Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

JUNE 2021

Guidelines for Enterprise Mobility

Mobile device management

Types of mobile devices

These guidelines describe the use of mobile devices such as laptops, mobile phones and tablets.

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 to ensure that they are protected in an appropriate manner.

Security Control: 1533; Revision: 2; Updated: Aug-19; Applicability: O, P, S, TS
A mobile device management policy is developed and implemented.

Security Control: 1195; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
A Mobile Device Management solution is used to ensure mobile device management policy is applied to all mobile devices.

Security Control: 0687; Revision: 6; Updated: Jun-21; Applicability: TS
Mobile devices do not process, store or communicate TOP SECRET data unless explicitly approved by the ACSC to do so.

Privately-owned mobile devices

If organisations choose to allow personnel to use privately-owned mobile devices to access their organisation's systems or data, they should ensure that the devices do not present an unacceptable security risk. Further information on security risks, and recommended security controls, for allowing the use of privately-owned mobile devices are discussed in the ACSC's ***Risk Management of Enterprise Mobility Including Bring Your Own Device (BYOD)*** publication.

Security Control: 1400; Revision: 5; Updated: Jun-21; Applicability: O, P
Personnel accessing official or classified systems or data using a privately-owned mobile device use an ACSC approved platform, a security configuration in accordance with ACSC guidance, and have enforced separation of official and classified data from any personal data.

Security Control: 0694; Revision: 6; Updated: Jun-21; Applicability: S, TS
Privately-owned mobile devices do not access highly classified systems or data.

Seeking legal advice for privately-owned mobile devices

Allowing privately-owned mobile devices to access an organisation's systems or data can increase liability risk. Organisations should seek legal advice to ascertain whether this scenario affects compliance with relevant legislation (e.g. compliance with government data retention laws in the ***Archives Act 1983***), and also consider whether the increased liability risks are acceptable to the organisation. Risks will be dependent on each organisation's mobile device usage policy and its implementation.

Security Control: 1297; Revision: 3; Updated: Jun-21; Applicability: O, P, S, TS
Legal advice is sought prior to allowing privately-owned mobile devices to access official or classified systems or data.

Organisation-owned mobile devices

If organisations choose to issue personnel with mobile devices to access their organisation's systems or data, they should ensure that the devices do not present an unacceptable security risk. Further information on security risks, and recommended security controls, for allowing the use of organisation-owned mobile devices are discussed in the ACSC's ***Risk Management of Enterprise Mobility Including Bring Your Own Device (BYOD)*** publication.

Security Control: 1482; Revision: 4; Updated: Jun-21; Applicability: O, P, S, TS
Personnel accessing official or classified systems or data using an organisation-owned mobile device use an ACSC approved platform with a security configuration in accordance with ACSC guidance.

Mobile device storage encryption

Encrypting the internal storage and removable media of mobile devices will lessen security risks associated with a lost or stolen device as it will present a significant challenge to an adversary looking to gain easy access to data stored on the device.

Security Control: 0869; Revision: 4; Updated: Jun-21; Applicability: O, P, S, TS
All data on mobile devices is encrypted using at least an Australian Signals Directorate Approved Cryptographic Algorithm.

Mobile device communications encryption

If appropriate encryption is not available, mobile devices communicating sensitive or classified data present a security risk. Encrypting communications, regardless of the protocol used, is the only way to have any assurances that the data is protected.

Security Control: 1085; Revision: 3; Updated: Jun-21; Applicability: O, P, S, TS
Mobile devices used to communicate sensitive or classified data over public network infrastructure use encryption approved for communicating such data over public network infrastructure.

Mobile device Bluetooth functionality

Bluetooth provides inadequate security for data that is passed between mobile devices and other Bluetooth devices. As such, Bluetooth is not suitable for use with highly classified mobile devices. Furthermore, as Bluetooth has a number of known weaknesses which can potentially be exploited, the range of Bluetooth communications for all other mobile devices should be limited.

Security Control: 1202; Revision: 1; Updated: Sep-18; Applicability: O, P
The range of Bluetooth communications between mobile devices and other Bluetooth devices is restricted to less than 10 metres by using class 2 or class 3 Bluetooth devices.

