



# Information security manual

## Guidelines for enterprise mobility

Last updated: September 2026

### Enterprise mobility

#### Context

Enterprise mobility generally refers to situations in which personnel work in a mobile manner, such as part of office hot-desking arrangements, when working from home, when travelling or simply when outside the office environment during normal business hours. While enterprise mobility has traditionally been used to refer to the use of mobile devices, such as smartphones, tablets and laptop computers, it is increasingly being applied to the use of desktop computers as part of working from home arrangements.

This section applies to privately owned and organisation-owned mobile devices and desktop computers that use either a mobile operating system or a desktop operating system.

#### Privately owned mobile devices and desktop computers

Allowing privately owned mobile devices and desktop computers to access an organisation's systems or data can increase liability risk. As such, an organisation should seek legal advice to ascertain whether this scenario affects compliance with relevant legislation, such as the [Privacy Act 1988](#) and the [Archives Act 1983](#). Furthermore, if an organisation chooses to allow personnel to use privately owned mobile devices or desktop computers to access their organisation's classified systems or data, they should ensure that it does not present an unacceptable security risk. This can be achieved in part through the enforced separation of classified data and personal data, preventing the storage of classified data on privately owned mobile devices and desktop computers, and disallowing the use of unapproved artificial intelligence agents.

**Control: ISM-1297; Revision: 6; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Legal advice is sought prior to allowing privately owned mobile devices and desktop computers to access systems or data.*

**Control: ISM-1400; Revision: 11; Updated: Jun-26; Applicable: OS, P; Essential 8: N/A**

*Personnel using privately owned mobile devices or desktop computers to access OFFICIAL: Sensitive or PROTECTED systems or data have enforced separation of classified data and personal data.*

**Control: ISM-1866; Revision: 2; Updated: Jun-26; Applicable: OS, P; Essential 8: N/A**

*Personnel using privately owned mobile devices or desktop computers to access OFFICIAL: Sensitive or PROTECTED systems or data are prevented from storing classified data on their privately owned mobile devices and desktop computers.*

**Control: ISM-2095; Revision: 1; Updated: Jun-26; Applicable: OS, P; Essential 8: N/A**

*Personnel using privately owned mobile devices or desktop computers to access OFFICIAL: Sensitive or PROTECTED systems or data are disallowed from granting access to unapproved artificial intelligence agents.*

**Control: ISM-0694; Revision: 9; Updated: Jun-26; Applicable: S, TS; Essential 8: N/A**

*Privately owned mobile devices and desktop computers do not access SECRET and TOP SECRET systems or data.*

## Organisation-owned mobile devices and desktop computers

If an organisation chooses to issue personnel with organisation-owned mobile devices or desktop computers to access their organisation's classified systems or data, they should ensure that it does not present an unacceptable security risk. This can be achieved in part by enforcing the separation of classified data and personal data.

**Control: ISM-1482; Revision: 9; Updated: Mar-26; Applicable: OS, P, S, TS; Essential 8: N/A**

*Personnel using organisation-owned mobile devices or desktop computers to access classified systems or data have enforced separation of classified data and personal data.*

## Mobile devices and desktop computers accessing the internet

When mobile devices and desktop computers access the internet, doing so via an organisation's internet gateway rather than directly can enable the provision of additional security functionality, such as web content filtering and protective Domain Name System services. However, in some cases, an organisation may instead accept the security risks associated with allowing direct connections to specific online services, such as web conferencing services and collaboration tools, for performance reasons.

When connecting mobile devices and desktop computers to an organisation's internet gateway via a virtual private network (VPN) connection, a split tunnel VPN can enable indirect access into the organisation's network from other networks, such as the internet. As such, if split tunnelling is not disabled, there is an increased security risk that the VPN connection could be used as an intrusion vector by malicious actors.

**Control: ISM-0874; Revision: 7; Updated: Mar-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile devices and desktop computers access the internet via an organisation's internet gateway rather than via a direct connection to the internet.*

**Control: ISM-0705; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*When accessing an organisation's network via a VPN connection, split tunnelling is disabled.*

## Further information

Further information on allowing the use of privately owned mobile devices and desktop computers by personnel to access their organisation's systems or data can be found in the Australian Signals Directorate's (ASD) [Bring Your Own Device for executives](#) publication.

Further information and specific guidance on enterprise mobility can be found in ASD's [Risk management of enterprise mobility \(including Bring Your Own Device\)](#) publication.

Further information on cyber supply chain risk management can be found in the 'Cyber supply chain risk management' section of the [Guidelines for procurement and outsourcing](#).

