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.

Approved Mobile Devices

Massey-supplied mobile devices

1. All Massey-supplied mobile devices must be procured from an authorised supplier via the University's purchasing system through ITS:

   the most current and up-to-date mobile handset list is available to all staff via the mobile phones page on the ITS intranet; other devices are available

Definitions:

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.

Malware means programming code, scripts, active content, and other software designed to disrupt, collect private information, or gain unauthorised access to system resources.

Network facilities are Information Communication and Technology (ICT) systems accessed via connection to the