



ACSC for Mobile Maturity Model

Version 1.4



Mobile Maturity Model

The Mobile Maturity Model was developed to create a bridge between the ACSC's current guidance for mobile, and what is available for Windows endpoints within the Essential 8 Framework. This model is impartial and purely focuses on controls provided by the ACSC.

Although based on the ACSC's mobile security controls, this Maturity Model **does not** replace the other advice provided by the ACSC. It must be used in conjunction with the other configuration guides, publications and mobility documentation.

How we developed the Maturity Model

These security controls were extracted from the Guidelines for Enterprise Mobility guide, then categorised into 5 consolidated topics and 3 levels of maturity. The maturity levels were specifically based on a least-restrictive to most-restrictive methodology.

The levels also considered the difference between security control types, such as organisational-based policies (E.g. Devices should be encrypted), versus security controls that are platform-based (E.g. MDM Payload to force-enable encryption). These controls were ordered in the same manner, with organisational-based policies relating to lower levels of maturity, and platform or physical relating to higher levels of maturity.

How to use the Mobile Maturity Model

The levels of maturity for each topic are cumulative. For organisations wanting to meet the highest level of maturity, they must first meet all the requirements within each previous level(s). Organisations also do not need to meet level 3 maturity of a specific topic before starting, or meeting level 3 in a different topic.

Resolving conflicts between ACSC documentation

Since there are a range of mobility documents available from the ACSC, you may find guidance that contradicts or overrides the security controls below. Here is the general guide on how to deal with these exceptions or contradictions:

- If different or conflicting guidance exists in an ACSC Configuration Guide, the Configuration Guide should take precedence over the relevant Security Controls within the Mobile Maturity Model.
- If guidance only exists in a Configuration Guide, but not as a Security Control within the Maturity Model, it should be included part of the organisations Level 1 maturity requirements. This will in effect require organisations to implement all relevant Configuration Guide guidance, to achieve level 1 Maturity.
- Have the expectation that there are conflicts, and ensure you thoroughly read the configuration guides to identify any conflicts that are relevant to your organisation. Later versions of this publication plan to identify and assess these conflicts.

How sensitive is your data?

A common theme among the ACSC's mobile guidance is reference to Classifications, such as [OFFICIAL: Sensitive] and [PROTECTED]. Although these relate to data sensitivity in a governmental setting, they serve as a good benchmark for private organisations to assess what security standards they should aim to meet.

If you are a private organisation, it may be helpful to first align your organisations data types to the classification framework, before continuing to the next stages of the document. Below are some examples of how a private organisation might align their data to the Classifications framework:

Risk Acceptance at different classifications

Overall, it is important to understand this framework as the ACSC believes only certain data sets should be processed on Mobile endpoints. Even though certain government organisations can circumvent recommendations via a risk-based approach, they are still required to complete a risk assessment – with their Authorising Officer formally accepting all residual risks. Finally, a risk-assessment can only replace guidance up to Protected, as government departments do not own the risk of Secret and Top Secret Data.

Secret and Top Secret Data

Additionally, it is good to note that there are only a few public references to handling highly classified or sensitive data – referred to as [SECRET] and [TOP SECRET] in the classification framework. This is not because there is a lack of guidance, it is due to those controls only being available to individuals under “Governmental Brief”. Finally, those individuals must also have relevant Security Clearances and a “need to know”.

Example of classifying data in a Public Company

Government definition of Impact from lost Data		Example Private Data
Unofficial	No damage. This information does not form part of official duty.	Public Presentations, eBooks or public product collateral.
Official: Sensitive	Limited damage to an individual, organisation or government generally if compromised.	Employee communications, internal announcements.
Protected	Damage to the national interest, organisations or individuals.	Commercial in Confidence, Quotes or Personally Identifiable Information.
Secret	Serious damage to the national interest, organisations or individuals.	Customers Sensitive Data, Competitive Information.
Top Secret	Exceptionally grave damage to the national interest, organisations or individuals.	Intellectual property or patents, acquisition or financial information.