Further information on the procurement and use of online services can be found in the 'Managed services and cloud services' section of the [Guidelines for procurement and outsourcing](#).

## Mobile device management

### Context

This section describes the hardening of privately owned and organisation-owned mobile devices, such as smartphones and tablets that use a mobile operating system. Alternatively, guidance for privately owned and organisation-owned mobile devices that use a desktop operating system is available in the 'Operating system hardening' section of the [Guidelines for system hardening](#).

### Mobile device management policy

Since mobile devices routinely leave the office environment, and the protection it affords, it is important that a mobile device management policy is developed, implemented and maintained to ensure that mobile devices are sufficiently hardened. In doing so, it is important that Mobile Device Management solutions that have completed a Common Criteria evaluation against the *Protection Profile for Mobile Device Management*, version 4.0 or later, are used to enforce mobile device management policy.

**Control: ISM-1533; Revision: 3; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*A mobile device management policy is developed, implemented and maintained.*

**Control: ISM-1195; Revision: 2; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile Device Management solutions that have completed a Common Criteria evaluation against the Protection Profile for Mobile Device Management, version 4.0 or later, are used to enforce mobile device management policy.*

### Approved mobile platforms

To ensure an appropriate level of security, mobile devices that access OFFICIAL: Sensitive or PROTECTED systems or data should use mobile platforms that have completed a Common Criteria evaluation against the *Protection Profile for Mobile Device Fundamentals*, version 3.3 or later, and are operated in accordance with the latest version of their associated ASD security configuration guide. Furthermore, to ensure interoperability and maintain trust, mobile devices that access SECRET or TOP SECRET systems or data must use mobile platforms that have been issued an Approval for Use by ASD and are operated in accordance with the latest version of their associated Australian Communications Security Instruction.

**Control: ISM-1867; Revision: 1; Updated: Mar-24; Applicable: OS, P; Essential 8: N/A**

*Mobile devices that access OFFICIAL: Sensitive or PROTECTED systems or data use mobile platforms that have completed a Common Criteria evaluation against the Protection Profile for Mobile Device Fundamentals, version 3.3 or later, and are operated in accordance with the latest version of their associated ASD security configuration guide.*

**Control: ISM-0687; Revision: 10; Updated: Sep-23; Applicable: S, TS; Essential 8: N/A**

*Mobile devices that access SECRET or TOP SECRET systems or data use mobile platforms that have been issued an Approval for Use by ASD and are operated in accordance with the latest version of their associated Australian Communications Security Instruction.*

## Encrypted storage

Suitably encrypting the internal storage, and any removable media, for mobile devices will help prevent malicious actors from gaining easy access to any sensitive or classified data stored on them if they are lost or stolen. As such, it is critical that ASD-approved cryptography is used.

**Control: ISM-0869; Revision: 6; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile devices encrypt their internal storage and any removable media using ASD-approved cryptography.*

**Control: ISM-1868; Revision: 0; Updated: Sep-23; Applicable: S, TS; Essential 8: N/A**

*SECRET and TOP SECRET mobile devices do not use removable media unless approved beforehand by ASD.*

## Encrypted communications

Failure to suitably encrypt mobile device communications, including those of mobile applications, when communicating sensitive or classified data presents an unacceptable security risk. As such, when encrypting data in transit, it is critical that ASD-approved cryptography is used.

**Control: ISM-1085; Revision: 5; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile devices encrypt all sensitive or classified data communicated over public network infrastructure using ASD-approved cryptography.*

**Control: ISM-2108; Revision: 0; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile applications encrypt all sensitive or classified data communicated over public network infrastructure using ASD-approved cryptography.*

## Maintaining mobile device security

Poorly secured mobile devices are more vulnerable to compromise and can provide malicious actors with a potential access point into any connected systems. Although an organisation may initially provide secure mobile devices, their security posture may degrade over time if personnel can install non-approved applications and disable or modify security functionality. Furthermore, it is important that security updates are applied to mobile devices as soon as they become available to maintain their security posture.

