Information Management & Technology Services

CYBER SECURITY POLICY

Date approved:		**Date Policy will take effect:**		**Date of Next Review:**	
Approved by:					
Custodian title & e-mail address:	Cyber Security Manager sah@uow.edu.au				
Author:	Scott Hamilton				
Responsible Faculty/ Division & Unit:	Information Management & Technology Services (IMTS)				
Supporting documents, procedures & forms of this policy:					
References & Legislation:	IT Acceptable Use Policy IT Server Security Policy Crimes Act, 1900 (New South Wales) Crimes Act, 1914 (Commonwealth) Student Conduct Rules Critical Security Controls, https://www.cisecurity.org/critical-controls/				
Audience:	Public – accessible to anyone				
Expiry Date of Policy:	Not applicable				

1 Purpose of Policy

a) This document sets out University policy on Cyber Security.

b) Cyber Security is about defending IT Facilities and Services and stored data from unauthorised access, use, disclosure, disruption, modification and destruction. It is concerned with ensuring integrity, availability, confidentiality and safety of data and services; and ensures controls are proportionate to risk.

c) The University recognises the importance of Cyber security. It is committed to ensuring all University activities involving information technology are appropriately defended against Cyber security threats.

d) The University recognises that successful implementation of Cyber security relies on having a well-informed user community combined with effective management procedures. This overarching policy is supported by a Cyber Security framework which includes supplementary policies and guidelines on specific topics; operational practices; action plans; technology controls; education programs and monitoring and assurance activities.

e) The University of Wollongong is committed to the appropriate use of Information Technology and Services to support its learning, teaching, research, administrative, and service functions. The IT Acceptable Use policy defines acceptable behaviour expected of Users of University IT Facilities and Services.

2 Definitions

Word/Term	Definition (with examples if required)
IT Facilities and Services	Information Technology facilities operated by or on behalf of the University. This includes services and systems and associated computing hardware and software used for the communication, processing and storage of information
Cyber security	The practice of defending computing devices, networks and stored data from unauthorised access, use, disclosure, disruption, modification or destruction
Cyber Security Team	Capability appointed by the Director, IMTS. Their responsibilities are outlined in the Cyber Security Policy
Director, IMTS	Director, Information Management & Technology Services
IMTS	Information Management & Technology Services
University	University of Wollongong and controlled entities
User	Any person using any of the IT Facilities and Services
University network	The network infrastructure used by the University of Wollongong including all network services on main campus, satellite campuses, and wholly owned subsidiaries with trusted access to UOW services

3 Application & Scope

a) This policy represents the University Institutional position and takes precedence over other relevant policies which may be developed at a local level.

b) All Users should be aware of this policy, their responsibilities and legal obligations. All Users are required to comply with the policy and are bound by law to observe applicable statutory legislation.

4 Policy Principles

a) University IT Facilities and Services will be protected by effective management of Cyber security risks at all levels of the University as laid down in the University's IT policies and procedures.

b) Use of IT Facilities and Services must comply with University policies and relevant legislation. Examples of legal regulation include privacy, copyright, government information (public access), equal employment opportunity, intellectual property and workplace health and safety.

c) The IT Facilities and Services will be provided, managed, and operated such that:

i. The 'Critical Security Controls' maintained by the Centre for Internet Security are adopted to establish a broad and effective defensive base. This is an evidence based, pragmatic and practical approach that recognises an expert consensus agreement on priority controls.

ii. Security critical infrastructure, application services and data are individually identified and are subject to risk based management and additional controls as appropriate.

iii. A monitoring program is approved annually to ensure ongoing effectiveness of cyber security that includes activities such as auditing, log and event analysis, vulnerability scanning and penetration testing.

iv. Disaster recovery plans for security critical applications and foundational IT infrastructure are developed and maintained and an associated testing program is approved annually.

5 Policy Responsibilities

The following responsibilities apply:

Director, IMTS

The Director of IMTS has the following responsibilities:

a) carriage of the University Cyber Security Policy and supporting framework;

b) ensuring effectiveness of Cyber security measures through monitoring programs;

c) ensuring effectiveness of disaster recovery plans with a program of testing;

d) appoint a Cyber Security team;

e) authorise complementary operational procedures to support this policy;

f) authorising the isolation or disconnection of any equipment or IT Facility from the University network which poses a severe and unacceptable risk; and

g) reporting to appropriate governance bodies including the Risk, Audit and Compliance Committee.

Cyber Security Team

The Cyber Security Team has the following responsibilities:

a) own and operate processes required by the cyber security policies and framework;

b) continuous development and improvement of cyber defences;

c) continuous monitoring and review of practices and defences; and

d) conduct education activities to ensure awareness of cyber security threats and defences.

Risk, Audit and Compliance Committee

The Risk, Audit and Compliance Committee has the following responsibilities:

a) monitor cyber security risks and controls by reviewing the outcomes of cyber risk management processes and monitor emerging risks; and

b) oversee the adequacy of cyber security capability and controls.

Staff with responsibility for managing any IT Facility

Staff whom manage any IT Facility have the following responsibilities:

a) Develop, operate and manage the IT Facility according to University Cyber Security policies;

b) Regularly monitor and assess the related cyber security controls to ensure ongoing effectiveness; and

c) Immediately report all security incidents and breaches to the Cyber Security Team.

Users of IT Facilities and Services

Individual Users have responsibility to:

a) Use IT Facilities and Services according to IT policies at all times;

b) Be aware of the security requirements of the IT Facilities and Services they use, and take every precaution to safeguard their access to these systems against unauthorised use; and

c) Immediately report any known or suspected security incidents and breaches to IMTS.

6 Version Control and Change History

Version Control	Date Effective	Approved By	Amendment