Cyber Security Policy

Version	Approved by	Approval date	Effective date	Next full review
4.0	Vice-Chancellor	18 November 2022	18 November 2022	November 2025

Policy Statement	
Purpose	This policy sets out the principles for ensuring that UNSW Information Resources (UNSW Information Services and UNSW Information Assets) that hold UNSW Digital Information are appropriately protected. UNSW must ensure that: a) accountability and responsibility are allocated for the governance and management of cyber security. b) UNSW Information Resources are identified and assessed for cyber security risk and appropriately protected from cyber security events. c) cyber security events are detected and responded to in a timely manner. d) UNSW Information Resources recover from cyber security incidents 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 UNSW Information Resources. 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 UNSW 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 is 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, and the need for academic freedom.

b) defines three levels of Cyber Security Risk Rating for UNSW Information Resources, derived from inherent risk.

c) adopts a “minimum defensible baseline” of cyber security controls for UNSW Information Resources with a Low and Medium Cyber Security Risk Rating, and additional “elevated” controls for UNSW Information Resources with a High Cyber Security Risk Rating.

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

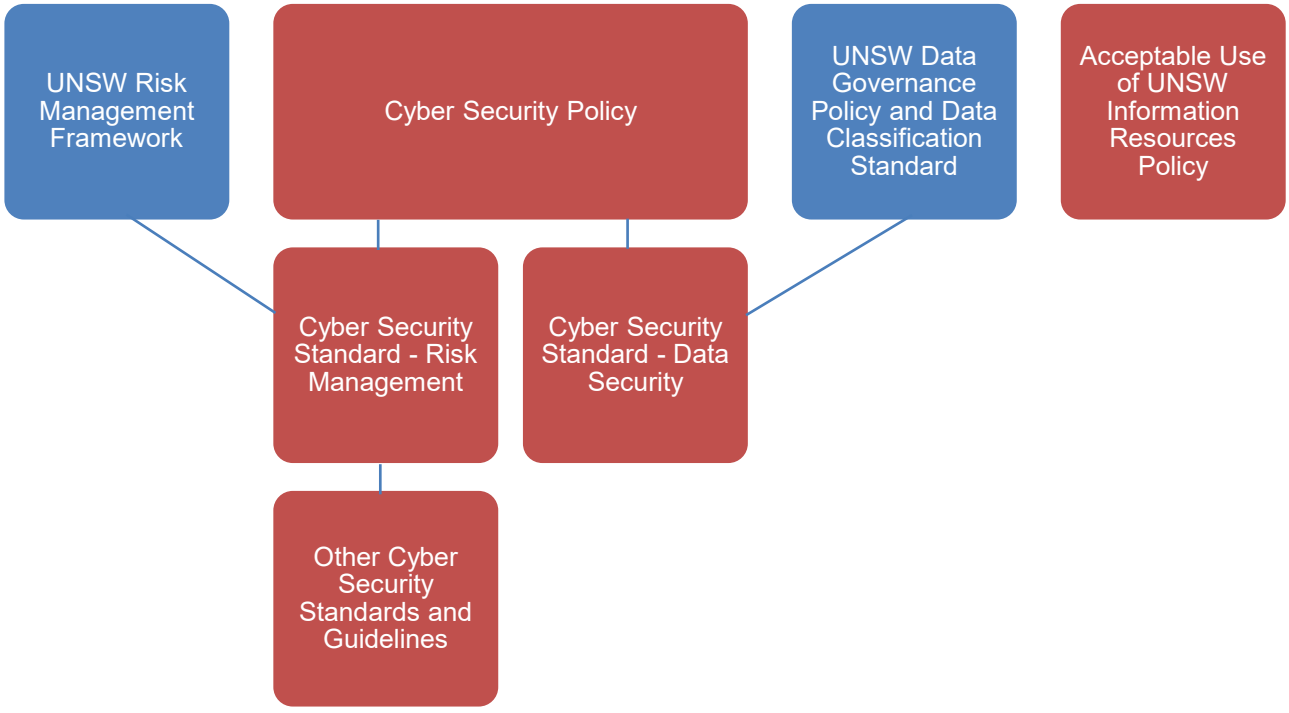

Figure 1.

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 UNSW Information Resource for each Cyber Security Risk Rating.

The Standard is used when a person needs to design, build, acquire, operate, or maintain a UNSW Information Resource, and has sections related to the following UNSW 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 – Data Security* defines the controls related to data handling, encryption, and key management.

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 management including cyber security risk.

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

a) establish mandatory Cyber Security Standards and Guidelines and determine the consultation process (in accordance with the *UNSW Policy Framework Policy*), including the authority to expedite changes to facilitate the management of 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 risks.

b) supporting UNSW management assurance over controls and attestation of compliance with the Cyber Security Risk Management 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 Risk Management Framework and respond to cyber security threats.

e) the design, implementation, and oversight of 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 Plan,* including the authority to contain, eradicate and rectify incidents within any area of UNSW.

