Restrictions on the use of applications on Victoria Police devices

Context

The Commonwealth Government has increased the scrutiny of potentially malicious social media applications. This has led governments across Australia and overseas to restrict the installation and use of malicious applications on government-issued devices due to significant concerns that malicious applications can potentially:

- monitor activity and capture data on a user's device and store that data in a way which can be accessed by foreign intelligence and national security agencies
- provide a gateway for the covert deployment of malicious software (i.e. viruses) on to a user's device
- be exploited for the purpose of social engineering and disinformation campaigns.

In line with Commonwealth Government guidance, and in response to the risks posed, there are new limitations for the Victorian Government and associated agencies regarding the use of the restricted high-risk applications on government provided devices.

Victoria Police policy strictly controls the use of restricted applications on Victoria Police devices, limiting use of these applications to circumstances where exemptions have been approved (i.e., legitimate business purposes) and mitigating controls are applied.

This policy aligns with wider Whole of Victorian Government policy, and provides guidelines on:

- the limitations in relation to use of restricted applications
- the circumstances in which restricted applications can be used for law enforcement purposes.

Victoria Police employees must exercise care when using social media and engaging in online activities and avoid any actions that might be damaging to the reputation or security of the organisation. Refer to **VPM Social media and online engagement**. **VPM Professional and ethical standards** applies whether employees are using social media in an official or a personal capacity.

Policy at a glance

This policy:

- describes the applications restricted for use on Victoria Police devices
- explains the exceptional circumstances restricted applications may be used on Victoria Police devices
- describes the applications process for accessing and using restricted applications
- details the system and security requirements for authorised use of restricted applications
- provides reporting avenues for unauthorised use of restricted applications.

Contents

Definitions

The following definitions apply to this policy:

Victoria Police device – a piece of information technology (IT) equipment owned and issued by Victoria Police and used by any person to carry out their duties and functions, including but not limited to smart phones, tablets, laptops and desktop computers.

Personal device – a piece of IT equipment that is not owned and issued by Victoria Police.

Legitimate business reason - means a lawful and valid need to install or access the restricted application on a Victoria Police device to conduct Victoria Police business and/or achieve a work objective of Victoria Police.

Personally identifiable information – information that, when used alone or with other relevant information, can identify a person.

Restricted applications – web-based and software applications identified by Victoria Police as potentially malicious and should not be accessed, installed or used on a Victoria Police device. Restricted applications are listed in Appendix A.

Stand-alone device – refers to a device that does not have the Victoria Police managed image on it and is not connected to the Victoria Police network.

Also refer to the general VPM Dictionary for definitions and acronyms.

Scope and application

This policy applies to all employees, contractors, service providers, consultants, vendors and any other parties who have access to Victoria Police networks, data or devices.

Responsibilities and procedures

1. Use of restricted applications

- Victoria Police prohibits the installation of restricted applications and requires the removal of existing instances of restricted applications on Victoria Police devices, unless a legitimate business reason exists necessitating the installation or ongoing presence of the application.
- Employees must not access, install or use restricted applications on a Victoria Police device without authorisation as per this policy.
- Restricted applications must only be accessed or installed where all of the following has occurred:
    - a legitimate business reason has been authorised by the relevant assistant

commissioner or executive director, considering any relevant risks

- the applicant has completed a risk assessment and mitigation strategies have been implemented to reduce associated risks. Contact Digital Services and Security Department (DSSD) via the IT-SECURITY-ADVICE-MGR PBEA for further advice
- the Chief Information Security Officer (CISO) has provided final approval.

- A legitimate business reason to access a restricted application includes:
  - to carry out regulatory functions including compliance and enforcement activities
  - for authorised crime investigation and intelligence activities that relate directly to duties or functions within Victoria Police, such as surveillance and intelligence gathering
  - for research to be conducted or communications to be sent to assist with a law enforcement purpose
  - to reach key audiences to undertake education, child safety, marketing or public relations activity on behalf of Victoria Police.
- Employees must not use their personal device to access or use restricted applications for law enforcement purposes.

2. Use for legitimate business reason

- There are a variety of investigative and intelligence functions that may constitute a legitimate business reason to use a restricted application.
- Investigations and inquiries using restricted applications are to be conducted according to established policies and guidelines, including the use of online personas; refer to **VPM Official online activities** and **VPM Assumed identities and online personas**.
- For guidance about investigation or intelligence gathering that involves discreet or covert official online activities, refer to **VPM Official online activities** and **VPM Assumed identities and online personas**.
- Where access or use of a restricted application is required for a legitimate business reason, employees must apply to install and use the restricted application using the application form located on the DSSD intranet page. This must include prior endorsement from the appropriate assistant commissioner/executive director and evidence of this provided with the completed application form.

3. Security controls for authorised use of restricted applications

- The CISO must approve the use of restricted applications on Victoria Police devices only where there is a legitimate business reason. The approval period will be for the duration of the legitimate business reason or for a period not exceeding 12 months and the following security controls must be met:
  - the restricted application must only be installed and/or accessed on a stand-alone device
  - the stand-alone device must be appropriately stored and secured when not in use. This includes the isolation of these devices from sensitive conversations and information (i.e. by switching off the device)
  - metadata must be removed from photos, videos and documents when uploading any content to restricted applications

  - personally identifiable information must not be shared on restricted applications
  - the use of restricted applications must be approved by the assistant commissioner /executive director and CISO
  - all accounts accessing restricted applications must use multi-factor authentication and unique passphrases
  - all devices that access restricted applications must use the latest available operating system to control individual application permissions. The CISO must establish processes to regularly check for and update the application to ensure the latest version is used
  - restricted applications must only be installed from trusted stores, such as the Microsoft Store, Google Play Store and the Apple App Store.
- Work unit managers must ensure restricted applications are accessed only by authorised users and that access is immediately revoked when there is no longer a business need for that access or use.
- The CISO must ensure that the terms and conditions of the restricted application are regularly reviewed, as well as application permissions with each update, to ensure appropriate risk management controls can be put in place or adjusted as required.
- Restricted applications must be deleted from devices when the legitimate business reason no longer exists or authorisation expires.

4. Unauthorised use of restricted applications

- Where an employee believes on reasonable grounds that another employee is, or has engaged in unauthorised or improper use of restricted applications they must report this behaviour to any one of:
  - the Security Incident Registry
  - a work unit manager
  - sub-officer or above
  - the Police Conduct Unit, Professional Standards Command via submission of a Complaint Form [VP 918]
  - the Independent Broad-based Anti-corruption Commission (IBAC) in accordance with either s.167(3), *Victoria Police Act 2013* or Part 2 of the *Public Interest Disclosure Act 2012*.

Related documents

- VPMG Portable computing devices
- VPM Recording devices, CCTV and digital asset management
- VPMG Mobile/smart phones
- VPM Official online activities
- VPM Assumed identities and online personas
- VPMP Appropriate use of information
- VPMP Information access
- VPMG Information system access

- CCI 10/17 Mobile Device Deployment

Further advice and information

For further advice and assistance regarding these Policy Rules, contact IT-SECURITY ADVISOR-MGR.

Update history

DATE UPDATED	SUMMARY OF CHANGE	FORCE FILE NUMBER
31/01/2025	New policy replaces **CCI 06/24 Restrictions on the use of applications on Victoria Police devices**.	FF-259443
15/05/2025	Updated Appendix A to include DeepSeek and Kaspersky Lab Incorporated as restricted applications.	FF-259443

Appendix A

The following are restricted applications:

- TikTok
- DeepSeek
- Kaspersky Lab Incorporated.