Monash University Policy

Policy Title	ICT Security and Risk Policy
Date Effective	01-August-2014
Review Date	01-August-2017
Policy Owner	Chief Information Officer
Category	Operational
Version Number	1.1
Content Enquiries	IT Service Desk - http://monash.edu/esolutions/contact/
Scope	• All Australian campuses • All staff, students and other Authorised Users
Purpose	To apply proportionate and effective management of ICT security risks throughout Monash University to enable the conduct of the University's business and necessary protection of the University's people, information and assets. To authorise the establishment of an IT Security and Risk Steering Committee and the Information Security Management System (ISMS).

POLICY STATEMENT

The Chief Information Officer is authorised to develop and implement ICT Security related Procedures, and the University Information Security Management System (ISMS).

The University's Information Security Management System (ISMS) will ensure sufficient and proportionate security controls are implemented to adequately protect information assets. The ISMS is part of an overall management system, based on a business risk approach which includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

The Chief Information Officer is responsible for assessing and monitoring the university's IT risk profile, ensuring active management of the IT risk register and related controls.
The IT Security and Risk Steering Committee will maintain oversight of the university's IT risk profile, and ICT Security related procedures and systems.

This policy applies to all Authorised Users of Monash University in their use of ICT Facilities and Services.

The University reserves the right to access, review and monitor Monash ICT Facilities and Services, and the University reserves the right to remove access or disconnect systems and services where risk is identified to the University.

Associated Framework: ICT Security and Risk Framework

Supporting Procedures	ICT Security Procedures
Responsibility for implementation	Chief Information Officer
Status	Revised

Approval Body	**Name**: Chief Operating Officer and Senior Vice-President (Administration) **Meeting**: n/a **Date**: 01-August-2014 **Agenda item**: n/a
Endorsement Body	**Name**: Chief Information Officer **Meeting**: n/a **Date**: 01-August-2014 **Agenda item**: n/a
Definitions	**Authorised Users**: All people authorised to use the ICT Facilities and Services for any purpose, including but not limited to students, staff, visitors to the University, members of partner organisations, staff of any entity/company in which Monash has an interest, honorary and adjunct appointees, contractors, alumni and users accessing via a federated access pathway. **Authorised Staff**: All people authorised by the CIO to monitor accounts, files, stored data and network data, and to disconnect IT equipment in the event of an IT security breach. Normally eSolutions Division staff. **CIO**: Chief Information Officer **ICT**: Information and Communications Technology **ICT Facilities and Services**: Shall include but not be limited to: all University-owned computers and associated ICT networks, internet access, email, hardware, data storage, computer accounts, software (both proprietary and those developed by the University) and telephony services; any computer or device owned or operated by someone other than the University when connecting to the University information network or being used for University Business; any computer account, software or information provided or created for University Business; all physical spaces using ICT and designated for teaching, study, research and administration across the University; ICT services provided by third parties that have been engaged by the University, including any hosted or similar service through which University information is stored or services are provided to enable Users to undertake University Business; and ICT services made accessible to Monash users through federated access arrangements. **ISMS**: Information Security Management System – set of standards-based documents that govern operation of the key information security management functions. The ISMS is that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. **Monitoring**; To Monitor: Tasks (including testing and scanning) undertaken by Authorised Staff to ensure maintenance of security of ICT services and systems **University**: Monash University **University Business**: Any activity conducted either in the course of employment or as part of or related to a University course or other University activity that is not purely personal.
Legislation Mandating Compliance	Information Privacy Act 2000 (Vic) - note Information Privacy Principles within the Act (Section 14 and Schedule 1) Privacy Act 1988 (Commonwealth) Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Commonwealth) Health Records Act 2001 (Vic) - note Health Privacy Principles within Act (Section 19 and Schedule 1) Higher Education Support Act 2003 (Commonwealth) - note Part 5-4 Management of Information, and specifically section 179-10 Use of Personal Information

	Education Services for Overseas Students Act 2000 (Commonwealth) - specifically The National Code 2007, Standard 3.1(d) Epidemiological Studies (Confidentiality) Act 1981 (Commonwealth) - where relevant to a research project (needed) Monash University (Council) Regulations Part 7 Monash University (Vice-Chancellor) Regulations Part 5 Monash University Statute
Related Policies	ICT Security and Risk Framework Electronic Information Security Policy Social Media Policy Acceptable Use of Information Technology Facilities by Students Policy Information Technology Use Policy - Staff & Other Authorised Users
Related Documents	Conduct and Compliance Procedure - Staff Use of Social Media Conduct and Compliance Procedure - Provision of University IT Equipment and Communication Facilities to Staff Conduct and Compliance Procedure - Privacy