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

i) ensuring the Cyber Security Policy, Cyber Security Standards and Cyber Security Guidelines 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. Deputy Vice-Chancellors, Vice-Presidents, Deans, and the Rector UNSW Canberra are accountable for the:

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

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

c) assignment of Business Owners for all UNSW Information Resources within their area of accountability.

d) identification and reporting UNSW Information Resources with a High Cyber Security Risk Rating to UNSW IT in accordance with the *Cyber Security Standard – Risk Management*.

e) 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) annual attestation of compliance to the Cyber Security Risk Management Framework, for High Cyber Security Risk Rated UNSW Information Resources within their area of accountability, in accordance with the *Cyber Security Standard – Risk Management*, and where necessary obtaining guidance and support from the Chief Information Security Officer.

3.7. Business Owners are responsible for:

a) ensuring all UNSW Information Resources within their area of responsibility 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 responsibility in accordance with the *Cyber Security Standard – Identity and Access Management.*

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

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

e) ensuring UNSW Information Resources within their area of responsibility 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 delegate responsibility for a UNSW Information Resource or group of UNSW Information Resources to an Information Service Owner (or System Owner) or an Information Asset Owner.

3.9. All users are responsible for:

a) ensuring any UNSW 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 other relevant *Cyber Security Standards.*

b) ensuring that all UNSW 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 Standards.*

d) completing 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 potential or actual cyber security incident must report it as soon as possible to the UNSW IT Service Centre or UNSW IT Cyber Security Team.

5. Non-compliance

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

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) *Copyright Act 1968* (Cth)
Supporting Documents	Cyber Security Standard – Risk Management Cyber Security Standard – Data Security Cyber Security Standard – Identity and Access Management 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 Data Breach Policy Data Breach Management Procedure Research Data Governance & Materials Handling Policy Research - Handling Research Material & Data Procedure
Superseded Documents	IT Security Policy, version 3.0, effective 7 June 2016
File Number	2022/069864

Definitions and Acronyms	
Area of accountability	means any area where a person has strategic, structural, operational or financial control over a UNSW Information Resource within that area.
Area of responsibility	means any area where a person has a direct or delegated responsibility to manage a UNSW Information Resource based on a contractual, verbal, or implied agreement.
Business Owner	means a person with primary responsibility 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 UNSW Information Resource may be in the UNSW IT unit or any other organisational unit.
Cyber security	means the measures used to protect the confidentiality, integrity and availability of UNSW Information Resources.
Cyber security control	means any management, operational or technical measure (including safeguards or countermeasures) put in place for cyber security objectives.

Cyber security event	means an occurrence of an UNSW 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 (in accordance with the Cyber Security Standards) to have a potential adverse impact on the confidentiality, integrity, or availability of an UNSW 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 Policy 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, or network.
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, administrative tools, process automation tools, 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 an UNSW Information Service and associated cyber security controls. Also known as “System Owner” or “IT service owner”.
Infrastructure as a Service (IaaS)	means a type of cloud computing service that provides the capability to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g. host firewalls).
Internet of Things (IoT)	means user or industrial devices that are connected to the internet. IoT devices include sensors, controllers, and household appliances or a network of devices that contain the hardware, software, firmware, and actuators that allow the devices to connect, interact, and freely exchange data and information.
Personal device	means a non-University owned or provided device that is used by an individual to access, store, process or transmit UNSW 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.

Platform as a Service (PaaS)	means a cloud environment where the capability is provided to the consumer to deploy onto the cloud infrastructure, consumer-created or acquired applications, created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and (in some circumstances) configuration settings for the application-hosting environment.
Software as a Service (SaaS)	means an application running on a cloud infrastructure. The application is accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Software-Defined Network (SDN)	means an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network. This model differs from that of traditional networks, which use dedicated hardware devices (i.e., routers and switches) to control network traffic. SDN can create and control a virtual network – or control a traditional hardware – via software.
UNSW Entity	means a university-owned, controlled, or fully managed entity, Examples include, but are not limited to, Business Units, faculties, divisions etc.
UNSW Digital Information	means Digital Information that is owned by UNSW or under the custody of 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 Resource that is owned, leased, operated, or managed by any UNSW organisational unit, or research undertaking, 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.
Virtual Desktop Infrastructure (VDI)	means is a full, thick-client user environment run as a virtual machine on a server and accessed remotely. VDI implementations comprise server virtualization software to host desktop software (as a server workload); brokering/session management software to connect users to their desktop environments; tools for managing the provisioning and maintenance (for example, reimages) of the virtual desktop software stack.

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	18 November 2022	18 November 2022	Full review and new title