Cyber Security Policy

Version	Approved by	Approval date	Effective date	Next full review
4.0				

Policy Statement	
Purpose	This policy sets out the principles for ensuring that UNSW Information Resources (Information Services and Information Assets) that hold UNSW digital information are appropriately protected. UNSW must ensure that: 1. Accountability and responsibility are allocated for the governance and management of cyber security. 2. UNSW Information Resources are identified and assessed for cyber security risk and appropriately protected from cyber security events. 3. Cyber security events are detected and responded to in a timely manner. 4. UNSW Information Resources recover from a cyber security incident in a secure and timely manner.
Scope	This policy applies to: a) All users of UNSW Information Resources, including but not limited to staff (including casuals), students, consultants, contractors, third parties, agency staff, alumni, associates and honoraries, conjoint appointments, affiliates, collaborative researchers, and visitors to the University. b) All University owned, controlled, or leased locations where UNSW Information Resources are located or used. c) All UNSW digital information. d) All Information Resources that store, process or transmit UNSW digital information, whether owned by UNSW, an external service provider, or user. e) All devices connected to a UNSW network or used to access UNSW Information Resources.

Policy Provisions

1. Cyber security principles

1.1. The existence, ownership, value, and cyber security requirements of critical UNSW Information Resources must be determined and documented.

1.2. Cyber security risks associated with Information Resources that store, process, or transmit UNSW digital information must be identified, documented, and managed prior to use, and continuously throughout their operational life.

1.3. UNSW Information Resources must be designed, deployed, maintained, and decommissioned according to their cyber security risk and any associated control requirements.

1.4. All access to UNSW Information Resources must be authorised, restricted based on need, and periodically reviewed.

1.5. Cyber security events and anomalous activities must be detected, collected, correlated, and analysed in a timely manner.

1.6. Cyber security incidents must be identified, reported, contained, eradicated, and recovered from, in a timely manner.

1.7. Business continuity and disaster recovery plans must be developed, documented, and enacted when required and must not increase cyber security risk.

1.8. UNSW Information Resources must be managed in accordance with all applicable laws and regulations (including those relating to critical infrastructure and mandatory cyber incident reporting).

2. Cyber Security Risk Management Framework

The Cyber Security Policy in conjunction with the Cyber Security Standards (shown in red in Figure 1 below), applicable Guidelines and other related UNSW policies and standards form a Cyber Security Risk Management Framework that sets the intent and establishes the direction and principles for the protection of UNSW Information Resources against cyber security threats.

The Cyber Security Risk Management Framework

a) takes into consideration

- the cyber security threat environment determined through periodic independent risk assessments, government, sector and industry forums, and targeted internal technical assessments.
- the federated nature of UNSW and its technology environment, as well as the higher education need for academic freedom.

b) defines three levels of cyber security risk rating for a UNSW information resource, derived from inherent risk.

c) adopts a “minimum defensible baseline” of cyber security controls for low and medium cyber security risk rating and additional “elevated” controls for Information Resources with a high cyber security risk rating.

The **Cyber Security Risk Management Framework** consists of the following documents:

