UNIVERSITY
OF WOLLONGONG
AUSTRALIA

CYBER SECURITY POLICY

Date first approved: 9 December 2016	**Date of effect:** 9 December 2016	**Date last amended:** (refer Version Control Table)	**Date of Next Review:** August 2024
First Approved by:	University Council		
Custodian title & e-mail address:	Cyber Security Manager, Infrastructure, IMTS it-security@uow.edu.au		
Author:	Cyber Security Manager, Infrastructure, IMTS		
Responsible Division & Unit:	Information Management & Technology Services (IMTS)		
Supporting documents, procedures & forms of this policy:	IT Acceptable Use Policy IT Server Security Policy Student Conduct Rules UOW Data Breach Response Plan		
Relevant Legislation & **External Documents:**	*Crimes Act 1900* (NSW) *Crimes Act 1914* (Commonwealth) Critical Security Controls Centre for Internet Security		
Audience:	Public		

Submit your feedback on this policy document using the Policy Feedback Facility.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Contents

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

1 Purpose of Policy

1. This document sets out University policy on Cyber Security.
2. 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.
3. 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.
4. 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; guidelines on specific topics; operational practices; action plans; technology controls; education programs and monitoring and assurance activities.
5. 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. The University requires users to comply with the IT policies and associated requirements governing the Use of IT Facilities and Services as a condition of their use. These are accessible on the University Policy Directory.

2 Definitions

Word/Term	Definition (with examples if required)
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
IMTS	Information Management & Technology Services at the University of Wollongong.
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
University	University of Wollongong and controlled entities
University network	The network infrastructure used by the University including all network services on main campus and satellite campuses with trusted access to UOW services
User	A person assigned a User Account by the University or a person who is otherwise authorised to use University IT Facilities and Services

3 Application & Scope

1. This policy applies to all Users and devices of IT Facilities and Services at the University of Wollongong.
2. All Users should be aware of this policy, their responsibilities and legal obligations.
3. All Users and devices are required to comply with the policy and are bound by law to observe applicable statutory legislation.

4 Policy Principles

1. All University IT Facilities and Services will be protected by effective management of Cyber security risks.
2. 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.
3. The IT Facilities and Services will be provided, managed, and operated such that:
    a. 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. The Critical Security Controls have been matured by an international community of institutions and individuals that:
        i. share insight into attacks and attackers, identify root causes, and translate these into classes of defensive action;
        ii. document stories of adoption and share tools to solve problems;
        iii. track the evolution of threats, the capabilities of adversaries, and current vectors of intrusions;
        iv. map the Controls to regulatory and compliance frameworks and bring collective priority and focus to them;
        v. share tools, working aids, and translations; and
        vi. identify common problems (such as initial assessment and implementation roadmaps) and solve them as a community instead of alone.

    These activities ensure that the Controls are a prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and compliant with all industry or government security requirements.

    b. Security critical infrastructure, application services and data are individually identified and are subject to risk based management and additional controls as appropriate.
    c. A monitoring program is approved annually by the Director of IMTS to ensure ongoing effectiveness of cyber security that includes activities such as auditing, log and event analysis, vulnerability scanning and penetration testing.
    d. Disaster recovery plans for security critical applications and foundational IT infrastructure are developed and maintained and an associated testing program is approved annually by the Director of IMTS.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

5 Roles & Responsibilities

Director, IMTS

1. The Director of IMTS has the following responsibilities:
    a. taking 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 through a program of testing;
    d. appointing a Cyber Security team;
    e. approving complementary operational procedures to support this policy;
    f. approving 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 on matters pertaining to cyber security.

Cyber Security Team

2. The Cyber Security Team has the following responsibilities:
    a. owning and operating processes required by the cyber security policies and framework;
    b. undertaking continuous development and improvement of cyber defences;
    c. undertaking continuous monitoring and review of practices and defences;
    d. conducting educational activities to ensure awareness of cyber security threats and defences; and
    e. reporting all relevant security incidents and breaches in line with the UOW Data Breach Response Plan.

Risk, Audit and Compliance Committee

3. The Risk, Audit and Compliance Committee has the following responsibilities:
    a. monitoring cyber security risks and controls by reviewing the outcomes of cyber risk management processes and monitoring emerging risks; and
    b. overseeing the adequacy of cyber security capability and controls.

Staff with responsibility for managing any IT Facility or Service

4. Staff whom manage any IT Facility have the following responsibilities:
    a. developing, operating and managing the IT Facility according to University Cyber Security policies;
    b. regularly monitoring and assessing the related cyber security controls to ensure ongoing effectiveness; and
    c. immediately reporting all security incidents and breaches to the Cyber Security Team.

Users of IT Facilities and Services

5. Individual Users have the following responsibilities for themselves and their devices:
    a. using IT Facilities and Services according to IT policies at all times;
    b. being 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 reporting any known or suspected security incidents and breaches to IMTS.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

6 Version Control and Change History

Version Control	Date Effective	Approved By	Amendment
1	9 December 2016	University Council	First version, resulting from major review of IT Policy suite.
2	19 August 2020	Chief Operating Officer	Administrative amendments as an outcome of review.