DEVICE SECURITY POLICY

Section	Information Technology Services
Contact	Chief Information Officer
Last Review	N/A
Next Review	November 2022
Approval	SLT 19/08/142
Effective Date	1 November 2019

Purpose:

This document specifies the University policy for the use, management and security of all devices that may hold or connect to Massey University's corporate network and information.

Key success factors:

- Confidential data that resides within Massey University's technology infrastructure, including internal and external cloud sources are protected
- Data is protected from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it could potentially be accessed by unsanctioned resources.

Policy:

This policy covers all devices and accompanying media connected to the Massey University network environment or handling University information, whether the device is owned by the user or the University.

All University staff or anyone performing work on behalf of the University (including contractors, consultants and volunteers) who use a device to access, store, back up, or relocate any University or client-specific data are subject to this policy. The policy addresses a range of threats to University data, or related to its use, such as:

Threat	Description
Device Loss	Devices used to transfer or transport work files that could be lost or stolen.
Data Theft	Sensitive corporate data is deliberately stolen and sold by an employee or unsanctioned third party
Copyright	Software copied onto a mobile device could violate licensing.
Malware	Viruses, Trojans, worms, spyware, malware, and other threats could be introduced via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the University to the risk of non-compliance with various identity theft and privacy laws.

Policy Statements:

1. The **Vice-Chancellor** has the overall responsibility for the confidentiality, integrity, and availability of corporate data.

2. The **Chief Information Officer** has delegated execution and maintenance of information technology and information systems.

3. All University staff are responsible to act in accordance with University policies and procedures.

4. Connectivity of all devices will be centrally managed by the University's Information Technology Services department who will use authentication and strong encryption measures. Although ITS will not directly manage personal devices purchased by employees, end users are expected to adhere to the same security protocols when connected to non-University equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the University's infrastructure.

5. It is the responsibility of University staff who use a device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any device that is used to conduct University business be used appropriately, responsibly and ethically. Failure to do so will result in immediate suspension of that user's account.

Access and Storage

1. ITS reserves the right to refuse the ability to connect devices to University connected infrastructure. ITS will engage in such action if such equipment is being used in a way that puts the University's systems, data, users, and clients at risk.

2. Classified information is material that the University deems to be confidential information (e.g. IN CONFIDENCE, SENSITIVE) that must be protected. When storing/processing classified information on a personally owned device, use of a University issued device (i.e. laptop or tablet) should always be seen as the preferred mechanism. Storage on personally owned devices can put classified information at risk of compromise. Anyone choosing to use their own personal device to handle University information is fully accountable and responsible for the security of their device.

3. IN CONFIDENCE and SENSITIVE information must be stored within and accessed from University information systems and Information Technology Services approved cloud providers, to ensure the security of and appropriate secure access to the information.

4. IN CONFIDENCE and SENSITIVE information must not be stored or transferred to a cloud computing service (such as personal OneDrive, Google Drive or Dropbox accounts for example) unless it is under a University negotiated contract.

Device and Physical Security

1. University staff using devices to access University information will, without exception use a strong password/passcode/passcode/ PIN enabled to reduce the opportunity for unauthorised access. Passwords and PIN's must be kept secure and be compliant with the Electronic Password Policy. The device must automatically lock after a maximum of five minutes of inactivity.

2. Devices used to access or store SENSITIVE information must be encrypted to reduce the opportunities for compromise or loss of information.

3. Devices should, where possible, have operating system and anti-virus updates enabled. “Jailbroken” or “Rooted” devices or those mobile devices which have otherwise circumvented the installed operating system security requirements (making them vulnerable to compromise) are not permitted to connect to the University ICT facilities.

4. Devices must not be left unsecured whether on or off University premises. When unattended the device must be locked (password/passcode/ PIN protected) and kept secure.

5. Users must take responsibility for a mobile device and not leave it unattended and unsecured.

6. All software contains security vulnerabilities, and software vendors are constantly supplying updates (patches) to address these vulnerabilities when they are identified. Device software operating systems and application software must be kept up to date with the latest security-related patches, as soon as it is practical to do so.

7. In the event of a lost or stolen device, it is incumbent on the user to report the incident to Massey University Service Desk and your manager immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than the ITS department. If the device is recovered it can be submitted to ITS for re-provisioning.

Definitions:

Classified Information consists of confidential information which has been classified using the University’s Data Classification Framework:

- IN CONFIDENCE information consists of information which if compromised would be likely to impede the effective operation of Massey University or adversely affect the privacy of its students or staff

- SENSITIVE information consists of information which if compromised would be likely to seriously damage the reputation of Massey University or endanger the safety of its students or staff.

Devices include, but are not limited to laptop computers and netbooks, tablet devices, smartphones, portable storage such as removable hard drives, USB memory sticks and data cards, portable audio visual equipment including data projectors, cameras etc.

Personally owned devices means any device that is held personally by an individual in a private capacity.

University issued device means any device that has been purchased, is owned or leased by the University (regardless of the source of funding).

University information means information relating to or connected with the University’s business or affairs.

Relevant Legislation:

Privacy Act, 1993.
Copyright Act, 1994.

Legal compliance:

Privacy Act 1993

Email communications and web activity may be monitored from time to time to support operational, maintenance, auditing, security and investigative activities. The Privacy Act 1993 governs the collection and use of information held by the University for the purposes of its management and administration. Personal information held for these

purposes must not be used for other purposes. Release of personal information otherwise than in accordance with the terms of the Privacy Act is strictly prohibited.

Copyright Act 1994

Email and the Internet make it very easy to copy the work of others. However, the Copyright Act 1994 makes it illegal to make or distribute copyright material without specific authorisation from the copyright owner. The University absolutely forbids the use of its computer and network facilities for a purpose which constitutes an infringement of copyright.

No material is to be used without the written permission of the copyright owner.

Copyright information is provided at the following intranet address: http://copyright.massey.ac.nz/

Note that the legal ownership of messages may not reside with the originator. For example, the ownership of intellectual property in the messages may rest with the University or other parties, depending on contracts, statutes and policies outside this document.

Related procedures / documents:

Massey University Collective and Individual Employment Agreements
Massey University Information Security Manual
Policy on Staff Conduct
Electronic Password Policy
Student Academic Integrity Policy
Intellectual Property Policy
Desktop Hardware and Software Policy

Document Management Control:

All policies should have a footer, which indicates the document number (if any); person who prepared the document; person/body who authorised the document (policy owner); the date the document was issued or revised; the date the policy is to be reviewed and a statement that this policy is the property of Massey University. This information should be set out as follows:

Prepared by:	Chief Information Officer
Authorised by:	Deputy Vice-Chancellor, Finance and Technology
Approved by:	SLT 19/08/1942
Date issued:	November 2019
Next review:	November 2022