Ivanti Maturity Levels

	Level 1	Level 2	Level 3
Device Management Policy	<p>A Device Management Policy has been developed (Security Control: 1533).</p> <p>The policy should include the following controls at a minimum for all supported device types, regardless of ownership (E.g. Corporate/BYOD):</p> <ul style="list-style-type: none"> ■ Device Storage Encryption (Security Control: 0869). ■ Sensitive or classified information sent over public networks is encrypted (Security control: 1085). ■ A mobile device emergency sanitisation process, and supporting emergency sanitisation procedures, is developed and implemented (Security Control: 0701). ■ After foreign travel, device are sanitised and reset, including all media used with them (Part of Security Controls: 1300). ■ Never use any gifted devices, especially media, when travelling or upon returning from travelling (Part of Security Controls: 1299). 	<p>The Policy is enforced through a Mobile Device Management solution (Security Control: 1195).</p> <p>Additional Controls at a minimum:</p> <ul style="list-style-type: none"> ■ Prevent installation/uninstallation of apps once provisioned (Security Controls: 0863). ■ Prevent disabling or modifying security functions (Security Controls: 0864). ■ Bluetooth range should be 10m or less and is managed according to standards (Security Controls: 1196, 1198, 1199, 1200, 1202). ■ 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 (Security Control: 0702). 	<p>It is ensured Mobile devices do not process, store or communicate TOP SECRET data unless explicitly approved by the ACSC to do so (Security Control: 0687). It is also ensured personally owned devices do not access highly classified systems or data (Security Control: 0694).</p> <p>Additional controls at a minimum:</p> <ul style="list-style-type: none"> ■ Web browsing from mobile devices is conducted through an organisation's internet gateway rather than via a direct connection to the internet (Security Control: 0874). ■ When accessing an organisation system via a VPN connection, split tunnelling is disabled (Security Control: 0705).
	<p>Security Controls: 0701, 0869, 1085, 1299, 1533.</p>	<p>Security Controls: 0702, 0863, 0864, 1195, 1196, 1198, 1199, 1200, 1202.</p>	<p>Security Controls: 0687, 0694, 0705, 0874.</p>

Ivanti Maturity Levels

	Level 1	Level 2	Level 3
Device Usage Policy	<p>A mobile device usage policy is developed and implemented (Security Control: 1082).</p> <p>The policy discusses the following controls at a minimum:</p> <ul style="list-style-type: none"> ■ Personnel are advised of the sensitivity or classification permitted for voice and data communications (Security Controls: 1083). ■ Advised of privacy and security risks when travelling overseas (Security Control: 1298). ■ Sensitive or classified data is not viewed or communicated in public unless care is taken to reduce chance of screen being observed (Security Control: 0866). ■ Sensitive or classified phone calls are not conducted in public unless care is taken to reduce chance of eavesdropping (Security Control: 1644). ■ Mobile devices are kept under continual direct supervision (Security Control 0871). 	<p>The policy discusses the following additional controls:</p> <ul style="list-style-type: none"> ■ Mobile carriers that are able to provide timely security updates for mobile devices are used (Security Control: 1365). ■ Mobile devices are carried or stored in a secured state when not being actively used (Security Control 0870). ■ 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 (Security Control: 1084). ■ Paging, Multimedia Message Service, Short Message Service or instant messaging apps are not used to communicate sensitive or classified data (Security Control: 0240). 	<p>Mobile devices are regularly tested to ensure that they meet organisation-defined security configurations and that patches are being applied.</p> <p>The policy discusses the following additional controls:</p> <ul style="list-style-type: none"> ■ Mobile devices are able to accept security updates from mobile carriers as soon as they become available (Security Control: 1366). <p>The following physical policy controls are also implemented:</p> <ul style="list-style-type: none"> ■ Privacy filters are applied to the screens of highly classified mobile devices (Security Control: 1145).
		<p>Security Controls: 0866, 0871, 1082, 1083, 1298, 1644.</p>	<p>Security Controls: 0240, 0870, 1084, 1365.</p>

Ivanti Maturity Levels

	Level 1	Level 2	Level 3
Privately-Owned Mobile Devices	<p>A risk assessment has been completed, to ensure the allowance of Personally owned devices to access organisations systems or data does not present an unacceptable risk.</p> <p>Legal advise was also sought prior to allowing privately-owned mobile devices to access official or classified systems or data (Security Control: 1297).</p>	<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: 1400).</p>	<p>The Security Configuration Guides were followed and implemented for all platforms in use, which may include Samsung and iOS devices.</p> <p>Close attention was paid to any controls relating to BYOD, especially regarding supervision, biometric usage and allowed levels of data.</p>
	<p>Refer to the “Risk Management of Enterprise Mobility Including Bring Your Own Device (BYOD)” publication for risk assessments.</p> <p>Security Control: 1297.</p>	<p>Security Control: 1400.</p> <p>For more on ACSC approved Platforms, see Data Processing by Device Type and ownership: Page 5.</p>	<p>See the iOS Guide & Samsung Guide. All Recommended and Required controls were implemented. Respectively, Not Permitted items were disallowed/disabled by MDM.</p>
Organisation-Owned Devices	<p>A risk assessment has been completed, to ensure that the devices do not present an unacceptable security risk.</p>	<p>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 (Security Control: 1482).</p>	<p>The Security Configuration Guides were followed and implemented for all platforms in use, which may include Samsung and iOS devices.</p>
	<p>Refer to the “Risk Management of Enterprise Mobility Including Bring Your Own Device (BYOD)” publication for risk assessments.</p>	<p>Security Control: 1482.</p>	<p>See the iOS Guide & Samsung Guide. All Recommended and Required controls were implemented. Respectively, Not Permitted items were disallowed/disabled by MDM.</p>

