THE UNIVERSITY OF
NOTRE DAME
AUSTRALIA

POLICY:
INFORMATION SECURITY

1 Purpose

The University of Notre Dame Australia (**University**) recognises the importance of ensuring that appropriate measures are in place to:

- Secure its Information & Communication (ICT) assets, systems, services, information and infrastructure.
- Provide protection from liability and damage arising from the use of its ICT Systems

This Policy sets out the principles and rules for achieving the objectives set out in paragraph 1.1 and has been developed in accordance with AS/NZS/IEC 27001:2006 *Information Technology – Security Techniques – Information Security Management Systems – Requirements*.

2 Definitions

The following definitions apply in this Policy:

Business Owner means the Senior Staff member with functional responsibility for particular Data, software, system or IT asset.

Data means any information stored electronically physically.

ICT Infrastructure means all information and communications technologies. Includes (but not limited to) software, systems, assets, network resources, servers and switches.

Users refers to all Staff Members, Students and to another person otherwise connected or associated with the University (but not employed) and/or who may utilise the University's ICT infrastructure. Includes Temporary Users.

User Card means either a University identification card (e.g. Staff, Student or Alumni Card) provided by the Student Administration or the Staffing Office or Temporary User/Visitor Card provided by the relevant University department.

User Number means either a Student or Staff number provided by the Student Administration or the Staffing Office or a Temporary User Identifier provided by the IT Department.

"Mobile Device" refers collectively to Mobile Telephones and Tablet Computers and includes the SIM or other activation card or service supplied with the Mobile Device or separately.

"Mobile Telephone" is a telephone, Personal Digital Assistant, *Blackberry*, Smartphone or any other emerging voice or data device that accesses a commercial mobile telecommunications service.

"Tablet Computer" includes *iPads*, *Android* computers, *BlackBerry* and *Windows* tablets.

IT Department means the University's IT Department.

Senior Staff Member means the relevant Dean, Executive Director, Director or Executive Staff.

Software any electronic system used by the University to store or process information.

Staffing Office means the relevant Staffing Office (National or Campus)
Student Administration Office means the relevant Student Administration Office (Fremantle and Broome or Sydney)

Temporary Users means persons provided with temporary access to the University ICT infrastructure for a specific purpose and finite period. E.g. Guests, consultants or technicians.

3 Scope

3.1 This Policy applies to all Staff Members, Students (including Alumni) and to another person otherwise connected or associated with the University (but not employed) and/or who may utilise the University's ICT infrastructure.

3.2 The University will make this policy available to all Users and to external providers who must comply with it and with any related Policies and Procedures.

4 Access

4.1 The University provides Users with access to its ICT Infrastructure in support of its learning, teaching, research and administrative activities. These facilities include (but are not limited to) Internet, email, file and print services, libraries, data network, Service Desk and Student computer facilities located across all campuses.

4.2 Each User will be provided with a User Card and a User Number. A User Card is proof of authorisation and must be carried at all times when on campus and using University ICT Infrastructure. Each User Card and User number must be protected by a password, that complies with the University Password Protocols maintained and published by the IT Department.

4.3 Each User is responsible for securing and maintaining their assigned User Card and User Number and for all activities in connection with that User Card and User Number. Knowingly disclosing passwords or providing a User Card or User Number to any other person will constitute a breach of this Policy and may result in disciplinary procedures.

4.4 The University expects that all Users will take all reasonable steps to protect and ensure the integrity and security of all ICT Infrastructure.

4.5 Where Temporary Users require access for a specific purpose, an expiry date based on the date of completion of the relevant task must be put in place to ensure that the temporary account is not accessible after that date.

4.6 Access for maintenance and support must only be granted to the relevant part of the IT Infrastructure required and be restricted to only the systems for which support or maintenance is required.

5 Access Termination or Suspension

5.1 The relevant Student Administration Office (Fremantle and Broome or Sydney) is responsible for ensuring that User access is immediately disabled when a student is no longer enrolled at the University or recognised as an Alumni of the University.

5.2 The relevant Staffing Office (National or Campus) is responsible for ensuring that User access is immediately disabled when a staff member or other person otherwise connected or associated with the University (but not employed) is no longer employed or connected with the University.

5.3 The IT Department is responsible for ensuring that Temporary User access is immediately disabled when access is no longer required for the prescribed purpose.

5.4 In circumstances in which User access needs to be disabled immediately (such as under a Staffing or other process) this must be authorised by the Vice Chancellor or Chief Operating Officer.

6 Network Usage

Interfering with or manipulating the University's network or IT Infrastructure is not permitted save in accordance with the procedures outlined in this Policy

7 Mobile Devices

7.1 Mobile Devices must be used in accordance with the POLICY: Mobile Telephones & Tablet Computers – Eligibility, Use & Management.

