IN THE MATTER OF THE ROYAL COMMISSION
INTO FAMILY VIOLENCE

ATTACHMENT WS AH-5 TO JOINT STATEMENT OF ASSISTANT COMMISSIONER WENDY MAREE STEENDAM AND SENIOR SERGEANT AILSA CAROLINE HOWARD

Date of document: 3 August 2015 Filed on behalf of: the Applicant Prepared by: Victorian Government Solicitor's Office Level 33 80 Collins Street Melbourne VIC 3000	[redacted]

This is the attachment marked **'WS AH-5'** produced and shown to **WENDY MAREE STEENDAM** and **AILSA CAROLINE HOWARD** at the time of signing their Joint Statement on 3 August 2015. [redacted]

Before me: . [redacted] ....

[redacted]

An Australian legal practitioner
within the meaning of the
Legal Profession Uniform Law (Victoria)

Attachment WS AH-5

Victoria Police Manual – Policy Rules

Information access

Context

Information that Victoria Police acquires, creates, stores and uses must at all times be used appropriately and kept secure from unauthorised access. This security and appropriate use of information is essential to the organisation's credibility and its ability to provide an effective and professional law enforcement service to the community.

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
- **availability** – to ensure that information and information systems are accessible and useable when required.

Victoria Police reserves the right to limit, restrict or extend access privileges to its information and information systems. Any employee, contractor or service provider who are authorised to access Victoria Police information, play an important role in maintaining the security of Victoria Police information and information systems and, as such, must familiarise themselves with their responsibilities in keeping police information secure and protected at all times from unauthorised access.

Victoria Police regards breaches or violations of this policy and/or the misuse of its information resources and privileges as particularly serious and may lead to disciplinary consequences and possible charges under section 227 and 228 of the *Victoria Police Act 2013*.

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 all Authorised Users granted access to police information.

Rules and Responsibilities

1. Access controls

1.1 Compliance

Access controls are an essential element to ensure the confidentiality, integrity and availability of Victoria Police information and information systems. The controls that must be implemented and maintained include:

- **Physical controls** – such as site access controls and storage facilities - see **VPMP Physical security** for details
- **Personnel controls** – including security checks and security clearances - see **VPMP Personnel security** for details
- **System controls** – including user identification and authentication - see **VPMG System access controls** for details
- **Information management controls** – including sharing, retention, disposal, security classification and associated handling procedures. These controls are supported by compliance of all Authorised Users with:
  - **VPMP Information use, handling and storage**
  - **VPMP Information review, retention and disposal**
  - **VPMP Information sharing.**

1.2 Responsible officers

While all Victoria Police employees are responsible for ensuring compliance with access controls, the following roles have responsibility for ensuring the implementation and maintenance of access controls:

	Physical Security	**Personnel Security**	**System Controls**	**Information Management Controls**
Work Unit Manager and/or Information Owner	Workplace / Site Security and Access	Staff identification and security clearances	Staff system access against current role and access criteria	Security of all work unit information and compliance to policy / departmental procedures and processes
Department Head	Site Security Plans	Position based security assessments		Compliance of departmental procedures and processes with policy
System Manager			User function access processes and auditing	Information security and records management processes and auditing
System Owner	System essential equipment location and security		System plans and implementation of user and function access controls	Application of information management principles to system development

1.3 *Criteria for access (employees and non-employees)*

- All Victoria Police information must have an owner who is responsible for the secure management of the information. This includes information stored in a Corporate Application (System Owner) or any 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 (Information Owner).

- Access to Victoria Police information and information systems must be authorised by the System or Information Owner of that information based on their judgement of the following factors:
  - relevant legislation and contractual obligations
  - whether the requestor has a legitimate business reason to access the information in order to perform their duties
  - sensitivity of the information involved
  - risk of damage to or loss of the particular information and/or information system.

- Once access has been approved the person becomes an Authorised User of that system.

- Pre-employment checks (VPM 301-3 and section 1.4) only provide clearance to access and handle police information below PROTECTED. Where an employee or other person will access or handle information at a higher security classification, an appropriate security clearance must be sought prior to providing access to the information. See **VPMP Personnel security** for policy rules on seeking security clearances.

- System and Information Owners may nominate a Victoria Police employee at an appropriate level as their delegate to be responsible for oversight of access requests and the timely removal or adjustment to access when required by section 1.5.

- **VPMG Information system access** outlines the procedure for obtaining access to information systems.

