REMOTE INFORMATION WORKER POLICY

Section	Information Technology Services
Contact	Chief Information Officer
Last Review	August 2016
Next Review	August 2019
Approval	SLT 16/08/160
Effective Date	August 2016

Purpose:

The purpose of this policy is to define the protocols and expectations for Massey University staff, contractors, and affiliates, who work on information and information systems remotely (Teleworkers).

This policy seeks to:

- protect the integrity and confidentiality of institutional data.
- prevent institutional data from being deliberately or inadvertently stored insecurely, viewed or intercepted from a device, or carried over an insecure network, where it be accessed by unsanctioned resources.

Audience:

All users of Massey University ICT, who use access information when away from the office.

Policy:

- Avoid carrying documentation or devices (including media such as CDs, DVDs, or USB drives) containing Massey University data in public locations as much as reasonably possible.
- Always ensure any devices, media, documents, or hard copy material containing sensitive, commercial or personal information are not visible to unauthorised parties, and are appropriately secured when not in use.
- When logging in or accessing Massey data or communications in external or public spaces, care must be taken to ensure information is not visible to unauthorised parties.
- Users must ensure that devices used to store or access Massey University Information systems:
  - Are protected with a user code and password (or key lock) when logging on, or when left unattended. As a minimum, these settings must comply with the Massey University User Code and Password Policy.
  - Not be set to remember user codes and passwords when logging into Massey University systems such as websites, applications or VPN clients.
  - Run up-to-date antivirus software.
  - Do not have private, sensitive or confidential data stored on them that is accessible by other device users.
  - Regularly review Massey University data, and erase local copies when no longer required.
  - By default, data or information updated or manipulated remotely is not backed up unless it is being worked on via a connected network share, or from within an online application. It is the user's responsibility to protect work or information in a reasonable way.
- Portable storage media, including CDs, DVDs, or USB drives, used to store or transfer institutional data must be kept physically secured at all times.
- Always treat public free internet or Wi-Fi networks as insecure:
  - Always verify with staff or signage the correct name of the Wi-Fi network and always double-check this on the device before joining.

© This Policy is the property of Massey University

  - Always disabled internet and file sharing from your device before connecting to Wi-Fi network.
  - Only log on to trusted web sites that use encryption (display a padlock), or where possible use the Massey VPN to safeguard data in transmission.
- Remote information workers who use Massey supplied Mobile Devices must also read and comply with the Mobile Device Policy.
- In the event information loss, or a suspected security breach, users must notify their manager, the information owner, and/or the Massey ITS Service Desk (as relevant to the breach), as soon as possible.
- For more information on this policy, or on how to manage and protect your data while you are working remotely, please contact the ITS Service Desk on 06-356-9099 extension 82111, or via the website: http://AskIT.massey.ac.nz.

Definitions:

ICT	Information and communications technology is an umbrella term used to cover all network, computing, software, and telecommunications systems and resources, including storage and peripheral devices, whether used for research, teaching or administration.
Information Security	Directly relates to providing for the confidentiality, integrity and availability of all digital resources within Massey University. This provides assurance that information is only accessible by those who are authorised to view it, records and data are valid and correct, and mission critical information is accessible when it is needed.
Key lock	In this document used as a term to describe screen saver passwords or other similar security mechanisms on mobile devices that require the device to be unlocked each time it is switched on or left idle for a period of time. This prevents unauthorised users from using the device.
Teleworker	Refers to staff, contractors, volunteers, or affiliates who work from home, in transit, or otherwise remotely from Massey University provided offices, and use Massey University information and information communication and technology (ICT) tools.
VPN	Or Virtual Private Network is a secure and encrypted connection between a remote client device and the internal Massey network. It acts to secure data transmitted over a typically insecure network (such as the internet) to a corporate (private) network.
Wi-Fi	Or Wireless network, allows mobile or portable devices to connect to a network (such as the internet) using radio frequency (RF) technology rather than via a network cable.

Legal compliance:

Privacy Act, 1993

Legal compliance:

- Privacy Act 1993
  Establishes a set of privacy principles to ensure the protection of personal privacy in respect of both public and private sector organisations. The Act is of prime importance and should be clearly understood by all information management professionals.

Related policy and procedure compliance:

Mobile Device Policy
User Code and Password Policy
Internet Use and Digital Communications Policy
Privacy Policy

© This Policy is the property of Massey University

Telecommunications Policy

Related procedures / documents:

ISO/IEC 27000:2014 – Information technology – Information security management systems
Information Security @ Massey University
Privacy @ Massey University
Massey University Information Security Manual

Document Management Control:

Prepared by: Information Technology Services
Authorised by: The Chief Information Officer
Approved by: SLT 16/08/160
Date issued: August 2016
Last review: August 2016
Next review: August 2019

DRAFT

© This Policy is the property of Massey University