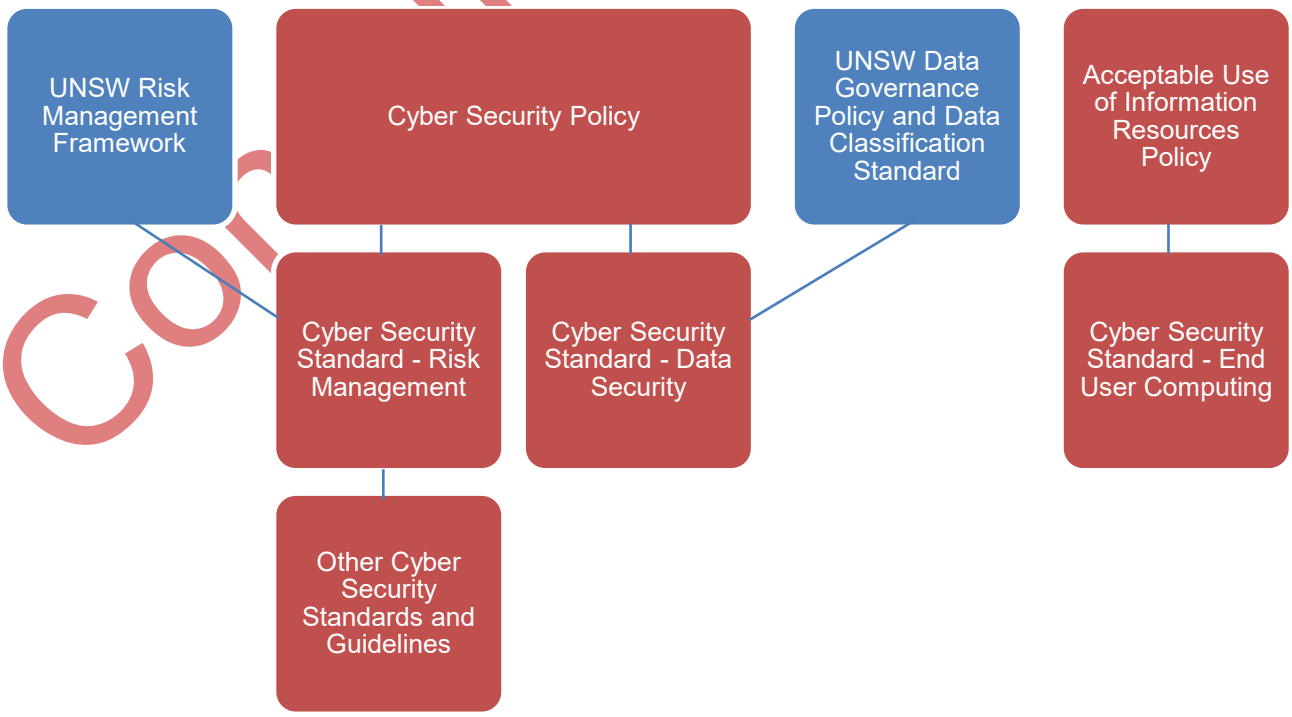

Figure 1.

The *Cyber Security Standard – Risk Management* defines

a) the process for identifying, assessing, monitoring, and reporting cyber security risks and the process for addressing control deficiencies through control improvements.

b) the minimum cyber security controls applicable to an Information Resource for each cyber security rating.

The Standard is used when a person needs to design, build, acquire, operate, or maintain an UNSW Information Resource, and has sections related to the following Information Resource types and whether they are delivered by a UNSW entity or non-UNSW entity:

- Applications (including SaaS and mobile).
- Endpoints (workstations, laptops, mobiles, IoT and VDI).
- Server instances (including virtual machines, IaaS and PaaS (including containers and serverless)).
- Data Services and Storage Services (including PaaS).
- Cyber Security Services including SaaS and PaaS.
- Networks and Network Devices (including SDN and Cloud).
- Hosting Platforms (including ESX hosts, data centres, IaaS, and PaaS).

The *Cyber Security Standard – End User Computing* – defines the additional cyber security controls applicable to personal devices and UNSWIT owned endpoints.

The *Cyber Security Standard – Data Security* defines the controls related to data handling, encryption and key management that are applicable to each cyber security risk rating.

Other Cyber Security Standards and Guidelines provide technical and procedural requirements for each of the controls in the *Cyber Security Standard – Risk Management.*

3. Roles and responsibilities

3.1. The University Council, Risk Committee and Information Technology Committee provide oversight, risk management and risk control mechanisms for cyber security. These are supported by decisions made by Management Board, Senior Leadership Team (SLT) and the Vice-President, Finance & Operations who oversee cyber security strategy, funding, and resourcing.

3.2. The *UNSW Risk Management Framework* defines UNSW functions and their accountabilities for risk including cyber security risk.

3.3. The Chief Information Officer has UNSW-wide authority to:

a) establish mandatory Cyber Security Standards and determine the consultation process for such Standards (in accordance with the *UNSW Policy Framework Policy*), including the authority to expedite Standards to facilitate the management of a high or extreme cyber security risks.

b) compel work, use of equipment, or an operation, ceases due to identified or perceived cyber security risk (or a major incident) caused by that work, operation, or activity.

c) assign UNSW wide management responsibilities for cyber security.

3.4. The Chief Information Security Officer has UNSW-wide accountability and authority for:

a) supporting UNSW management in identification, assessment, treatment, and reporting of cyber security risk.

b) supporting UNSW management assurance over controls and attestation of compliance with the Cyber Security Framework.

c) conducting cyber security reviews.

d) providing cyber security advice and awareness, to improve the ability of UNSW users to comply with the requirements of the Cyber Security Framework and respond to cyber security threats.

e) the design, implementation and oversight of the UNSW cyber security strategy, plans, programs, capabilities, and controls.

f) the design, implementation, and assignment of cyber security training.

g) managing cyber security incidents on behalf of UNSW, in accordance with the Cyber Security Standard – Incident Management, and Major Incident Management Process including the authority to contain, eradicate and rectify incidents within any area of UNSW.

h) recommending Cyber Security Standards to the Chief Information Officer.

i) ensuring the Cyber Security Policy and Cyber Security Standards conform with the requirements of any relevant International Standard and its defined scope within UNSW.

