Government of South Australia

SACSF Mobile Device Security Standard

SACSF/S19.1

Across Government Standard

Purpose

The Mobile Device Security Standard aims to help safeguard South Australia (SA) Government's information resources accessed on mobile devices. It establishes minimum security requirements for mobile devices, thereby protecting sensitive information, and reducing risks associated with the use of mobile devices, leading to enhanced security, efficiency, and reliability in government operations.

Scope

This standard applies to South Australian public sector agencies (as defined in section 3(1) of the *Public Sector Act 2009*) and to any other person or organisation that is generally subject to the direction of a Minister of the Crown; all of which are referred to in this standard as "Agencies".

The standard supports the following policy statement from the South Australian Cyber Security Framework (SACSF):

- *SACSF Policy Statement 2.10: Mobile Device Management and Remote Working* – Technical and procedural controls must be in place to address the risks associated with the use of mobile devices including smartphones, tablets, laptops, portable electronic devices, portable storage and other portable internet-connected devices. Additionally, secure practices for remote working must be established and understood by agency employees, with technical controls implemented to enable secure remote access to agency information.

The requirements in this standard apply to all South Australian Government public sector agencies, including:

- Agency owned and issued (corporate) mobile phones and tablets including iOS, Android and Windows OS devices.
- Personally owned mobile devices used by employees to access agency information assets. This includes but is not limited to personally owned mobile phones, tablets, and laptop computers.

Standard detail

Background

Agencies increasingly rely on mobile devices to enhance productivity and streamline operations. However, the use of mobile devices to access agency information assets introduces significant security risks, including data breaches, unauthorised access, and cyberattacks. Securing mobile devices safeguards sensitive information, supports alignment with compliance and regulatory requirements, and preserves the integrity of government operations.

Mobile Application Management (MAM) and Mobile Device Management (MDM) are key systems used for securing mobile access to agency information.

- MAM controls application usage and data security within applications. It reduces risk associated with unmanaged devices by protecting data at the application level, reducing vulnerabilities and risk associated with data leaks and unauthorised access.
- MDM focuses on managing device settings, enforcing security policies, and enabling remote actions. It reduces risks associated with unmanaged devices by ensuring that the device is secure.

Agencies should assess the risks linked to mobile devices and identify the required level of control before determining if MAM, or a combination of or MAM and MDM, is more appropriate for their operations. If only MDM is used, then it must be in conjunction with access control for applications with access to agency information.

The SACSF Tier Two requirement that agencies must implement a mobile device management solution refers to the use of either a MAM and/or MDM solution.

Standard Format

This document provides requirements in a format which can be used to develop the potential solution options to deliver on those requirements. The MoSCoW method is a prioritisation technique used in management, business analysis, project management, and software development to reach a common understanding with stakeholders on the importance they place on the delivery of each requirement. The categories are:

- "**Must**" - Requirements labelled as Must are mandatory for the compliance of this standard.
- "**Should**" Requirements labelled as Should are important but there may exist compensating security controls to justify not implementing the requirement, or the associated security risks are accepted based on Agency's defined risk appetite and management decisions.
- "**Could**" requirements labelled as Could are desirable but not necessary and could improve the user experience.
- "**Won't**" requirements labelled as Won't, have been agreed by stakeholders as the least-critical, lowest-payback items, or not appropriate at that time.

Standard requirements

The below standard requirements are to be implemented for mobile devices accessing agency information assets.

The standard is divided into requirements for SACSF Tier One agencies that apply to all agencies, and requirements for SACSF Tier Two, Three and Four agencies. For information on which Tier applies to your agency, contact your IT Security Adviser.

Requirements for Tier One agencies and above (all agencies):

Device Compliance and Security Baseline	
Must	• Authority for the use of personal mobile devices to access agency information assets must be formally approved and documented, such as in agency security policy.
Should	• Restrict agency information asset access to a set of approved applications as determined by the agency.

