Australian Government
Australian Signals Directorate

# Information Security Manual

**Published:** 1 December 2023

# Guidelines for Enterprise Mobility

## Enterprise mobility

### Introduction to enterprise mobility

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 both 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 work data from personal data as well as by preventing the storage of any classified data on privately-owned mobile devices and desktop computers.

***Control: ISM-1297; Revision: 5; Updated: Sep-23; Applicability: All; Essential Eight: 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: 8; Updated: Sep-23; Applicability: OS, P; Essential Eight: N/A***
*Personnel accessing OFFICIAL: Sensitive or PROTECTED systems or data using privately-owned mobile devices or desktop computers have enforced separation of work data from personal data.*

***Control: ISM-1866; Revision: 0; Updated: Sep-23; Applicability: OS, P; Essential Eight: N/A***
*Personnel accessing OFFICIAL: Sensitive or PROTECTED systems or data using privately-owned mobile devices or desktop computers are prevented from storing classified data on their privately-owned mobile devices and desktop computers.*

***Control: ISM-0694; Revision: 8; Updated: Sep-23; Applicability: S, TS; Essential Eight: 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 systems or data, they should ensure that it does not present an unacceptable security risk. This can be achieved in part by either prohibiting its use for personal purposes or by enforcing the separation of work data from any personal data.

***Control: ISM-1482; Revision: 7; Updated: Sep-23; Applicability: OS, P, S, TS; Essential Eight: N/A***
*Personnel accessing systems or data using an organisation-owned mobile device or desktop computer are either prohibited from using it for personal purposes or have enforced separation of work data from any personal data.*

### Connecting mobile devices and desktop computers to the internet

When connecting mobile devices and desktop computers to the internet, good practice generally involves establishing a Virtual Private Network (VPN) connection to an organisation's internet gateway rather than a direct connection to the internet. In doing so, mobile devices and desktop computers will typically be protected by additional security functionality, such as web content filtering, provided by an organisation's internet gateway. Note, however, in some cases an organisation may accept the security risks associated with allowing direct connections to specific online services, such as web conferencing services and collaboration tools, for performance reasons.

In connecting mobile devices and desktop computers to an organisation's internet gateway, a split tunnel VPN can allow access into the organisation's network from other networks, such as the internet. If split tunnelling is not disabled, there is an increased security risk that the VPN connection will be susceptible to intrusions from other networks.

***Control: ISM-0874; Revision: 6; Updated: Sep-23; Applicability: All; Essential Eight: N/A***
*Mobile devices and desktop computers access the internet via a VPN connection to an organisation's internet gateway rather than via a direct connection to the internet.*

***Control: ISM-0705; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: 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 (ASD)'s *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

### Mobile device management

This section describes the management of mobile devices, such as smartphones and tablets, that use a mobile operating system. Alternatively guidance for mobile devices that use a desktop operating system is available in the *Guidelines for System Hardening* and the *Guidelines for System Management*.

### 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; Applicability: All; Essential Eight: N/A***
*A mobile device management policy is developed, implemented and maintained.*

***Control: ISM-1195; Revision: 2; Updated: Sep-23; Applicability: All; Essential Eight: 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

In order to ensure an appropriate level of security, mobile devices that access OFFICIAL: Sensitive or PROTECTED systems or data must use mobile platforms that have completed a Common Criteria evaluation against the *Protection Profile for Mobile Device Fundamentals*, version 3.2 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: 0; Updated: Sep-23; Applicability: OS, P; Essential Eight: 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 3.2 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; Applicability: S, TS; Essential Eight: 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.*

## Data storage

Encrypting the internal storage, and any removable media, for mobile devices will prevent malicious actors from gaining easy access to any sensitive or classified data stored on them if they are lost or stolen.

***Control: ISM-0869; Revision: 5; Updated: Dec-21; Applicability: All; Essential Eight: N/A***
*Mobile devices encrypt their internal storage and any removable media.*

***Control: ISM-1868; Revision: 0; Updated: Sep-23; Applicability: S, TS; Essential Eight: N/A***
*SECRET and TOP SECRET mobile devices do not use removable media unless approved beforehand by ASD.*

## Data communications

If appropriate encryption is not available to protect data in transit, mobile devices communicating sensitive or classified data will present a security risk.

