Monash University Procedure

Procedure Title	ICT Security Procedures
Parent Policy	ICT Security and Risk Policy
Date Effective	01-August-2014
Review Date	01-August-2017
Procedure Owner	Chief Information Officer
Category	Operational
Version Number	2.0
Content Enquiries	IT Service Desk – http://monash.edu/esolutions/contact/
Scope	• All Australian campuses • All Staff, students and other Authorised users
Purpose	Monash University's Information and Communication Technology (ICT) Facilities and Services are provided to further the objectives of the University and are integral to the effective performance of its operations. ICT Security is the process that ensures the availability, integrity and confidentiality of ICT Facilities and Services. Effective ICT security is essential to ensure the University meets its obligations for security, privacy, and preservation of intellectual property. Monash University recognizes that all Authorised Users should be made aware of their responsibilities for ICT security and for the need for effective ICT security management.
PROCEDURE STATEMENT	

1. Authorised Users - The Authority to Use

1.1. Authorised Users are authorised to use ICT Facilities and Services consistent with the terms of the University's policies on Information Technology Use Policy - Staff & Other Authorised Users and Acceptable Use of Information Technology Facilities by Students.

1.2. Subject to correct registration of IT equipment through the University's 'Addhost' service, Authorised Users are authorised to connect such IT equipment to the Monash University network via wall outlets or radio links installed by or on behalf of the eSolutions Division.

1.3. eSolutions Authorised Staff are authorised to disconnect IT equipment from the Monash University network in the event of a breach outlined in Section 4 below.

Responsibility

All users
CIO
Authorised Staff

Monash University Procedure

2. University Right to Monitor

2.1. As owner, Monash University has the right to monitor the use of its ICT systems and services, which includes any device connected to Monash systems. Where Monash University has contracted third party service provision, monitoring may occur under the Terms of Service or license conditions or policies of that service.

2.2. Monitoring will be undertaken routinely by eSolutions Authorised Staff in the normal course of their duties to maintain technical security and operational efficiency of the system/service. Any extraordinary action taken to monitor IT services must be authorized by the CIO or Executive Director Human Resources (or delegate).

2.3. Monitoring will occur in cases of suspected breach of law, condition of employment, or University policy, including the University's policies Information Technology Use Policy - Staff & Other Authorised Users and Acceptable Use of IT Facilities by Students and Social Media Policy. In these cases, inspection of personal information will be undertaken in accordance with requirements of relevant Privacy legislation and only after approval by relevant senior officer (Executive Director, Human Resources Division, CIO, Executive Director Student Services or University Solicitor).

2.4. Electronic data, information and material created by Authorised Users will be treated as confidential during monitoring and all monitoring references destroyed if determined not relevant. Access to such information will be strictly on a need- to-know basis for technical or administrative purposes.

2.5. Except for normal administrative processes, the accounts, files, stored data and network data including e-mail messages created by Authorised Users, are held secure from intervention by other users.

Responsibility

CIO
Authorised staff
Executive Director, Human Resources
Chief Operating Officer
Executive Director Student Services
Deans and PVCs Malaysia and South Africa
University Solicitor

3. Security Breaches

3.1. Where Authorised Users become aware of any breach of ICT security that may impact the availability of ICT Facilities and Services, they should notify eSolutions Division IT Security and Risk team or the CIO.

3.2. It is not appropriate for Authorised Users to broadcast or publicise widely any security breach or suspected breach of ICT security. All communication should be directed solely to the above-named officers. Authorised Users should be aware that any such broadcast or widespread publicity will result in increased risk to the integrity of ICT Facilities and Services, and may be subject to sanctions as detailed in Section 4.

Monash University Procedure

Responsibility

All users
CIO
eSolutions IT Security and Risk

4. Sanctions

4.1. eSolutions Authorised Staff may disconnect ICT equipment from the Monash University network when monitoring detects a breach in ICT security or a breach of the law or University policy. Such disconnection would normally be preceded by notice to the relevant Authorised User, but in an emergency, notice will follow disconnection.

4.2. In the event of a breach in the law or University policy, disciplinary proceedings, where appropriate, will be instituted in accordance with Monash University Statutes and regulations, or according to relevant contracts and/or workplace agreements.

Responsibility

CIO
Authorised Staff

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
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

Monash University Procedure

	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

Monash University Procedure

	Conduct and Compliance Procedure - Provision of University IT Equipment and Communication Facilities to Staff Conduct and Compliance Procedure - Privacy