Security Control: 0682; Revision: 4; Updated: Sep-18; Applicability: S, TS
Bluetooth functionality is not enabled on highly classified mobile devices.

Mobile device Bluetooth pairing

To mitigate security risks associated with pairing mobile devices with other Bluetooth devices, Bluetooth version 2.1 introduced secure simple pairing and extended inquiry response. Secure simple pairing improved the pairing experience for Bluetooth devices and introduced a form of public key cryptography while extended inquiry response provided more data during the inquiry procedure to allow for better filtering of Bluetooth devices.

In addition to using Bluetooth devices that support at least Bluetooth version 2.1, personnel should consider the location and manner in which they pair Bluetooth devices. For example, by avoiding pairing devices in public locations.

Security Control: 1196; Revision: 1; Updated: Sep-18; Applicability: O, P
Mobile devices are configured to remain undiscoverable to other Bluetooth devices except during Bluetooth pairing.

Security Control: 1200; Revision: 3; Updated: Sep-18; Applicability: O, P
Bluetooth pairing is performed using Bluetooth version 2.1 or later.

Security Control: 1198; Revision: 1; Updated: Sep-18; Applicability: O, P
Bluetooth pairing is performed in a manner such that connections are only made between intended Bluetooth devices.

Security Control: 1199; Revision: 1; Updated: Sep-18; Applicability: O, P
Bluetooth pairings are removed from mobile devices when there is no longer a requirement for their use.

Configuration control

Poorly controlled mobile devices are more vulnerable to compromise and provide an adversary with a potential access point into systems. Although organisations may initially provide secure mobile devices, the state of security may degrade over time. The security of mobile devices should be audited regularly to ensure their integrity.

Security Control: 0863; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Mobile devices prevent personnel from installing or uninstalling applications once provisioned.

Security Control: 0864; Revision: 3; Updated: Apr-19; Applicability: O, P, S, TS
Mobile devices prevent personnel from disabling or modifying security functions once provisioned.

Maintaining mobile device security

It is important that mobile devices are regularly tested to ensure that they meet organisation-defined security configurations and that patches are being applied.

Security Control: 1365; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Mobile carriers that are able to provide timely security updates for mobile devices are used.

Security Control: 1366; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Mobile devices are able to accept security updates from mobile carriers as soon as they become available.

Connecting mobile devices to the internet

During the time mobile devices are connected to the internet for web browsing they are directly exposed to targeted cyber intrusions originating from the internet. Should web browsing be required, best practice involves establishing a Virtual Private Network (VPN) connection and browsing the web though an organisation's internet gateway.

A split tunnel VPN can allow access to systems from another network, including unsecured networks such as the internet. If split tunnelling is not disabled there is an increased security risk that the VPN connection is susceptible to targeted cyber intrusions from such networks. Disabling split tunnelling may not be achievable on all mobile devices. Organisations can refer to the relevant ACSC guidance for mobile devices on how to manage security risks associated with split tunnelling.

Security Control: 0874; Revision: 4; Updated: Sep-18; Applicability: O, P

Web browsing from mobile devices is conducted through an organisation's internet gateway rather than via a direct connection to the internet.

Security Control: 0705; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
When accessing an organisation system via a VPN connection, split tunnelling is disabled.

Further information

Further information on the use of mobile devices can be found in the mobile device usage section of these guidelines.

Further information on using Bluetooth to communicate sensitive or classified data can be found in the wireless devices and Radio Frequency transmitters section of the ***Guidelines for Physical Security***.

Further information on the use of encryption to reduce storage and physical transfer requirements is detailed in the cryptographic fundamentals section of the ***Guidelines for Cryptography***.

Further information on ACSC approved platforms can be found on the ***Evaluated Products List*** at https://www.cyber.gov.au/acsc/view-all-content/epl-products.

Further information on allowing the use of privately-owned devices by personnel to access their organisation's systems and data can be found in the ACSC's ***Bring Your Own Device for Executives*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/bring-your-own-device-executives.

Further information and specific guidance on enterprise mobility can be found in the ACSC's ***Risk Management of Enterprise Mobility Including Bring Your Own Device (BYOD)*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/risk-management-enterprise-mobility-including-bring-your-own-device.

