CYBER SECURITY POLICY 2019

The Vice-Chancellor as delegate of the Senate of the University of Sydney, as the governing authority of the University of Sydney, by resolution adopts the following policy.

Dated: 15 July 2019

Last amended:

Signature:

Position: Vice Chancellor

CONTENTS

1 Name of policy

This is the Cyber Security Policy 2019.

2 Commencement

This policy commences on 1 August 2019.

3 Policy is binding

Except to the extent that a contrary intention is expressed, this policy binds the University, staff, students and affiliates.

4 Statement of intent

This policy:

(a) sets out the principles for protecting the confidentiality, integrity and availability of the University's information and communications technology resources;

(b) establishes compliance requirements for cyber security;

(c) allocates responsibilities for the governance and management of cyber security;

(d) establishes a framework for managing cyber security; and

(e) supports the University's values of respect and integrity.

Note: See the *University's Strategic Plan 2016-20*.

5 Application

This policy applies to:

(a) the University, its staff, affiliates and students;

(b) any visitor, including any contractor, using or accessing the University's ICT resources; and

(c) all digital information and ICT resources.

6 Definitions

In this policy:

business system owner	means a person with primary accountability for the business or technology functions provided by one or more University ICT resources, including any associated cyber security risk (also known as ICT Service Sponsors).
cyber security	means the measures taken to: • protect ICT, electronic systems, networks, devices and digital information from compromise or interruption; and • facilitate rapid and effective detection and response to any compromise or interruption.
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 event relating to any cyber security control protecting University ICT resources from compromise or interruption. This includes internal or external acts which: • may bypass or contravene applicable controls, policies or procedures; or • may potentially compromise the confidentiality, integrity or availability of ICT resources.

cyber security incident	means a cyber security event that may, in the opinion of the Head of Cyber Security, adversely impact the confidentiality, integrity or availability of a University ICT resource.
digital information	means information that is in a digital or electronic form and is stored, processed or transmitted within an ICT service or ICT asset.
ICT	means information and communications technology within the remit of any University organisational unit.
ICT asset	means hardware, software, cloud-based services, communication devices, data centres, or networks that are owned by the University or provided by the University to users.
ICT resource	means any ICT service, ICT asset or digital information.
ICT service	means any business or technology function provided using one or more ICT assets, including, but not limited to: • application systems (including software-as-a-service); and • ICT infrastructure services such as operating systems, databases, voice and data telecommunications services, network services, media services, file and print services, and email services.
Organisational Resilience Framework	has the meaning provided in the *Risk Management Policy 2019* which at the date of this policy is: the document or set of documents required by clause 10 of the *Risk Management Policy 2019*
organisational unit	means any of the following: • faculty; • University school; • a portfolio or professional services unit controlled by a Principal Officer; • a level 4 centre, as described in the *Centres and Collaborative Networks Policy 2017*.
Principal Officer	has the meaning provided in the *University of Sydney (Delegations of Authority – Administrative Functions) Rule 2016* which at the date of this policy is: means a collective reference to: Vice-Chancellor and Principal; Deputy Vice-Chancellor; Vice-Principal; General Counsel; Director, University Libraries.
procedures	means the *Cyber Security Procedures 2019*

risk	has the meaning provided in the *Risk Management Policy 201*9, , which at the date of this policy is: the effect of uncertainty on objectives.
Risk Management Framework	has the meaning provided in the *Risk Management Policy 201*9 which at the date of this policy is: the set of documents required by clause 9 of the *Risk Management Policy 2019*, which provide the foundation and arrangements for designing, implementing, monitoring, reviewing and continually improving risk management at the University.
risk owner	has the meaning provided in the *Risk Management Policy 2019*, which is: the role recorded against a particular risk in a risk register to discharge the responsibilities specified in clause 11 of the *Risk Management Policy 201*9.
technical standards	means the mandatory standards for specific ICT activities determined by the Chief Information Officer under clauses 8 and 10 of this policy.
technology risk owner	means any person to whom a cyber security related risk is assigned in any organisational unit local risk register.
University Executive	means the management committee of that name which comprises members of the University's senior leadership.

7 Cyber security principles

(1) Cyber security risks to individuals, the University's operations and its ICT resources must be:

(a) identified and assessed; and

(b) managed with an appropriate risk treatment plan

in accordance with the Risk Management Framework.

(2) The University's ICT resources and external environment must be appropriately monitored in order to detect cyber security events.

(3) Cyber security response and recovery plans must be:

(a) maintained;

(b) tested;

(c) coordinated with internal and external stakeholders; and

(d) periodically improved;

in accordance with the Organisational Resilience Framework

(4) The effectiveness of the University's management of cyber security risks must be regularly assessed and improved.

