ACSC Guidelines for Enterprise Mobility

"The Australian Cyber Security Centre (ACSC) produces the *Information Security Manual* (ISM). The purpose of the ISM is to outline a cyber security framework that organisations can apply, using their risk management framework, to protect their systems and data from cyber threats. The ISM is intended for Chief Information Security Officers, Chief Information Officers, cyber security professionals and information technology

These guidelines below describe the use and protection of mobile devices, such as smartphones, tablets and laptops.

https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-enterprise-mobility

Control #	Control category	Organisational control	Relevance to Telecoms and mobile ICT
ISM-1533	Mobile device management policy	*A mobile device management policy is developed, implemented and maintained.*	There are quite a few policy requirements - this is just one. TL;DR: organisations need a detailed poloicy for all aspects of mobile device management *AND* usage, and it needs to tie in with their HR policies too.
ISM-1195	Mobile device management policy	*A Mobile Device Management solution is used to ensure mobile device management policy is applied to all mobile devices.*	MDM or UEM is required, and must be maintained.
ISM-0687	ASD-approved platforms	*Mobile devices do not process, store or communicate SECRET or TOP SECRET data until approved for use by ASD.*	Management system that can apply differrent restrictions to any legacy non-ASD-approved devices compared to ASD-approved devices.
ISM-1482	Organisation-owned mobile devices	*Personnel accessing systems or data using an organisation-owned mobile device use an ASD-approved platform, a security configuration in accordance with ACSC guidance, and have enforced separation of work and personal data.*	Procurement platform would need to support product catalogues so that device choices can be restricted to ASD-approved devices for those departments/units where necessary. Containerisation required too.
ISM-0869	Storage encryption	*Mobile devices encrypt their internal storage and any removable media.*	Mobile encryption - A device's internal storage becomes encrypted once the user enables a passcode on the device
ISM-1085	Communications encryption	*Mobile devices encrypt all sensitive or classified data communicated over public network infrastructure.*	iOS, iPadOS, and macOS support Transport Layer Security (TLS 1.0, TLS 1.1, TLS 1.2,TLS 1.3) and Datagram Transport Layer Security (DTLS). The TLS protocol supports both AES128 and AES256, and prefers cipher suites with forward secrecy. Internet apps such as Safari, Calendar, and Mail automatically use this protocol to enable an encrypted communication channel between the device and network services App Transport Security provides default connection requirements so that apps adhere to best practices for secure connections when using NSURLConnection, CFURL, or NSURLSession APIs. App Transport Security is automatically applied to apps that are compiled for iOS 9 or later and macOS 10.11 or later. https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf Android has an equivalent approach, although different. In all cases, a key requirement is that all devices are always using the latest released OS version and update, and this requires enforcement via a management system.
ISM-1196	Bluetooth functionality	*OFFICIAL and PROTECTED mobile devices are configured to remain undiscoverable to other Bluetooth devices except during Bluetooth pairing.*	Management system that can control bluetooth permissions and use
ISM-1200	Bluetooth functionality	*Bluetooth pairing for OFFICIAL and PROTECTED mobile devices is performed using Secure Connections, preferably with Numeric Comparison if supported.*	Management system that can control bluetooth permissions and use
ISM-1198	Bluetooth functionality	*Bluetooth pairing for OFFICIAL and PROTECTED mobile devices is performed in a manner such that connections are only made between intended Bluetooth devices.*	Management system that can control bluetooth permissions and use
ISM-1199	Bluetooth functionality	*Bluetooth pairings for OFFICIAL and PROTECTED mobile devices are removed when there is no longer a requirement for their use.*	Management system that can control bluetooth permissions and use
ISM-0682	Bluetooth functionality	*Bluetooth functionality is not enabled on SECRET and TOP SECRET mobile devices.*	Would require a system capable of enforcing different usage restrictions on different devices
ISM-0863	Maintaining mobile device security	*Mobile devices prevent personnel from installing or uninstalling non-approved applications once provisioned.*	Management system that can limit/block side-loading
ISM-0864	Maintaining mobile device security	*Mobile devices prevent personnel from disabling or modifying security functionality once provisioned.*	Management system that can lock settings

ISM-1366	Maintaining mobile device security	*Security updates are applied to mobile devices as soon as they become available.*	Management system that can automatically push updates
ISM-0874	Connecting mobile devices to the internet	*Mobile devices access the internet via a VPN connection to an organisation's internet gateway rather than via a direct connection to the internet.*	This requires a data connection setting to the VPN, as well as device controls preventing the user from changing the setting or establishing any other data connection.
ISM-0705	Connecting mobile devices to the internet	*When accessing an organisation's network via a VPN connection, split tunnelling is disabled.*	This requires a VPN-control capability such that when a corporate VPN is active, all other comms channels to/from the device (such as app-specific tunnelling, for example) are forced down the corporate VPN.
ISM-1400	Privately-owned mobile devices	*Personnel accessing OFFICIAL and PROTECTED systems or data using a privately-owned mobile device use an ASD-approved platform, a security configuration in accordance with ACSC guidance, and have enforced separation of work and personal data.*	Containerisation is required to achieve this.
ISM-0694	Privately-owned mobile devices	*Privately-owned mobile devices do not access SECRET and TOP SECRET systems or data.*	Requires a system capable of enforcing different usage restrictions on BYOD devices versus organisation-owned devices
ISM-1145	Using mobile devices in public places	*Privacy filters are applied to the screens of SECRET and TOP SECRET mobile devices.*	Kitting capability required.

END OF DOCUMENT