Further information on securely configuring mobile devices can be found in the following ACSC publications:

- ***Security Configuration Guide – Apple iOS 14 Devices*** at https://www.cyber.gov.au/acsc/view-all-content/publications/security-configuration-guide-apple-ios-14-devices
- ***Security Configuration Guide – Samsung Galaxy S10, S20 and Note 20 Devices*** at https://www.cyber.gov.au/acsc/view-all-content/publications/security-configuration-guide-samsung-galaxy-s10-s20-and-note-20-devices
- ***Security Configuration Guide – Viasat Mobile Dynamic Defense*** at https://www.cyber.gov.au/acsc/view-all-content/publications/security-configuration-guide-viasat-mobile-dynamic-defense.

Further information on configuring personal mobile devices can be found in the ACSC's ***Security Tips for Personal Devices*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/security-tips-personal-devices.

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***, at https://csrc.nist.gov/publications/detail/sp/800-121/rev-2/final.

Mobile device usage

Mobile device usage policy

Since mobile devices routinely leave the office environment, and the protection it affords, it is important that organisations develop a mobile device usage policy governing their use.

Security Control: 1082; Revision: 2; Updated: Aug-19; Applicability: O, P, S, TS
A mobile device usage policy is developed and implemented.

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.

Security Control: 1083; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Personnel are advised of the sensitivity or classification permitted for voice and data communications when using mobile devices.

Paging and message services

As paging and message services do not appropriately encrypt data they cannot be relied upon for the communication of sensitive or classified data.

Security Control: 0240; Revision: 6; Updated: Jun-21; Applicability: O, P, S, TS
Paging, Multimedia Message Service, Short Message Service or instant messaging apps are not used to communicate sensitive or classified data.

Using mobile devices in public spaces

Personnel should be aware of the environment they use mobile devices in to view or communicate sensitive or classified data, especially in public areas such as public transport, transit lounges and coffee shops. In such locations, personnel should take care to ensure that sensitive or classified data is not observed by other parties. 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.

Security Control: 0866; Revision: 5; Updated: Jun-21; Applicability: O, P, S, TS
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.

Security Control: 1145; Revision: 3; Updated: Sep-18; Applicability: S, TS
Privacy filters are applied to the screens of highly classified mobile devices.

Security Control: 1644; Revision: 0; Updated: Jun-21; Applicability: O, P, S, TS
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 do not leave mobile devices unattended when being actively used.

Security Control: 0871; Revision: 3; Updated: Apr-19; Applicability: O, P, S, TS
Mobile devices are kept under continual direct supervision when being actively used.

Security Control: 0870; Revision: 3; Updated: Apr-19; Applicability: O, P, S, TS
Mobile devices are carried or stored in a secured state when not being actively used.

Carrying mobile devices

As mobile devices used outside the office will be carried through areas not authorised to process the data stored on them, carrying them in a secured state (i.e. encryption is active when they are not in use) will decrease the likelihood of accidental or deliberate compromise of data. Depending on the type of mobile device, the effectiveness of encrypting

its internal storage might be reduced if the device is lost or stolen while it is in sleep mode or powered on with a locked screen.

Security Control: 1084; Revision: 3; Updated: Jun-21; Applicability: O, P, S, TS
If unable to apply encryption to mobile devices that is suitable for them to be carried through areas not authorised to process the data stored on them, they are physically transferred in a security briefcase or an approved multi-use satchel, pouch or transit bag.

Mobile device emergency sanitisation process and procedures

The sanitisation of mobile devices in emergency situations can assist in reducing the potential for compromise of data by an adversary. This may be achieved through the use of a remote wipe capability or a cryptographic key zeroise or sanitisation function if present.

Security Control: 0701; Revision: 4; Updated: Aug-19; Applicability: O, P, S, TS
A mobile device emergency sanitisation process, and supporting mobile device emergency sanitisation procedures, is developed and implemented.

Security Control: 0702; Revision: 4; Updated: Aug-19; Applicability: S, TS
If a cryptographic zeroise or sanitise function is provided for cryptographic keys on highly classified mobile devices, the function is used as part of the mobile device emergency sanitisation process.

