Protective Security.

Update history

Date of first issue	24/02/2012	
Date updated	Summary of change	Force File number
07/12/15	Legislative reference update to <i>Privacy and Data Protection Act 2014</i> .	FF-096355
25/03/19	Administrative amendments to reflect name change from IMSSD to Protective Security.	FF-139207