Secure Access and Authentication	
Must	• Mobile devices accessing agency information assets must utilise secure authentication methods, including strong PINs and passwords in line with the agency's password policy. • Deploy Multi-Factor Authentication (MFA), focusing on phishing-resistant MFA, to access agency information assets such as Microsoft 365 applications.
Should	• Biometric authentication mechanisms such as fingerprint or face recognition should be implemented on mobile devices accessing agency information assets.
Could	• Require the use of a Virtual Private Network (VPN) for secure communication and access to corporate networks from mobile devices.

Information Security	
Must	• Encryption of storage is enabled on all laptops and mobile devices to reduce the risk of unauthorised information disclosure. • Where security classified information is accessed on mobile devices, relevant security controls in line with the requirements of the South Australian Protective Security Framework (SAPSF) must be implemented. ○ *Currently information classified as PROTECTED, SECRET, and TOP SECRET is considered classified under the SAPSF.*
Should	• Implement controls to prevent backing up agency information to unauthorised cloud or backup services. • Require agency information on mobile devices to be wiped when the user is terminated.

User Engagement	
Must	• Require staff to report lost or stolen agency managed mobile devices as soon as possible, or at most within 24 hours to enable timely action and mitigate data breaches.
Should	• Provide regular training to users on mobile device security best practices and the importance of adhering to agency security policies.

Requirements for Tier Two, Three and Four agencies:

Device Compliance and Security Baseline	
Must	• User mobile devices must have the agency's Mobile Application Management (MAM) system applied. • Establish policies to monitor compliance with device posture, emphasising adherence to specified minimum Operating System (OS) and application versions to address vulnerabilities. • Restrict agency information asset access to a set of approved applications as determined by the agency. Regularly review these applications and their approved versions for security compliance.
Should	• Restrict access to agency information assets from devices that are not protected by the agency's MAM system.
Could	• Establish regular health checks for mobile devices to identify vulnerabilities and maintain mobile device security standards. • Enforce that all mobile applications and operating systems containing or authenticating work data receive regular security patches and updates to mitigate vulnerabilities.

Information Security	
Must	• All mobile devices accessing agency information assets must encrypt application data to reduce the risk of unauthorised information disclosure. • Enable remote wipe functionality to erase agency information from devices if they are lost, stolen, or compromised. • Measures must be established to prevent copying and pasting of agency information outside of the managed applications, maintaining data security and keeping sensitive information within controlled environments/applications. • Policies are enforced prohibiting users from taking screenshots or printing agency information from mobile devices. • Controls must be implemented to prevent backing up agency information to unauthorised cloud or backup services. • Require the agency information on the mobile device to be wiped when the user is terminated.
Could	• Access to agency information on mobile devices is revoked after a device has been offline for a pre-defined period of time.

Implementation advice

It is recommended that the following process is followed for implementation of the above standard requirements.

- **Determine if MAM or a combination of MAM and MDM is most appropriate:** MAM should be used as an initial step to meet the baseline security requirements to protect agency information accessed on mobile devices. MAM restricts access to agency information to only agency approved applications, and applies security controls to those approved applications such as requiring authentication, encryption of information, and the ability to remote wipe. MAM can be configured with no-touch of the devices by the agency, and minimum effort from users. It also maintains the privacy of staff by separating their personal applications and data from work so that the agency only has control over the information in the work apps (for example, so the agency cannot wipe staff members personal photos).