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/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.

Security Control: 1298; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
Personnel are advised of privacy and security risks when travelling overseas with mobile devices.

Security Control: 1554; Revision: 0; Updated: Oct-19; Applicability: O, P, S, TS
If travelling overseas with mobile devices to high/extreme risk countries, personnel are:

- *issued with newly provisioned accounts and devices 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 devices*
- *advised to avoid taking any personal devices, especially if rooted or jailbroken.*

Security Control: 1555; Revision: 0; Updated: Oct-19; Applicability: O, P, S, TS
Before travelling overseas with mobile devices, personnel take the following actions:

- *record all details of the devices being taken, such as product types, serial numbers and International Mobile Equipment Identity numbers*
- *update all applications and operating systems*
- *remove all non-essential accounts, applications and data*
- *apply security configuration settings, such as lock screens*
- *configure remote locate and wipe functionality*
- *enable encryption, including for any media used*
- *backup all important data and configuration settings.*

While travelling overseas with mobile devices

Personnel lose control of mobile devices and media any time they are not on their person. This includes when placing mobile devices and media in checked-in luggage or leaving them in hotel rooms (including hotel room safes). In addition, allowing untrusted people to access mobile devices provides an opportunity for them to be tampered with.

Security Control: 1299; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
Personnel take the following precautions when travelling overseas with mobile devices:

- *never leaving devices or media unattended for any period of time, including by placing them in checked-in luggage or leaving them in hotel safes*
- *never storing credentials with devices that they grant access to, such as in laptop bags*
- *never lending devices to untrusted people, even if briefly*
- *never allowing untrusted people to connect other devices or media to their devices, including for charging*
- *never using designated charging stations, wall outlet charging ports or chargers supplied by untrusted people*
- *avoiding connecting devices to open or untrusted Wi-Fi networks*
- *using an approved Virtual Private Network to encrypt all device communications*
- *using encrypted mobile applications for communications instead of using foreign telecommunication networks*
- *disabling any communications capabilities of devices when not in use, such as cellular data, wireless, Bluetooth and Near Field Communication*
- *avoiding reuse of media once used with other parties' devices or systems*
- *ensuring any media used for data transfers are thoroughly checked for malicious code beforehand*
- *never using any gifted devices, especially media, when travelling or upon returning from travelling.*

Security Control: 1088; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
Personnel report the potential compromise of mobile devices, media or credentials to their organisation as soon as possible, especially if they:

- *provide credentials, decrypt devices or have devices taken out of sight by foreign government officials*
- *have devices or media stolen that are later returned*
- *lose devices or media that are later found*
- *observe unusual behaviour of devices.*

After travelling overseas with mobile devices

Following overseas travel with mobile devices, personnel should take appropriate precautions to ensure that their devices don't pose an undue security risk to their organisation's systems and data. In most cases, sanitising and resetting mobile devices, including all media used with them, will be sufficient; however, upon returning from high/extreme risk countries, additional precautions will likely be needed.

Security Control: 1300; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
Upon returning from travelling overseas with mobile devices, personnel take the following actions:

- *sanitise and reset devices, including all media used with them*
- *decommission any physical credentials that left their possession during their travel*
- *report if significant doubt exists as to the integrity of any devices following their travel.*

Security Control: 1556; Revision: 0; Updated: Oct-19; Applicability: O, P, S, TS
If returning from travelling overseas with mobile devices to high/extreme risk countries, personnel take the following additional actions:

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

Further information

Further information on the management of mobile devices can be found in the mobile device management section of these guidelines.

Further information on using mobile devices in highly classified areas can be found in the wireless devices and Radio Frequency transmitters section of the ***Guidelines for Physical Security***.

Further information on travelling overseas with mobile devices can be found in the ACSC's ***Travelling Overseas with Electronic Devices*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/travelling-overseas-electronic-devices.

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

Further information on approved multi-use satchels, pouches and transit bags can be found in the Security Construction and Equipment Committee's ***Security Equipment Evaluated Products List*** at https://www.scec.gov.au/catalogue.