**Control: ISM-1886; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile devices are configured to operate in a supervised (or equivalent) mode.*

**Control: ISM-2096; Revision: 0; Updated: Mar-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile devices are configured to enforce separation between organisational and personal mobile applications and data.*

**Control: ISM-2097; Revision: 0; Updated: Mar-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile devices are configured with always on VPN functionality.*

**Control: ISM-1887; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile devices are configured with remote locate and wipe functionality.*

**Control: ISM-1888; Revision: 1; Updated: Mar-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile devices are configured with secure password-based lock screens.*

**Control: ISM-2098; Revision: 0; Updated: Mar-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile devices are configured to prevent data transfers over Universal Serial Bus connections.*

**Control: ISM-0863; Revision: 5; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile devices prevent personnel from installing non-approved applications once provisioned.*

**Control: ISM-0864; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile devices prevent personnel from disabling or modifying security functionality once provisioned.*

**Control: ISM-1366; Revision: 2; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Security updates are applied to mobile devices as soon as they become available.*

## Further information

Further information on cyber supply chain risk management can be found in the 'Cyber supply chain risk management' section of the [Guidelines for procurement and outsourcing](#).

Further information on evaluated products can be found in the 'Evaluated product procurement' section of the [Guidelines for evaluated products](#).

Further information on Common Criteria Protection Profiles for mobile devices can be found in the following United States' National Information Assurance Partnership publications:

- [Protection Profile for Mobile Device Management Version 4.0](#)
- [Protection Profile for Mobile Device Fundamentals Version 3.3](#).

Further information on hardening mobile platforms can be found in the following ASD publications:

- [Security configuration guide: Apple iOS 14 devices](#)
- [Security configuration guide: Samsung Galaxy S10, S20 and Note 20 devices](#)
- [Security configuration guide: Viasat Mobile Dynamic Defense](#).

Further information on encrypting mobile devices and their communications can be found in the 'Cryptographic fundamentals' section of the [Guidelines for cryptography](#).

## Mobile device usage

### Context

This section describes the usage of privately owned and organisation-owned mobile devices that use either a mobile operating system or a desktop operating system.

### Mobile device usage policy

Since mobile devices routinely leave the office environment, and the protection it affords, it is important that an organisation develops, implements and maintains a mobile device usage policy governing their use.

**Control: ISM-1082; Revision: 3; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*A mobile device usage policy is developed, implemented and maintained.*

## Personnel awareness

As mobile devices often have voice and data communication capabilities, personnel should be made aware of the sensitivity or classification of voice and data that mobile devices have been approved to process, store and communicate. In addition, personnel should be made aware of common security practices for mobile device usage.

**Control: ISM-1083; Revision: 2; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Personnel are advised of the sensitivity or classification permitted for voice and data communications when using mobile devices.*

**Control: ISM-1299; Revision: 4; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Personnel are advised to take the following precautions when using mobile devices:*

- *never leave mobile devices or removable media unattended, including by placing them in checked-in luggage or leaving them in hotel safes*
- *never store credentials with mobile devices that they grant access to, such as in laptop computer bags*
- *never lend mobile devices or removable media to untrusted people, even if briefly*
- *never allow untrusted people to connect their mobile devices or removable media to your mobile devices, including for charging*
- *never connect mobile devices to designated charging stations or wall outlet charging ports*
- *never use gifted or unauthorised peripherals, chargers or removable media with mobile devices*
- *never use removable media for data transfers or backups that have not been checked for malicious code beforehand*
- *avoid reuse of removable media once used with other parties' systems or mobile devices*
- *avoid connecting mobile devices to open or untrusted Wi-Fi networks*
- *consider disabling any communications capabilities of mobile devices when not in use, such as Wi-Fi, Bluetooth, Near Field Communication and ultra-wideband*
- *consider periodically rebooting mobile devices*
- *consider using a VPN connection to encrypt all cellular and wireless communications*
- *consider using encrypted email or messaging apps for all communications.*

## Using paging, message services and messaging apps

As paging, messaging services and many messaging apps do not sufficiently encrypt data in transit, they cannot be relied upon for the communication of sensitive or classified data.

**Control: ISM-0240; Revision: 7; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Paging, Multimedia Message Service, Short Message Service and messaging apps are not used to communicate sensitive or classified data.*



## Using Bluetooth functionality

To mitigate security risks associated with pairing mobile devices with other Bluetooth devices, Bluetooth version 4.1 introduced the Secure Connections functionality for Bluetooth Classic, while Bluetooth version 4.2 introduced the Secure Connections functionality for Bluetooth Low Energy. This functionality uses keys generated using Elliptic Curve Diffie-Hellman cryptography, offering greater security compared to previous key exchange protocols. However, personnel should still consider the location and way they pair non-classified, OFFICIAL: Sensitive and PROTECTED mobile devices with other Bluetooth devices, such as by avoiding pairing devices in public locations, and remove all Bluetooth pairings when there is no longer a requirement for their use. In contrast, the Bluetooth protocol provides inadequate protection for the communication of SECRET and TOP SECRET data. As such, Bluetooth functionality is not suitable for use with SECRET and TOP SECRET mobile devices.

