

Cyber Security

Policy UP19/2

Approver	Senate
Sponsor	Deputy Vice-Chancellor (Operations)
Owner	Chief Information Officer
Secretary	Corporate Secretary
Policy Type	Institutional
Policy Category	Operations and Support Services

1 Purpose

- 1.1 The purpose of this Policy is to —
- (a) express the commitment of the University in maintaining effective and risk-based Cyber Security as an enabler of academic freedom, student and staff security, and trusted research;
 - (b) express accountability and responsibilities for Cyber Security;
 - (c) express guiding principles for safeguarding University Digital Resources and ensure compliance; and
 - (d) contribute to maintaining a University culture of integrity.
- 1.2 This Policy is to be read in conjunction with the following —
- (a) Acceptable Use of IT Policy;
 - (b) Cyber Security Strategy;
 - (c) Mandatory Cyber Security standards;
 - (d) Optional cyber security guidelines;
 - (e) Cyber Security Controls Catalogue;
 - (f) Information Protection Policy;
 - (g) Information Retention Policy;
 - (h) Information Privacy Policy; and
 - (i) The Codes of Ethics and Codes of Conduct.

2 Definitions

Term	Definition
Business System Owner	A senior Employee who is responsible for managing University Information stored within a University Information Management System in accordance with University policies.
Cyber Security	The protection of the confidentiality, integrity and availability of Digital Resources. Cyber Security focuses on the technical aspects of safeguarding University Information, forming an integral part of Information Protection.
Cyber Security Control Exemption	A formally acknowledged and documented non-compliance with a requirement or safeguard prescribed in the Cyber Security framework.
Cyber Security Incident	An unwanted or unexpected Cyber Security event or events that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service or the University prompting the need for a response and recovery.
Cyber Security Risk Rating	A numeric value representing the confidentiality, availability and integrity requirements of a Digital Resource. The rating is established using the

Term	Definition
	University IT Risk Management Standard within the Cyber Security Framework.
Digital Identity	Information, such as user account, password or an email address, used by computer systems to represent a member of the University Community.
Digital Resources	Any IT Service, IT Asset, Digital Identity or digital Information of UWA.
IT Assets	Any tangible thing, belonging to, or contracted to the University, which is worth protecting and used to access, process, store or transmit data.
IT Services	The combination of processes, expertise and resources by which University IT deliver value to the University Community to enable the achievement of their business objectives.
Misconduct	Conduct that includes, but is not limited to — (1). negligence in the performance of an Employee's duties; (2). misbehaviour; (3). refusal to carry out a lawful and/or reasonable instruction; (4). a breach of the University's Code of Ethics and Code of Conduct; or (5). a breach of Policy.
Misconduct Process	A series of steps and decisions used to address and manage alleged Misconduct and Serious Misconduct.
Personal Device	A non-University owned and/or provided device that is used to access IT Services or University Information. This includes, but not limited to, smartphones, tablets or equivalent devices, laptop and desktop computers, Internet of Things devices, radio communication devices, peripheral devices and portable storage devices.
Personal Use	Use of Digital Resources that is not for the purposes of University Activity. That is studying and/or working at the University, and/or taking part in recreation or other activities organised by the Guild and/or University; and/or any services and/or performance of official duties of the University, regardless of location.
Policy	An approved instrument registered on the UWA Policy Library that expresses principles to regulate behaviour and practice.
Regulated Digital Content	Material, including but not limited to — (1). in breach of intellectual property or copyright; (2). malware; (3). unauthorised software; (4). in violation of academic integrity requirements; (5). unlawfully obtained; (6). containing child exploitation material; (7). advocates for a terrorist act; (8). detailed instruction or promotion in crime or violence; (9). instruction in paedophilic activity; (10). gratuitous, exploitative and offensive depictions of violence or sexual violence; (11). has been classified RC or X 18+ by the Classification Board.
Risk Appetite	The degree of risk that the University is willing to accept in pursuit of its strategic and operational objectives. It articulates the boundaries for risk taking, enables a consistent approach to risk taking across the University and helps find the balance between risk taking and risk avoidance.
Technical System Owner	A senior UWA employee responsible for the day-to-day management, maintenance and administration of a University Digital Resource as per agreed standards, policies and expectations of the Business System Owner of the Digital Resource.
Third Party	Any individual other than a Student or Employee, or any organisation that is not part of the University Group or affiliated bodies.
University	Is The University of Western Australia, and any and all subsidiary or associated entities.
University Activity	Studying and/or working at the University, and/or taking part in recreation or other activities organised by the Guild and/or University; and/or any services and/or performance of official duties of the University, regardless of location.

Term	Definition
University Community	All individuals who engage in University activity and/or use University property.
University Information Management System	Any system used for creating, capturing, processing, storing and/or sharing University Information, endorsed by University IT.
University Officer	Any of the following — (1). Senate Members and members of committees of the Senate (2). Employees (3). Clinical Academics (4). Contractors (5). Honorary, Adjunct, Clinical (excluding Clinical Academics) or Emeritus Appointments (6). Committee Members (7). individuals acting in the name of the University on a Financial Commitment.
University Property	Tangible and non-tangible things, belonging to, or contracted to the University or members of the University Community, including campuses, facilities and services.

3 Scope

- 3.1 The scope of this Policy applies to –
- (a) the entire University; and
 - (b) Controlled Entities and affiliated and partner organisations when utilising University Digital Resources.
- 3.2 This Policy applies to the entire University Community with formal responsibilities for procuring, implementing, administering, decommissioning or overseeing University Digital Resources.