3.5. The Chief Data and Insights Officer is accountable for Data and Information Governance within UNSW including the *Data Classification Standard* and is jointly responsible for the *Cyber Security Standard - Data Security*.

3.6. Deans, Head of Schools, Heads of Research Centres, and Heads of Administrative Units are accountable for:

a) identifying and effectively managing cyber security risk within their area of accountability, including where necessary obtaining guidance and support from the Chief Information Security Officer.

b) promoting an appropriate cyber security risk management culture within their area of accountability, including by requiring all staff (including casual staff and contractors) to participate in any cyber security awareness training specified by the Chief Information Security Officer.

c) assigning Business Owners for UNSW Information Resources within their area of accountability that have a high cyber security risk rating.

d) identifying and reporting UNSW Information Resources with a high cyber security risk rating to UNSWIT in accordance with the *Cyber Security Standard – Risk Management.*

e) ensuring compliance with all applicable cyber security laws and regulations, including those relating to critical infrastructure and mandatory data breach reporting, within their area of accountability.

f) attesting annually to the compliance of high cyber security risk rated UNSW Information Resources within their area of accountability, to the Cyber Security Policy Framework, in accordance with the *Cyber Security Standard – Risk Management.*

3.7. Business Owners are accountable for:

a) ensuring all UNSW Information Resources within their area of accountability have:

- a cyber security risk rating determined in accordance with the *Cyber Security Standard – Risk Management*.
- controls designed, built, operated, and maintained in accordance with the requirements in the *Cyber Security Standard – Risk Management*, and where necessary guidance and support from the Chief Information Security Officer or delegate.

b) overseeing all access to UNSW Information Resources within their area of accountability in accordance with the *Cyber Security Standard – Access Control.*

c) identifying and managing cyber security risks associated with UNSW Information Resources and third-party service providers within their area of accountability.

d) providing support for and participating in, any cyber security reviews conducted by the Chief Information Security Officer.

e) ensuring Information Resources within their area of accountability are compliant with all applicable cyber security laws and regulations, including those relating to critical infrastructure.

f) reporting and escalating identified cyber security risks in accordance with the *Cyber Security Standard – Risk Management.*

3.8. Business Owners may assign management of a UNSW Information Service or group of UNSW Information Services to an Information Service Owner (or System Owner) or retain the associated responsibilities within this policy and the Cyber Security Standards.

3.9. All users are responsible for:

a) ensuring any Information Resource they develop, acquire, or in any way control, is classified, designed, built, operated, and maintained (or in any way changed) in accordance with the *Cyber Security Standard – Risk Management,* and relevant *Cyber Security Standards.*

b) ensuring that all digital information within their area of accountability is classified in accordance with the *Data Classification Standard* and handled in accordance with the *Cyber Security Standard – Data Security.*

c) ensuring any personal device used to store, process, or transmit UNSW digital information, or connect to a UNSW Information Resource complies with the *Cyber Security Standard – End User Computing.*

d) participating in cyber security training and awareness activities provided by UNSW and following cyber security guidance provided by UNSW.

4. Reporting cyber security events

4.1. Any person noticing a cyber security event must report it as soon as possible to the UNSWIT Service Centre.

4.2. Users must not:

a) perform any action to manage or address a cyber security event unless authorised or explicitly instructed by the UNSW IT Service Centre or UNSW IT Cyber Security Team.

b) disclose information relevant to any cyber security event other than in accordance with the *Cyber Security Standards.*

5. Non-compliance

5.1. Any non-compliance with this policy or the Cyber Security Standards must be approved in accordance with the *Cyber Security Standard – Framework Exemption*, including a mandatory risk assessment and agreed compensating controls.

5.2. In the event of unauthorised non-compliance with this policy or the Cyber Security Standards (as determined by the Chief Information Security Officer), UNSW may:

a) withdraw or restrict a user's access to UNSW Information Resources.

b) commence disciplinary action:

- for staff: disciplinary action in accordance with the *UNSW Code of Conduct* and the applicable University of New South Wales Enterprise Agreement, which may include termination of employment.
- for students: action for misconduct under the *Student Code of Conduct* and associated *Student Misconduct Procedure*, which may include exclusion from the University.
- for non-staff members, commensurate action, which may include termination or non-renewal of their appointment or contract.