**Control: ISM-1196; Revision: 4; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A**

*Non-classified, OFFICIAL: Sensitive and PROTECTED mobile devices are configured to remain undiscoverable to other Bluetooth devices except during Bluetooth pairing.*

**Control: ISM-1200; Revision: 7; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A**

*Bluetooth pairing for non-classified, OFFICIAL: Sensitive and PROTECTED mobile devices is performed using Secure Connections, preferably with Numeric Comparison if supported.*

**Control: ISM-1198; Revision: 4; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A**

*Bluetooth pairing for non-classified, OFFICIAL: Sensitive and PROTECTED mobile devices is performed in a manner such that connections are only made between intended Bluetooth devices.*

**Control: ISM-1199; Revision: 5; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A**

*Bluetooth pairings for non-classified, OFFICIAL: Sensitive and PROTECTED mobile devices are removed when there is no longer a requirement for their use.*

**Control: ISM-0682; Revision: 5; Updated: Dec-21; Applicable: S, TS; Essential 8: N/A**

*Bluetooth functionality is not enabled on SECRET and TOP SECRET mobile devices.*

## Connecting mobile devices to connected vehicles

Connected vehicles often monitor, record, aggregate and communicate data on vehicle occupants, their connected mobile devices and their surrounding environment. In many cases, this data is then sent to the vehicle manufacturer, which could then be sold to or shared with third parties.

**Control: ISM-2099; Revision: 0; Updated: Mar-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile devices are not connected to the infotainment systems of connected vehicles.*

## Using mobile devices within or near connected vehicles

Personnel should be aware of the environment in which they use mobile devices to view or communicate sensitive or classified data. Including by ensuring that sensitive or classified data is not viewed or communicated within or near connected vehicles due to the potential for mobile device screens to be recorded by cameras or for conversations to be recorded, retained and communicated by connected vehicle infotainment systems or connected services.

**Control: ISM-2100; Revision: 0; Updated: Mar-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Sensitive or classified data is not viewed on mobile devices within or near connected vehicles.*

**Control: ISM-2101; Revision: 0; Updated: Mar-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Sensitive or classified phone calls and conversations are not conducted within or near connected vehicles.*

## Using mobile devices in public spaces

Personnel should be aware of the environment in which they use mobile devices to view or communicate sensitive or classified data. Including by ensuring that sensitive or classified data is not observed by other parties in public areas, such as on public transport, in transit lounges and at coffee shops. In some cases, privacy filters can be applied to the screen of a mobile device to prevent onlookers from reading content off its screen.

In addition, personnel should maintain awareness of the environments from which they conduct sensitive or classified phone calls and the potential for their conversations to be overheard.

**Control: ISM-0866; Revision: 6; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Sensitive or classified data is not viewed on mobile devices in public locations unless care is taken to reduce the chance of the screen of a mobile device being observed.*

**Control: ISM-1145; Revision: 4; Updated: Dec-21; Applicable: S, TS; Essential 8: N/A**

*Privacy filters are applied to the screens of SECRET and TOP SECRET mobile devices.*

**Control: ISM-1644; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Sensitive or classified phone calls and conversations are not conducted in public locations unless care is taken to reduce the chance of conversations being overheard.*

## Maintaining control of mobile devices

As mobile devices are portable in nature, and can be easily lost or stolen, personnel should maintain continual direct supervision of them when being actively used and ensure they are carried or stored in a secured state when not being actively used. While mobile devices may be encrypted, the effectiveness of encryption might be reduced if they are lost or stolen while in sleep mode or powered on with a locked screen.

**Control: ISM-0871; Revision: 3; Updated: Apr-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile devices are kept under continual direct supervision when being actively used.*

**Control: ISM-0870; Revision: 3; Updated: Apr-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile devices are carried or stored in a secured state when not being actively used.*

**Control: ISM-1084; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*If unable to carry or store mobile devices in a secured state, they are physically transferred in a security briefcase or an approved multi-use satchel, pouch or transit bag.*

## Mobile device emergency sanitisation processes and procedures

The sanitisation of mobile devices in emergencies can assist in reducing the potential for compromise of data by malicious actors. This may be achieved by using a remote wipe capability, a cryptographic key zeroise or sanitisation function if present.