***Control: ISM-1085; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A***
*Mobile devices encrypt all sensitive or classified data communicated over public network infrastructure.*

## 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 are capable of installing non-approved applications and disabling or modifying security functionality. Furthermore, it is important that security updates are applied to mobile devices as soon as they become available in order to maintain their security posture.

***Control: ISM-1886; Revision: 0; Updated: Dec-23; Applicability: All; Essential Eight: N/A***
*Mobile devices are configured to operate in a supervised (or equivalent) mode.*

***Control: ISM-1887; Revision: 0; Updated: Dec-23; Applicability: All; Essential Eight: N/A***
*Mobile devices are configured with remote locate and wipe functionality.*

***Control: ISM-1888; Revision: 0; Updated: Dec-23; Applicability: All; Essential Eight: N/A***
*Mobile devices are configured with secure lock screens.*

***Control: ISM-0863; Revision: 5; Updated: Dec-23; Applicability: All; Essential Eight: N/A***

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

***Control: ISM-0864; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A***
*Mobile devices prevent personnel from disabling or modifying security functionality once provisioned.*

***Control: ISM-1366; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: 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 3.2*
- *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

### Mobile device usage

This section describes the usage of 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; Applicability: All; Essential Eight: N/A***
*A mobile device usage policy is developed, implemented and maintained.*

### Personnel awareness

Mobile devices can have both a voice and data communications component. In such cases, personnel should know 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; Applicability: All; Essential Eight: 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; Applicability: All; Essential Eight: 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; Applicability: All; Essential Eight: 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, thereby offering greater security compared to previous key exchange protocols. However, personnel should still consider the location and manner in which they pair 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.

Note, however, 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: 3; Updated: Sep-23; Applicability: OS, P; Essential Eight: N/A***
*OFFICIAL: Sensitive and PROTECTED mobile devices are configured to remain undiscoverable to other Bluetooth devices except during Bluetooth pairing.*

***Control: ISM-1200; Revision: 6; Updated: Sep-23; Applicability: OS, P; Essential Eight: N/A***
*Bluetooth pairing for OFFICIAL: Sensitive and PROTECTED mobile devices is performed using Secure Connections, preferably with Numeric Comparison if supported.*

***Control: ISM-1198; Revision: 3; Updated: Sep-23; Applicability: OS, P; Essential Eight: N/A***
*Bluetooth pairing for 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: 4; Updated: Sep-23; Applicability: OS, P; Essential Eight: N/A***
*Bluetooth pairings for 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; Applicability: S, TS; Essential Eight: N/A***
*Bluetooth functionality is not enabled on SECRET and TOP SECRET mobile devices.*

## 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. In particular, personnel should take care to ensure 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: 5; Updated: Jun-21; Applicability: All; Essential Eight: N/A***
*Sensitive or classified data is not viewed or communicated 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; Applicability: S, TS; Essential Eight: N/A***
*Privacy filters are applied to the screens of SECRET and TOP SECRET mobile devices.*

***Control: ISM-1644; Revision: 0; Updated: Jun-21; Applicability: All; Essential Eight: N/A***
*Sensitive or classified phone calls 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, it is strongly advised that personnel maintain continual direct supervision of them when they are being actively used and carry or store them in a secured state when they are not being activity used. Note, 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; Applicability: All; Essential Eight: N/A***
*Mobile devices are kept under continual direct supervision when being actively used.*

***Control: ISM-0870; Revision: 3; Updated: Apr-19; Applicability: All; Essential Eight: 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; Applicability: All; Essential Eight: 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 emergency situations can assist in reducing the potential for compromise of data by malicious actors. This may be achieved through the use of a remote wipe capability or a cryptographic key zeroise or sanitisation function if present.

***Control: ISM-0701; Revision: 6; Updated: Dec-22; Applicability: All; Essential Eight: 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; Applicability: S, TS; Essential Eight: 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; Applicability: All; Essential Eight: N/A***
*Personnel are advised of privacy and security risks when travelling overseas with mobile devices.*

***Control: ISM-1554; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A***
*If travelling overseas with mobile devices to high or extreme risk countries, personnel are:*

- *issued with newly provisioned 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: 2; Updated: Dec-23; Applicability: All; Essential Eight: 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 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; Applicability: All; Essential Eight: 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 and data. 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; Applicability: All; Essential Eight: 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: 2; Updated: Dec-22; Applicability: All; Essential Eight: 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 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*.

Further information on travelling overseas with mobile devices can be found in ASD's *Travelling Overseas With Electronic Devices* publication.