Ivanti Maturity Levels


	Level 1	Level 2	Level 3
Carrying & Travelling	<p>Personnel should also be aware that when they leave Australian borders they also leave behind any expectations of privacy.</p> <p>Controls for travelling to high/extreme risk countries (Security Control: 1554):</p> <ul style="list-style-type: none"> issued with newly provisioned accounts and devices from a pool of dedicated work travel devices advised on how to apply and inspect tamper seals advised to avoid taking any personal devices <p>Before travelling overseas (Security Controls: 1555):</p> <ul style="list-style-type: none"> record all details of the devices being taken, such as product types, serial numbers and IMEIs update all applications and operating systems remove all non-essential accounts, applications and data apply security configuration settings configure remote locate and wipe functionality enable encryption, including for any media used backup all important data and configuration settings. 	<p>Personnel take the following precautions when travelling overseas (Security Control: 1299):</p> <ul style="list-style-type: none"> never storing credentials with devices that they grant access to, never lending devices to untrusted people, 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 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 when not in use, such as cellular, wireless, Bluetooth and NFC 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 	<p>Upon returning from travelling overseas, personnel take the following actions (1300):</p> <ul style="list-style-type: none"> decommission any physical credentials that left possession. report if significant doubt exists as to the integrity of any devices. <p>Returning from high/extreme risk countries, the following additional actions are taken (Security Control: 1556):</p> <ul style="list-style-type: none"> 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. <p>Personnel report the potential compromise of mobile devices, media or credentials to their organisation as soon as possible, especially if they (1088):</p> <ul style="list-style-type: none"> provide credentials, decrypt devices or have devices taken out of sight by foreign government officials have devices/media stolen or lost, even if later returned or found observe unusual behaviour of devices.
		Security Controls: 1554, 1555.	Security Controls: 1299.

Additional Recommended Controls

	Level 1	Level 2	Level 3
Policies and Controls	<ul style="list-style-type: none"> ■ Unauthorised Paging, Multimedia Message Service, Short Message Service or instant messaging apps are blocked via the Device Management Solution (Ivanti Recommendation: 0001). ■ Devices that no longer have security or OS updates available should be replaced before support has ended (Ivanti Recommendation: 0002). ■ Disable Safeboot, recovery and other boot modes on devices where possible (Ivanti Recommendation: 0003). ■ Users do not share accounts, such as Apple ID's (Ivanti Recommendation: 0004). ■ Users will Remove any device Activation Locks if required (Ivanti Recommendation: 0005). ■ Users do not have the expectation of privacy on devices processing classified information (Ivanti Recommendation: 0006). ■ Devices may be tracked, locked, unlocked or wiped at any time (Ivanti Recommendation: 0007). 	<ul style="list-style-type: none"> ■ Systematically generated Identity Certificates are used for authentication. Examples of this may include accessing systems, applications, services and networks (Ivanti Recommendation: 0008). ■ The MDM is integrated with Gateways, Network Access Control (NAC), Conditional Access and other similar identity solutions. This allows such solutions to evaluate the devices compliance status, before granting access to data or systems (Ivanti Recommendation: 0009). ■ Continual risk monitoring of the networks mobile devices are connected to (Ivanti Recommendation: 0010). ■ Continual risk monitoring of mobile apps (Ivanti Recommendation: 0011). ■ Continual risk monitoring of the mobile device host posture (Ivanti Recommendation: 0012). 	<ul style="list-style-type: none"> ■ VPN-Chaining or Nested-VPNs are used to access sensitive information (Ivanti Recommendation: 0013). ■ An ISM Compliant Email Client, with an ISM Compliant Classifications engine is used (Ivanti Recommendation: 0014).
	Ivanti Recommendations: 0001, 0002, 0003, 0004, 0005, 0006, 0007.	Ivanti Recommendation: 0008, 0009, 0010, 0011, 0012.	Ivanti Recommendation: 0013, 0014.

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit [ivanti.com.au](https://www.ivanti.com.au)

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".A vertical bar on the right side of the page, transitioning from red at the top to orange at the bottom.

www.ivanti.com.au

+61 2 8966 1800

contact-anz@ivanti.com