Information Technology - User Device Security Standard

Section 1 - Purpose

(1) The purpose of this standard is to:

a. manage information security risks associated with user devices, and
b. protect RMIT information and prevent unauthorised access.

Section 2 - Authority

(2) Authority for this document is established by the Information Technology and Security Policy.

Section 3 - Scope

(3) This Standard applies to all staff, researchers, contractors, visitors, and any other parties (collectively referred as "Users") who have access to the IT assets of RMIT University and its controlled entities ("RMIT"). It is applicable for all devices (RMIT managed as well as non-RMIT managed devices that are used for the conduct of RMIT business) including but not limited to computers, laptops, tablets, phones, wearables, computer peripherals, and the internet of things.

Section 4 - Standard

Corporate (RMIT-Owned) Devices

(4) All devices and mobile services must be procured through Information Technology Services (ITS) using the approved mobile device process. ITS is responsible for maintaining a central register of devices.

(5) Device procurement must comply with the Business Expenses Policy as well as Procurement and Expenditure Policy.

(6) Cost centre managers are responsible for ensuring that devices and SIMs are returned by users when their engagement with RMIT terminates.

(7) Devices provided by RMIT remain the property of RMIT and can be revoked or reassigned as needed.

(8) RMIT has the rights to remove unauthorised or modified applications from devices and related content without notice or warning if it is deemed to be a security risk.

(9) RMIT may temporarily retain any device assigned to an individual to complete security or forensic investigation.

(10) RMIT may remotely lock, wipe, or reconfigure any device if it is deemed to be a security risk.

(11) Damaged devices must be repaired at an authorised service agent nominated by ITS. Costs associated with the repairs are paid by the owning cost centre.

(12) Lost or stolen devices must be reported immediately via the ITS Service and Support centre.

(13) Authorised users requiring international roaming services on an RMIT device whilst travelling overseas must complete an international roaming request at least five (5) days prior to departure.

Using a Non-RMIT Managed Device

(14) Information generated by RMIT users relating to RMIT business or operations remains the property of RMIT and is accessible by authorised RMIT staff.

(15) RMIT reserves the right to disconnect a non-RMIT managed device and disable services to that device without notification if it is deemed to be a security risk.

(16) RMIT is not responsible for any damaged, lost or stolen non-RMIT managed device an RMIT user may choose to use while conducting RMIT business nor for non-RMIT data damaged or lost on that device.

(17) Activity within RMIT work related apps, tools and tasks being conducted on non-RMIT managed device may be tracked to meet the legal and regulatory requirements of RMIT.

(18) Users must use only authorised applications to interact with RMIT data, and to ensure that all software used for RMIT business is legally licensed. The use of illegally obtained or unapproved applications is strictly prohibited.

(19) Users must maintain a non-RMIT managed device compatible with RMIT's published technical specifications (e.g. Hardening Standard) which will be updated by ITS as needed. Users should only use devices meeting these specifications to access RMIT network and data.

(20) When using a non-RMIT managed device (e.g. mobile or laptop) to access RMIT systems or data, users must:

a. keep the operating system and applications up to date; most updates include security patches
b. keep a current antivirus software version running
c. keep a screen lock enabled that uses a unique authentication method, PIN, pattern or fingerprint
d. enable a 'find my device' capability and ensure it is usable if the device is lost or stolen
e. use only Microsoft Office as the email client to access RMIT email
f. change their RMIT account password immediately if their device is lost or stolen
g. not store RMIT data locally on the device memory
h. have hard disk encryption enabled.

(21) Users must provide access to non-RMIT managed devices when notified that the device has been selected as in scope for e-discovery or if required for any investigation of a regulatory notifiable data breach or information security incident or litigation or if compelled by a court of law.

Status and Details

Status	Current
Effective Date	3rd June 2024
Review Date	3rd June 2029
Approval Authority	Senior Policy Advisor
Approval Date	18th April 2024
Expiry Date	Not Applicable
Policy Owner	Teresa Finlayson Chief Operating Officer
Policy Author	Sinan Erbay Chief Information Officer
Enquiries Contact	ITS Governance, Risk and Compliance