1.4 *Pre access checks for non-employees*

Work Unit Managers must ensure that any person under their supervision that does not have a current and valid Employee Number or Registered Number recorded in the Victoria Police personnel system (such as contractors and/or consultants) who require access to information and information systems for legitimate business reasons:

- successfully undergo a full criminal records and fingerprinting check; and,

- sign a Deed of Confidentiality [Form 1063] before being granted access to Victoria Police information and information systems.

1.5 Revising, revoking or removing access (employees and non-employees)

- Authorised Users must advise their Work Unit Manager when they intend to transfer, resign, retire, take extended leave or when they no longer require their allocated access.

- Work Unit Managers (or the responsible officer for an Contracted Third Party (CTP) or Approved Third Party (ATP) arrangement – refer to sections 6 and 7 for details) must ensure that access to all information or information systems is revised, revoked or removed when an Authorised User:
  - dies or ceases employment or engagement with Victoria Police
  - transfers to another Victoria Police work unit
  - takes leave of absence of any type in excess of three months
  - completes, or is no longer working on, a CTP contract (see section 6)
  - no longer requires the specified access to perform their duties, or
  - (in the case of employees only) are suspended or required to take leave pending a Professional Standards Command (PSC) investigation.

- In the above situations (excluding Victoria Police internal transfers) Work Unit Managers must ensure that:
  - all keys held by the person are collected
  - that all access cards are collected and disabled
  - all system access is disabled
  - any information (hardcopy or electronic) or police issued IT/information storage equipment held by the person (including "personal holdings") is collected and retained on police premises.

- If a person is being transferred within Victoria Police, Work Unit Managers must ensure that:
  - all keys held by them are collected unless still required for the new position
  - that all access cards are altered to reflect the access needs of the new position
  - all system access is disabled or amended to reflect the new position
  - any information (hardcopy or electronic) or police issued IT/information storage equipment held by the person, is collected and retained on police premises, or officially transferred to the gaining unit.

- **VPMG Information system access** provides further guidance on requesting changes to information systems access.

- The System Owner or System Manager may revise, revoke or remove an Authorised User's access to information or information systems if they believe the criteria for access (section 1.3) are no longer met.

- When an Authorised User with access to system administration accounts meets the above criteria for information access revision, revocation or removal, the System Managers must ensure that all system level passwords (and related authentication credentials such as ssh keys and certificates) known to that person are changed immediately.

1.6 *System access crosschecks*

- Human Resources must prepare regular, timely and accurate reports accessible electronically by System Managers, listing the cessation of duty of Victoria Police employees. System Managers must ensure that all access rights to information systems for these prior employees have been removed, and that the UserID is cancelled, in a timely manner.

- PSC must advise all System Managers, when an Authorised User is:
  - dismissed
  - suspended
  - required to take accrued leave prior to suspension or dismissal or
  - under investigation (only when access revocation is deemed appropriate by PSC).

- System Managers must ensure that all access rights are immediately revoked and only reinstated after authorisation from PSC.

- If the above crosschecks identify an ongoing failure of Work Unit Managers to meet the requirements' of section 1.5, the System Manager should report this to the Security Incident Manager, Information Management, Standards and Security Division (IMSSD).

1.7 *Maintenance of access controls*

- Work Unit Managers must conduct audits of who has access to the unit's information to ensure only Authorised Users with a current legitimate business reason retain access. This includes network folders/directories, physical storage, any non corporate systems and the physical work locations they are responsible for. This must be audited at least annually.

- For network folder/directory audit requests, the Work Unit Manager/ Information Owner must complete and submit a Request for Access Audit of a Shared Directory [Form 1131].

- Work Unit Managers must audit the currency and level of all personnel security clearances to ensure they remain appropriate to the security classification of the position held and the information managed.

- System Managers must maintain system user and function access controls (see **VPMG System access controls** for details) and implement user access changes requested by Work Unit Managers promptly.

2. Conditions of access for specific authorised groups

In instances where Work Unit Managers and other authorised Victoria Police groups require access to personal directories, email accounts and shared directories for reasons outside the general conditions of access, there are specific approved and authorised procedures. These are documented in VPMG System access for specific groups.

3. Password management

- A mandatory password(s) reset is required if Authorised Users discover any of the following incidents have occurred in relation to their password(s):
  - unauthorised discovery or usage by another person
  - system compromise (unauthorised access to a system or account)
  - transmission of a password, for example via email
  - disclosure of password to another person (accidental or intentional) or
  - a new password is provided to them and the IT support staff knows the password. For example, IT support staff provides a new password or has to reset an existing password.
- In the instance of suspected compromise of a password by any of the above incidents, a password(s) reset must be arranged immediately. Refer to **VPMG Information system access** for details of procedure.
- Any of the first four incidents noted above must also be reported to the Security Incident Manager, IMSSD.
- Refer to **VPMG Password management** for instructions on selection of secure passwords to comply with the password complexity business rules.
- If anyone requests or demands an Authorised Users' password(s) the requestor must be referred to this policy or to the Security Incident Manager, IMSSD.
- Audits of password quality may be performed on a periodic or random basis. Authorised Users are required to arrange a password reset if it is guessed or discovered during such an audit.