7.2 University supplied Mobile Devices must be configured with a password or pin code in order to access the device.

7.3 All Mobile Devices must be set up with an inactivity screensaver which requires a unique password for reactivation and has an idle time of no more than 15 minutes before activation.

8 Electronic Communications

The University's electronic communications and internet systems must be used solely in accordance with the POLICY: Email & Internet usage.

9 Software

New Software and Software Development

9.1 This Policy details the requirements for the introduction, development and testing of new Software. In all cases, Users are not permitted to develop or install Software using the University's ICT Infrastructure. The development and installation of new Software must only be undertaken by the IT Department.

9.2 No new Software can be introduced, developed or used on the University's ICT Infrastructure without prior approval in accordance with the ICT Governance Committee Terms of Reference or ICT policies in force from time to time.

9.3 Any Software introduced or used in breach of this Policy that causes harm or adversely affects the ICT Infrastructure or the confidentiality or privacy of the University and its Staff Members and/or Students will be considered and treated as a direct attempt to compromise the University and will be dealt with accordingly and on this basis.

9.4 Software development and testing must only be performed in a controlled, test environment until such time that all potential flaws, bugs and vulnerabilities are removed. Only then can the developed Software be applied to a production environment.

Antivirus Security and End Point Security

9.5 Where possible, University issued Mobile Devices and relevant ICT Infrastructure must have end-point security software installed which has automatic updates enabled. This is to ensure that University Software remains updated to meet the latest threats. The University employs antivirus systems in place checking its email systems.

9.6 The University expects that any non-University devices also have current updated antivirus software installed. Where a user accesses the University's IT Infrastructure or services from a non-University device, it is the sole responsibility of the User to ensure that the non-University device has current updated antivirus software installed and does not expose the University to potentially disruption and damage due to virus infected computers.

9.7 Any non-University issued device connected to the University network remains the responsibility of the owner. The University will take no responsibility for any damage that may be caused to a non-University device that is connected by a User to the University network.

10 Data Security

10.1 Users may only access or view Data or be given access to Data and as required by their position, enrolment or job function. Any User who gains access to Data without permission shall be deemed as unauthorised and will be subject to disciplinary action.

10.2 No Data may be transferred or stored outside of the University without the written consent of Vice Chancellor or relevant officer authorised by the Vice Chancellor from time to time.

11 Communications Security

Users may only use communications systems that have been authorised and permitted by the University’s IT Department. Communications include, but are not restricted to wireless access, voice via land line, voice via computer network (VOIP), email, electronic file transfer, Virtual Private Network (VPN) connections, dial-up modem, Infra-Red, Bluetooth and ICT network infrastructure.

12 Physical Security

12.1 Purchase and disposal of Mobile Devices and ICT infrastructure must be carried out in accordance with the relevant University policy.

12.2 All offices, computer rooms and work areas containing confidential information, or access to confidential information must be physically protected and (during working hours) appropriately supervised.

12.3 The University requires that any PC/ Laptop/Portable computer on University premises be logged out and turned off at the end of the working day unless the IT Department specifically requests that equipment remain on for overnight processing or updating.

12.4 No computer equipment can be moved unless specific authorisation has been granted by the IT Department. This does not apply to Mobile Devices provided to allow the User to work while away from campus.

12.5 All Users who have been issued with portable equipment or Mobile Devices have personal responsibility to ensure that these remain secured at all times.

13 Disaster Recovery

13.1 All major IT systems within the University must be backed up on a regular basis. The IT Department will have and maintain a Backup Plan & Strategy which details the frequency of backups.

13.2 All major IT systems within the University must be subject to appropriate Change Control processes, as determined by the ICT Governance Committee. These will ensure that ICT facilities and services are maintained and kept running at appropriate performance and functionality levels. Change Control processes must ensure that the disruption is kept to a minimum and appropriate procedures exist to address any issues arising during system changes.

13.3 The IT Department will maintain a Disaster Recovery Plan to support the University’s Business Continuity Plan. This will provide for and put in place procedures and processes that ensure that services are returned to normal operation in the shortest possible time.

14 Authorisation & Rights

14.1 The University reserves the right to examine any information on its facilities and to monitor use. This right may only be exercisable by the Vice Chancellor or such officer as may be authorised in writing by the Vice Chancellor from time to time.

14.2 The Standing Delegations of Authority, as authorised by the Vice Chancellor and in force from time to time set out the University's financial delegations and apply to all IT expenditure.

14.3 The ICT Governance Committee Terms of Reference detail specific requirements relating to IT Expenditure.

15 Reporting

The IT Department shall maintain a central register of all IT Software, licences and IT Infrastructure and report to the Vice Chancellor or relevant Executive as required.