**Control: ISM-0701; Revision: 6; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Mobile device emergency sanitisation processes, and supporting mobile device emergency sanitisation procedures, are developed, implemented and maintained.*



**Control: ISM-0702; Revision: 5; Updated: Dec-21; Applicable: S, TS; Essential 8: N/A**

*If a cryptographic zeroise or sanitise function is provided for cryptographic keys on a SECRET or TOP SECRET mobile device, the function is used as part of mobile device emergency sanitisation processes and procedures.*

## Before travelling overseas with mobile devices

Personnel travelling overseas with mobile devices face additional security risks compared to travelling domestically, especially when travelling to high or extreme risk countries. As such, appropriate precautions should be taken. Personnel should also be aware that when they leave Australian borders, they also leave behind any expectations of privacy.

**Control: ISM-1298; Revision: 2; Updated: Oct-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Personnel are advised of privacy and security risks when travelling overseas with mobile devices.*

**Control: ISM-1554; Revision: 2; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*If travelling overseas with mobile devices to high or extreme risk countries, personnel are:*

- *issued with newly provisioned user accounts, mobile devices and removable media from a pool of dedicated travel devices which are used solely for work-related activities*
- *advised on how to apply and inspect tamper seals to key areas of mobile devices*
- *advised to avoid taking any personal mobile devices, especially if rooted or jailbroken.*

**Control: ISM-1555; Revision: 3; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Before travelling overseas with mobile devices, personnel take the following actions:*

- *record all details of the mobile devices being taken, such as product types, serial numbers and International Mobile Equipment Identity numbers*
- *update all operating systems and applications*
- *remove all non-essential data, applications and user accounts*
- *backup all remaining data, applications and settings.*

## While travelling overseas with mobile devices

Personnel lose control of mobile devices and removable media any time they are not on their person. In addition, allowing untrusted people to access mobile devices provides an opportunity for them to be tampered with.

**Control: ISM-1088; Revision: 6; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Personnel report the potential compromise of mobile devices, removable media or credentials to their organisation as soon as possible, especially if they:*

- *provide credentials to foreign government officials*
- *decrypt mobile devices for foreign government officials*
- *have mobile devices taken out of sight by foreign government officials*
- *have mobile devices or removable media stolen, including if later returned*

- *lose mobile devices or removable media, including if later found*
- *observe unusual behaviour of mobile devices.*

## After travelling overseas with mobile devices

Following overseas travel with mobile devices, personnel should take appropriate precautions to ensure that they do not pose an undue security risk to their organisation's systems. In most cases, sanitising and resetting mobile devices, including all removable media, will be sufficient. However, upon returning from high or extreme risk countries, additional precautions will likely be needed.

**Control: ISM-1300; Revision: 6; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*Upon returning from travelling overseas with mobile devices, personnel take the following actions:*

- *sanitise and reset mobile devices, including all removable media*
- *decommission any credentials that left their possession during their travel*
- *report if significant doubt exists as to the integrity of any mobile devices or removable media.*

**Control: ISM-1556; Revision: 3; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A**

*If returning from travelling overseas with mobile devices to high or extreme risk countries, personnel take the following additional actions:*

- *reset credentials used with mobile devices, including those used for remote access to their organisation's systems*
- *monitor user accounts for any indicators of compromise, such as failed logon attempts.*

## Further information

Further information on Bluetooth security can be found in National Institute of Standards and Technology Special Publication 800-121 Rev. 2, [Guide to Bluetooth Security](#).

Further information on usage of mobile devices in SECRET and TOP SECRET areas can be found in the 'Facilities and systems' section of the [Guidelines for physical security](#).

Further information on security briefcases can be found in the Australian Security Intelligence Organisation's Security Equipment Guide-005, *Briefcases for the Carriage of Security Classified Information*. This publication is available from the Protective Security Policy GovTEAMS community or the Australian Security Intelligence Organisation by email.

Further information on approved multi-use satchels, pouches and transit bags can be found on the Security Construction and Equipment Committee's [Security Equipment Evaluated Products List](#).

## Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

## Copyright

© Commonwealth of Australia 2026

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license (<https://creativecommons.org/licenses/by/4.0/>).

For the avoidance of doubt, this means this license only applies to material as set out in this document.



The details of the relevant license conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 license (<https://creativecommons.org/licenses/by/4.0/legalcode.en>).

## Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (<https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines>).



**Australian Government**  
**Australian Signals Directorate**

**ASD**

AUSTRALIAN  
SIGNALS  
DIRECTORATE

**ACSC**

Australian  
**Cyber Security**  
Centre