4 Cyber Security Governance

- 4.1 The University maintains and continually improves a Cyber Security Framework that provides detailed minimum requirements for effective protection of University Digital Resources.
- 4.2 The Cyber Security Framework adopts a risk-based approach, with control requirements proportionate to the criticality of Digital Resources, in line with the UWA Risk Management Framework and Risk Appetite Statement. The Cyber Security Team establishes Cyber Security Risk Ratings for Digital Information Resources to enable resource prioritisation.
- 4.3 Enabling regulatory compliance and international recognition, the Cyber Security Framework reflects recommended better practices of the:
- (a) Western Australian Cyber Security Policy;
 - (b) Australian Signals Directorate Information Security Manual; and
 - (c) USA National Institute of Standards and Technology Cybersecurity Framework.
- 4.4 The University does not support the payment of ransoms. Any ransom demands related to cyber security incidents will be referred to the Western Australian Government and Police Force.

5 Cyber Security Roles and Responsibilities

- 5.1 Senate is responsible for —
- (a) overseeing and monitoring the assessment and management of Cyber Security risk across the University;
 - (b) setting the University's Cyber Security Risk Appetite and tolerance levels; and
 - (c) reviewing and approving the Cyber Security Policy as an institutional Policy of the University.
- 5.2 Executive Members are responsible for —

- (a) overall Cyber Security risk management and compliance across the University;
- (b) overseeing the allocation of resources to enable effective Cyber Security risk management and delivery of the Cyber Security Strategy;
- (c) promoting an appropriate Cyber Security culture across the University;
- (d) endorsing the strategic direction of Cyber Security;
- (e) assigning University-wide management responsibilities for Cyber Security; and
- (f) governing the implementation of adequate Cyber Security measures through University Committees.

5.3 Business System Owners are responsible for —

- (a) understanding the Cyber Security Risk Rating and related requirements of University Digital Resources within their area of responsibility;
- (b) ensuring that University Digital Resources are not acquired or implemented within their area of responsibility without prior input and authorisation by University IT;
- (c) allocating sufficient resources and support for their University Digital Resources to have all controls designed, acquired, implemented, operated, and maintained in accordance with the Cyber Security Framework;
- (d) identifying, reporting, owning and managing Cyber Security risks associated with their University Digital Resources and related third party suppliers, vendors and partners;
- (e) supporting the University IT Cyber Security Function in delivering the Cyber Security Strategy and when conducting Cyber Security reviews; and
- (f) where deemed necessary, formally assign management of University Digital Resources within their area of responsibility to Technical System Owners or retain associated responsibilities.

5.4 Technical System Owners are responsible for —

- (a) understanding the Cyber Security Risk Rating and related requirements of Digital Resources within their area of responsibility;
- (b) familiarising themselves with all Cyber Security policies, standards and guidelines applicable to their Digital Resources;
- (c) ensuring that their Digital Resources have all controls designed, acquired, implemented, operated, and maintained in accordance with the Cyber Security Framework;
- (d) confirming the effectiveness of Cyber Security controls applicable to their Digital Resources;
- (e) identifying, reporting, owning and managing Cyber Security risks associated with their Digital Resources, third party suppliers, vendors and partners; and
- (f) supporting the University IT Cyber Security Function in delivering the Cyber Security Strategy and when conducting Cyber Security reviews.

5.5 Chief Information Officer will be responsible for —

- (a) acting as Business System Owner for shared University Digital Resources that are not directly attributable to a single business capability;
- (b) allocating sufficient resources and support for managing Cyber Security risks;
- (c) suspending access to University Digital Resources by members of the University Community where such access —
 - i. risks causing a major Cyber Security incident; or
 - ii. constitute unauthorised non-compliance with requirements of the Cyber Security Framework.
- (d) taking steps to cease any University Digital Resource operation or activity that —
 - i. risks causing a major Cyber Security incident; or
 - ii. constitute unauthorised non-compliance with requirements of the Cyber Security Framework.

5.6 The University IT Cyber Security Team is responsible for —

- (a) maintaining and communicating requirements of the Cyber Security Framework;
- (b) setting and delivery of the Cyber Security Strategy;
- (c) recommending appropriate technical controls to owners of University Digital Resources;
- (d) providing Cyber Security advice, training and awareness, to support the University Community in safeguarding University Digital Resources and ensuring compliance;
- (e) obtaining assurance over the effectiveness of Cyber Security controls;
- (f) supporting Executive Members, Business System Owners and Technical System Owners in identifying and managing Cyber Security risks;
- (g) conducting Cyber Security reviews;
- (h) liaising with state and federal agencies on Cyber Security matters; and
- (i) managing Cyber Security incidents.

- 5.7 The University Information Governance Team is responsible for —
- (a) identifying and maintaining information governance roles, including Business System Ownership as endorsed by Executive Members;
 - (b) overseeing the design and effectiveness of information protection requirements; and
 - (c) providing information privacy, protection and retention advice, training and awareness.

6 Non-Compliance

- 6.1 Any non-compliance with requirements of the Cyber Security Framework must be reported to the University IT Cyber Security Team.
- 6.2 Authorised and time-limited control exemption may be granted by the University IT Cyber Security Function following risk assessment.
- 6.3 Material breaches or negligence in the performance of responsibilities set out by the Cyber Security Framework may be considered as Misconduct and addressed through formal Misconduct Process as defined in the Managing Employee Misconduct Policy.

Legislative Context

Relevant Legislation or Regulations
<i>University of Western Australia Act 1911 (WA)</i>
<i>University of Western Australia Statute (2020)</i>
Western Australian Cyber Security Policy
Australian Signals Directorate Information Security Manual
USA National Institute of Standards and Technology Cybersecurity Framework

End