  MDM provides more control over the security of devices, but is likely to be less palatable to staff using personal phones to access agency information as it typically gives full control over the device to the agency. MDM should be considered for agency-owned devices, and where there may be highly sensitive information being accessed that requires a higher level of control and protection. It may also be considered where work apps that cannot be managed by the MAM solution are required and must be maintained by the agency.
- **Phased implementation:** Initiate a pilot program for MAM/MDM with select teams and/or users to identify potential issues and refine procedures, then gradually expand the rollout across the agency to reduce operational disruption. Agencies can use the guidance documents prepared by the Office of the Chief Information Officer (OCIO) to prepare an action plan for MAM/MDM roll out available at Microsoft Intune Service Catalogue.
- **Provide transparency on the controls enforced:** Clearly communicate the scope of MAM/MDM systems, outlining their abilities to enforce security policies, manage app installations, and perform remote wipes while emphasising restrictions on accessing personal data, such as photos or private messages, to reassure users about privacy and control over personal content. It is important to inform staff about what personal information the system may be able to access (if any) and what can be remotely wiped on the mobile device.
- **Exemption criteria and processes:** Establish clear criteria for exemptions, requiring detailed justification and approval through a formal process involving ITSA and relevant agency leadership to ensure only necessary exemptions are granted. Where the requirements can't be implemented for a group of users and/or team, a formal exemption should be obtained.
- **Maintain a centralised exemption register:** Develop a system to log all exemptions. Include details such as user identity, reason for exemption, approval authority, and expiration dates.
- **Microsoft Intune baseline:** The requirements of this standard are technology agnostic and can be applied using a range of different mobile device security solutions. However, agencies within the M365 central tenancy can access the whole of government Microsoft Intune MAM and MDM system within the M365 central tenancy that has the recommended baseline security configuration for mobile devices. Agencies can opt-in to the Intune MAM or MDM services which enforces the baseline requirements on their mobile devices. However, a risk-based assessment should be performed by the agencies to assess if this baseline is adequate for their operations or more stringent security requirements need to be enforced.

Policy Exemption

Where an entire agency cannot implement the above **Must** requirements, an exemption must be obtained following the process linked below.

- Exemption | Department of Treasury and Finance

Exempting limited groups of users from agency's MAM enrolment must be done after assessing the associated risks and after seeking an approval from the agency's ITSA and appropriate leadership. This does not require an exemption from OCIO.

Aboriginal Impact Statement

The needs and interests of Aboriginal people have been considered in the development of this standard. There is no specific impact on Aboriginal people.

Roles and responsibilities

Position title or unit/team	Listed responsibilities
Chief Executive	Accountable for the effective implementation of, and compliance, with this standard within their agency.
Senior Executives, Directors and Managers	Responsible for ensuring • the standard is implemented and observed by staff • staff are fully informed of their obligations and responsibilities under the standard, and trained where required • any reporting requirements are met.
IT Security Advisors	Responsible for providing advice on the appropriate implementation of this standard to reduce identified cyber security risks.
Team leaders and supervisors	Responsible for ensuring that the standard is observed by staff and that business processes support the standard requirements.
All staff	Required to comply with the standard and any related procedures, and to play an active role in ensuring the compliance of others.

Related Documents

- Email Usage Policy
- Exemption | Department of Treasury and Finance
- South Australian Cyber Security Framework
- South Australian Protective Security Framework

Definitions

Term	Definition
Information assets	Any information or asset supporting the use of the information that has value to the agency, such as collections of data, processes, ICT, people and physical documents.
Mobile Application Management (MAM)	Software and services that control access to mobile applications used in business settings, managing their lifecycle without necessarily managing the entire device.
Mobile device	Mobile phones, smartphones, tablets, laptops, portable electronic devices, portable storage, and other portable internet-connected devices.
Mobile Device Management (MDM)	Software used to monitor, manage, and secure employees' mobile devices.
Virtual Private Network (VPN)	A network that maintains privacy through a tunnelling protocol and security procedures. Virtual Private Networks may use encryption to protect network traffic.

Document Control

Approved by	CIO Steering Committee	Version	FINAL V1.0
Approved date	8 July 2026	Next review date	8 July 2027
Original date of approval	8 July 2026	Compliance	Mandatory
Contact person	Office of the Chief Information Officer		
Contact email	cybersecurity@sa.gov.au		