Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

SEPTEMBER 2019

Guidelines for Enterprise Mobility

Mobile device management

Types of mobile devices

These guidelines describe the use of mobile devices including mobile phones, smartphones, tablets, laptops, portable electronic devices and other portable internet-connected devices.

Device-specific guidance

To complement the security controls in this document, the Australian Cyber Security Centre (ACSC) publishes device-specific guidance. Where device-specific guidance exists, it should be consulted in conjunction with the security controls in this document.

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; Priority: Must
A mobile device management policy is developed and implemented.

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

Security Control: 0687; Revision: 5; Updated: Sep-18; Applicability: TS; Priority: Must
Mobile devices do not process, store or communicate TOP SECRET information unless explicitly approved by the ACSC to do so.

Privately-owned mobile devices

If organisations choose to allow personnel to use their personal mobile devices to access their organisation's systems and information, they should ensure that the devices do not present an unacceptable security risk. 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 and other hardening guidance available from the ACSC.

Security Control: 1400; Revision: 2; Updated: Aug-19; Applicability: O, P; Priority: Must

Personnel accessing official or classified information using a privately-owned mobile device use an ACSC approved platform, a security configuration in accordance with ACSC hardening guidance, and have enforced separation of official and classified information from any personal information.

Security Control: 0694; Revision: 4; Updated: Sep-18; Applicability: S, TS; Priority: Must
Privately-owned mobile devices do not access highly classified systems.

Seeking legal advice for privately-owned mobile devices

Allowing privately-owned mobile devices to access an organisation's systems and information 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: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Prior to allowing privately-owned mobile devices to connect to an organisation's systems, legal advice is sought.

Organisation-owned mobile devices

If organisations choose to issue personnel with mobile devices to access their organisation's systems and information, they should ensure that the devices do not present an unacceptable security risk. 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 and other hardening guidance available from the ACSC.

Security Control: 1482; Revision: 1; Updated: Aug-19; Applicability: O, P, S, TS; Priority: Must
Personnel accessing official or classified information using an organisation-owned mobile device use an ACSC approved platform with a security configuration in accordance with ACSC hardening 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 information stored on the device.

Security Control: 0869; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
All information on mobile devices is encrypted using at least an Australian Signals Directorate Approved Cryptographic Algorithm (AACA).

Mobile device communications encryption

If appropriate encryption is not available, mobile devices communicating sensitive or classified information present a security risk to such information. Encrypting communications, regardless of the protocol used (e.g. Bluetooth, infrared, Wi-Fi, 3G/4G/5G or other wireless protocols) is the only way to have any assurances that the information is protected.

Security Control: 1085; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Mobile devices used to communicate sensitive or classified information over public network infrastructure use encryption approved for communicating such information over public network infrastructure.

Mobile device Bluetooth functionality

Bluetooth provides inadequate security for information 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; Priority: Should
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; Priority: Must
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 information 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; Priority: Must
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; Priority: Must
Bluetooth pairing is performed using Bluetooth version 2.1 or later.

Security Control: 1198; Revision: 1; Updated: Sep-18; Applicability: O, P; Priority: Must
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; Priority: Should
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; Priority: Should
Mobile devices prevent personnel from installing or uninstalling applications once provisioned.

Security Control: 0864; Revision: 3; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Must
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; Priority: Should
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; Priority: Should
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 hardening 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; Priority: Should
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; Priority: Must
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 information 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 Using Cryptography***.

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/publications/risk-management-of-enterprise-mobility-including-bring-your-own-device.

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; Priority: Must
A mobile device usage policy is developed and implemented.

Personnel awareness

Mobile devices can have both a voice and data component capable of processing or communicating information. In such cases, personnel should know the sensitivity or classification of information that mobile devices have been approved to process, store and communicate.

Security Control: 1083; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
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 information they cannot be relied upon for the communication of sensitive or classified information.

Security Control: 0240; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Paging, Multimedia Message Service, Short Message Service or instant messaging apps are not used to communicate sensitive or classified information.

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 information, especially in public areas such as public transport, transit lounges and coffee shops. In such locations personnel taking care to ensure information is not observed or conversations are overheard will assist in maintaining the confidentiality of their organisation's information. In some cases, privacy filters can be applied to the screen of a mobile device to prevent onlookers from reading content off its screen.

Security Control: 0866; Revision: 4; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Must
Sensitive or classified information is not viewed or communicated in public locations unless care is taken to reduce the chance of conversations being overheard or the screen of a mobile device being observed.

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

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; Priority: Must
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; Priority: Must
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 information 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 information. 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: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
If unable to apply encryption to mobile devices that is suitable for them to be carried through areas not authorised to process the information 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 information 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; Priority: Must

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; Priority: Must
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. Taking steps to mitigate these security risks will assist in protecting their organisation's information. When personnel leave Australian borders they also leave behind any expectations of privacy.

Prior to the departure of personnel travelling overseas with mobile devices, organisations can:

- patch applications and operating systems
- implement multi-factor authentication
- backup all data
- remove all non-essential data
- disable applications that are not essential for the period of travel
- disable Bluetooth and wireless connectivity
- configure wireless to connect only to known secure networks.

Security Control: 1298; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
User education and the implementation of security controls are conducted prior to personnel travelling overseas with mobile devices.

While travelling overseas with mobile devices

Personnel lose control of information stored on mobile devices any time devices are not on their person. This includes storing mobile devices in checked-in luggage or in hotel rooms (including hotel room safes). Such situations provide an opportunity for mobile devices to be stolen or tampered with.

Security Control: 1087; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
When travelling overseas with mobile devices and media, personnel retain control over them at all times, this includes by not placing them in checked-in luggage or leaving them unattended for any period of time.

Security Control: 1299; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Personnel take the following precautions when travelling overseas with mobile devices:

- *avoiding storing authentication details or tokens and passphrases with mobile devices*
- *avoiding connecting to open Wi-Fi networks*
- *clearing web browsers after each browsing session including history, cache, cookies and temporary files*
- *encrypting emails where possible*
- *ensuring login pages are encrypted before entering passphrases*
- *avoiding connecting to untrusted computers or inserting removable media.*

Security Control: 1088; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
If personnel are requested to decrypt mobile devices for inspection by customs personnel, or their devices leave their possession at any time, they report the potential compromise of information to their organisation as soon as possible.

After travelling overseas with mobile devices

Inspecting mobile devices after overseas travel allows organisations to check for evidence that devices may have been compromised, and if so, take appropriate actions such as resetting devices and all passphrases for accounts associated with the devices.

Security Control: 1300; Revision: 3; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Should
If upon returning from overseas mobile devices are suspected of being compromised, the devices and all passphrases for accounts associated with the devices are reset.

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/publications/travelling-overseas-with-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 govdex 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.