4. Information system virus controls

- System Owners must ensure that:
  - software installation is only undertaken by personnel authorised by the System Owner (or his/her delegate) for that Information System and
  - information systems within their control are regularly scanned to ensure that viruses have not entered the systems.
- Authorised Users must prevent the introduction of computer viruses onto Victoria Police information systems by ensuring they:
  - do not install any software on any Victoria Police information system

- do not open suspicious email attachments
- do not attempt to disable or circumvent antivirus software
- do not connect any unauthorised systems or links to a Victoria Police information system
- scan all removable media and devices before use, irrespective of their source and
- immediately advise the Help Desk if a virus, unauthorised software or unauthorised connection is suspected or detected.

5. Physical controls

Authorised Users must ensure that all non public domain information is physically protected from viewing or access by persons that do not have approval to access the information. This includes ensuring:

- the content of all official and security classified information is unobservable by people without a legitimate business need and appropriate security clearance to access that information

- all security classified information and other valuable resources are secured appropriately when unattended in line with **VPMP Information use, handling and storage** and **VPMG Portable computing devices**

- compliance with the site security plans and local work unit instructions/procedures

- all removable storage media or portable computing devices are secured and handled in line with **VPMP Information use, handling and storage** and **VPMG Portable computing devices**

- they have regard for the best practice recommendations in **VPMG Clear desk principles.**

6. Contracted Third Parties

- Contracted Third Parties (CTP) includes any suppliers, contractors, consultants or service providers. Where CTPs manage, access or hold Victoria Police information under contractual arrangements, the contract must:
  - recognise Victoria Police's legal ownership of Victoria Police records held or accessed by the CTP, and the information they contain
  - enable Victoria Police to have full and timely access to relevant records held
  - ensure the transfer of all records to Victoria Police at the completion of the contract
  - ensure that CTP staff who will access Victoria Police information and information systems comply with section 1.4

  - require the CTP to comply with Victoria Police's information management and information security standards, policies, procedures and guidelines for as long as they hold the information.

- Victoria Police Procurement Department and Legal Services Department are responsible for ensuring that all new or extended contracts involving management of Victoria Police information by CTPs include these requirements.

- The nominated Service Monitor (as defined under the **Victoria Police Contract Management Framework**) is responsible for ensuring the CTP meets these requirements through contract compliance checks or auditing.

- Where a CTP has an ongoing contract to provide IT services to Victoria Police (such as an outsourced service provider), the relevant Department Head may delegate the responsibility for managing access for the CTP staff to a representative of that organisation. However, the accountability for this function remains with the Department Head.

7. Approved Third Parties

- Approved Third Parties (ATPs) are other government agencies that have been granted direct access to Victoria Police information repositories through their IT system or are periodically sent Victoria Police information.

- All ATPs must only access Victoria Police repositories in accordance with a governing arrangement developed in accordance with **VPMP Formal arrangements with external agencies**.

- Each ATP arrangement must have a Victoria Police nominated employee and an ATP nominated employee as the responsible officers for management of access and appropriate use by ATP employees.

Quick Links

- VPMP Appropriate use of information
- VPMG Information system access
- VPMG Password management
- VPMG System access for specific groups
- VPMG Use of email
- VPMG Use of internet
- VPMG Clear desk principles

- VPMG Portable computing devices

Further Advice and Information

For further advice and assistance regarding these Policy Rules, contact Information Management, Standards and Security Division.

Update history

Date of first issue	03/12/2012	
Date updated	**Summary of change**	**Force File number**
	This instruction and the new *VPMP Information system access* replace the previous *VPMP Access and use of information* after a comprehensive review by IMSSD in 2012.	069562/11
21/01/13	Updated to reflect organisational governance and structural changes.	FF-074790
23/09/13	Minor changes to align terminology with amendments to *VPMG Password management.*	073882/12
18/11/13	References to redundant instruments following IMSSD review have been updated with corresponding new instruments.	069562/11
28/02/14	References to redundant instruments following IMSSD review have been updated with corresponding new instruments.	069562/11
01/07/14	Legislative references updated due to commencement of *Victoria Police Act 2013.*	069562/11
15/09/14	Alignment of security classification references to the Australian Government Protective Security Policy Framework	069562/11