

Victoria Police Manual – Procedures and Guidelines

Information system access

Source Policy

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

- Organisational Policy Statement - Information Management and Information Security
- VPMP Information access
- VPMP Appropriate use of information

Application

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

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

Procedures and Guidelines

1. Applying for access

- As stated in section 1.3 and 1.4 of **VPMP Information access**, employees and other individuals are required to meet certain criteria before they can access to information systems.
- If they are satisfied that this criteria has been met, Work Unit Managers may apply for the initial access to information systems for employees and other individuals under their management. They are to apply for access through the following methods:
 - for network and mainframe access, change of access, additional access or revocation of access (excluding administrative accounts), complete a Request for Computer Access [Form 1250]

- for remote access to the Victoria Police network via a Victoria Police laptop computer or creation of service or administrative accounts, complete an IT Service Request [Form 1234]
- for access, change of access, additional access or revocation of access to a non-corporate application system, contact the relevant System Owner directly.
- The request is sent to the System or Information Owner for authorisation. They are to ensure that the criteria for access, as detailed in sections 1.3 and 1.4 of **VPMP Information Access** are met before authorising access.
- Following approval and authorisation, the Helpdesk or System Owner is responsible for implementing the request. The applicant is then considered an 'Authorised User' of the information system.
- If a System or Information owner (or delegate) is not recorded or cannot be identified for a given resource – then the request should be postponed until formal ownership of the resource is confirmed and recorded.

2. Variation to access

- As stated in **VPMP Information access**, Authorised Users and Work Unit Managers are required to amend or revoke access to information systems when the Authorised User:
 - no longer meets the criteria for access, or
 - transfers to another work unit, dies, completes contract, ceases employment, takes extended leave (more than 3 months), is suspended or required to take leave pending a Professional Standards Command investigation or when they no longer require their allocated access.
- Variations to access are processed through the same methods as section 1.
- Authorised Users are required to apply for access variation and submit this to the Work Unit Manager for approval who will submit it to the appropriate System or Information Owner, as appropriate.
- If the Authorised User is not able to submit an access variation request, the Work Unit Manager is to submit the request.

3. Password resets

- Authorised Users who require a password reset to an information system administered by Victoria Police, (for example network, mainframe, corporate application system, or shared network folders/directories) are to contact a Sergeant/VPS-3 or above who can attest to the identity of the individual, to complete a Password Reset Form [Form 1023] on their behalf and submit it to the Help Desk for action.

- Authorised Users who require a password reset to information systems administered by an external organisation, (for example CrimTrac, interstate systems, VicRoads) are to contact the LEAP Management Unit for assistance.
- Authorised Users who require a password reset to a non-corporate application system (for example locally managed forensic databases), should contact the relevant System Owner directly for assistance.

4. Contracted Third Parties (CTP) or Approved Third Parties (ATP)

- Applications for access, or variation of access, for an individual under a CTP or ATP arrangement are to include the details of the:
 - Victoria Police nominated employee accountable for the ATP or CTP and
 - ATP or CTP employee responsible for ensuring compliance with requirements of the ATP or CTP arrangement including the appropriate access and use of information.
- Minimum details to be provided are:
 - full name and registered/employee number of the Victoria Police nominated employee
 - full name of the ATP or CTP employee overseeing the assignment, review and revocation of system access privileges
 - name of the ATP or CTP organisation
 - position/role within the ATP or CTP organisation
 - work address
 - contact phone number
 - non-Victoria Police email address, where available.
- The nominated employee is required to notify System Managers of any updates to these details.

Further Advice and Information

For further advice and assistance regarding these Policy Rules, contact Protective Security or your Work Unit Manager.

Update history

Date of first issue	03/12/2012	
Date updated	Summary of change	Force File number
	This instruction and the new <i>VPMP Information access</i> replace the previous <i>VPMP Access and use of information</i> after a comprehensive review by IMSSD in 2012	069562/11
21/01/13	Updated to reflect organisational governance and structural changes.	FF-074790
25/03/19	Administrative amendment to reflect name change from IMSSD to Protective Security.	FF-139207