Accountabilities	
Responsible Officer	Vice-President, Operations
Contact Officer	Chief Information Officer
Supporting Information	
Legislative Compliance	This Standard supports the University's compliance with the following legislation: *Privacy and Personal Information Protection Act 1998 (NSW)* *Security of Critical Infrastructure Act 2018 (Cth)* *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (Cth)*
Supporting Documents	Cyber Security Standard – Risk Management Cyber Security Standard – Data Security Cyber Security Standard – End User Computing Cyber Security Standard – Access Control Cyber Security Standard – Incident Management Cyber Security Standard – Framework Exemption
Related Documents	Acceptable Use of UNSW Information Resources Policy Data Governance Policy Data Classification Standard Risk Management Framework Code of Conduct Student Code of Conduct
Superseded Documents	IT Security Policy, version 3.0 effective 7 June 2016
File Number	[For Governance Use]

Definitions and Acronyms	
	For additional definitions, refer to the *Cyber Security Standards – Glossary*.
Area of accountability	means any area where a person has strategic, structural, operational or financial control over a UNSW Information resource within that area.
Business Owner	means a person with primary accountability for the business or technology functions provided by one or more UNSW Information Resources, including any associated cyber security risk. Note: The Business Owner of an Information Service may be in the UNSWIT unit or any other organisational unit.
Cyber security	means the measures used to protect the confidentiality, integrity and availability of information resources.
Cyber security control	means any management, operational or technical measure (including safeguards or countermeasures) put in place for cyber security.
Cyber security event	means an occurrence of an information resource state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.
Cyber security incident	means a cyber security event that has been assessed to have a potential adverse impact on the confidentiality, integrity, or availability of an Information resource.

Cyber security review	means review, assess, and audit to determine compliance with the Cyber Security Risk Management Framework or any other policy, legislative, compliance, or contractual requirements.
Cyber security risk	means the risk of a cyber security event or incident.
Data	means the representation of facts, concepts, or instructions in a formalised (consistent and agreed) manner suitable for communication, interpretation or processing by human or automatic means. Typically comprised of numbers, words or images. The format and presentation of data may vary with the context in which it is used. Data is not Information until it is used in a particular context for a particular purpose. In the context of this Standard this term includes all institutional data including research, administrative, and learning and teaching artefacts.
Digital information	means information that is in a digital or electronic form and is stored, processed or transmitted within an Information service or Information asset.
High cyber security risk rated	means a rating of high, assessed using the *Cyber Security Standard – Risk Management.*
Information	means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual.
Information asset	means any hardware (including IoT devices), software, cloud-based services, communication devices, networks, that is stores, processes or transmits UNSW digital information.
Information asset owner	means the person who is responsible for the day-to-day operation and protection of a UNSW Information Asset.
Information resource	means any Information service, Information asset or digital information.
Information service	means any business or technology function using one or more Information assets including but not limited to: (a) application systems (including software-as-a-service); and (b) IT infrastructure services such as operating systems, databases, voice and data telecommunications services, network services, media services, file and print services, and email services. Also known as ICT service, IT service, or system.
Information service Owner	means the person responsible for defining, operating, measuring, and improving a UNSW Information service and associated cyber security controls. Also known as “System Owner” or “IT service owner”.
Personal device	means a non-University owned or provided device that is used by an individual to access, store, process or transmit University data or digital information. This includes desktops and laptop computers, personal digital assistants, tablets, smartphones, mobile PIN pads, radio communication devices, USB keys or any form of portable storage device.
UNSW digital Information	means digital information that is owned by UNSW.
UNSW Information Asset	means any Information Asset that is owned, leased, operated, or managed by any UNSW organisational unit, or provided by any UNSW organisational unit to users.
UNSW Information Resource	means any Information Service that is owned, leased, operated, or managed by any UNSW organisational unit, or provided by any UNSW organisational unit to users.
UNSW Information Service	means any Information Service that is owned, leased, operated, or managed by any UNSW organisational unit, or provided by any UNSW organisational unit to users.
User	means a user of any UNSW Information Resource including but not limited to staff (including casuals), students, consultants, contractors, third parties, agency staff, alumni, associates and honoraries, conjoint appointments, affiliates, collaborative researchers, and visitors to UNSW, including any use before, during and after any formal relationship exists.

Revision History				
Version	**Approved by**	**Approval date**	**Effective date**	**Sections modified**
1.0	VCAC			
2.0	Vice-Chancellor	18 February 2004	1 March 2004	Full review
2.1	Head, Governance Support	18 February 2010	18 February 2010	Sections 3.1, 5, 12
3.0	President & Vice-Chancellor	7 June 2016	7 June 2016	Full review
4.0	Vice-Chancellor			Full review and rename