(5) All access to a University ICT service or ICT asset must be:

(a) authorised;

(b) restricted on the basis of need; and

(c) periodically verified.

(6) All users have a shared responsibility for maintaining the security of University ICT resources that they use or manage.

(7) Users must not communicate the University's cyber security risks, controls, events and incidents outside the University except where required or authorised to do so by law, University policy or procedures, or applicable technical standards.

8 Technical standards

(1) The Chief Information Officer may determine mandatory technical standards for specific ICT activities and operations.

(2) The technical standards must be published on the University Intranet.

9 Cyber security framework

The University's cyber security framework consists of:

(a) this policy;

(b) the procedures; and

(c) the technical standards

10 Roles and responsibilities

(1) **Senate** is accountable for the overall management of cyber security risk at the University. It is also responsible for:

(a) setting the University's cyber security risk appetite and tolerance levels; and

(b) considering and responding appropriately to reports about the University's cyber security risks and their management.

(2) **The Vice-Chancellor** is responsible for:

(a) overall cyber security risk management and compliance across the University;

(b) promoting an appropriate cyber security risk management culture across the University; and

(c) overseeing the allocation of resources to enable effective cyber security risk management.

(3) **The Provost** is responsible for:

(a) promoting an appropriate cyber security risk management culture across the University;

(b) receiving and acting on reports of cyber security risk management issues from faculties and University schools; and

(c) raising cyber security risk management issues with the Vice-Chancellor and University Executive where appropriate.

(4) The **University Executive** is responsible for

(a) overseeing and advising on the application of the Risk Management Framework to the University.

(b) considering and responding appropriately to reports about the University's cyber security risk and its management.

(5) The **University Executive Operations Committee** is responsible for:

(a) endorsing the strategic direction and governance of cyber security measures;

(b) endorsing cyber security related purchases and acquisitions; and

(c) overseeing and advising on the application of the Risk Management Framework to cyber security; and

(d) considering and responding appropriately to reports about the University's cyber security risk and its management.

(6) **The Vice-Principal (Operations)** is responsible for overseeing development of, and approving, the University's cyber security strategy.

(7) **The Chief Information Officer** is responsible for:

(a) managing cyber security risks within the Information and Communications Technology unit, including assigning risk owners;

(b) managing cyber security funding;

(c) assigning management responsibility for cyber security; and

(d) determining technical standards.

(8) The **Head of Cyber Security** is responsible for:

(a) overseeing the design and implementation of the University's cyber security strategy and capabilities;

(b) reviewing and reporting on the management of cyber security risks;

(c) reviewing and reporting on the operation of cyber security controls within the University's organisational units;

(d) determining the cyber security controls and cyber security related ICT Services required to support:

(i) the University's cyber security strategy; and

(ii) the University's strategic priorities, legal and contractual obligations, policies and procedures;

(e) recommending appropriate technical standards to the Chief Information Officer;

(f) administering technical standards to implement the required cyber security controls and services; and

(g) reporting on the University's cyber security risks as required, including to Senate, the Vice Chancellor, the University Executive and relevant committees.

(9) **Heads of organisational units** are responsible for:

(a) identifying and effectively managing cyber security risk;

(b) promoting an appropriate cyber security risk management culture within their unit;

(c) assigning technology risk owners for cyber security risks within their local risk register;

(d) assigning one or more business systems owners within their unit, in consultation with the Chief Information Officer or Head of Cyber Security; and

(e) reporting and escalating identified cyber security risks in accordance with the Risk Management Framework, and applicable technical standards.

(10) **Technology risk owners** and **business system owners** are responsible for:

(a) complying with this policy, the procedures, and applicable technical standards;

(b) managing cyber security risks associated with ICT resources and third party service providers under their remit;

(c) requiring the development, implementation and maintenance of any necessary cyber security capabilities or cyber security controls for ICT resources under their remit, in accordance with the Risk Management Framework and applicable technical standards; and

(d) reporting and escalating identified cyber security risks in accordance with the Risk Management Framework, and applicable technical standards.

11 Rescissions and replacements

This document replaces the *Information Security Policy 2010,* which is rescinded as from the date of commencement of this policy.

NOTES

Cyber Security Policy 2019

Date adopted:	15 July 2019
Date commenced:	1 August 2019
Administrator:	Chief Information Officer
Review date:	1 August 2024
Rescinded documents:	*Information Security Policy 2010*
Related documents:	*Cyber Security Procedures 2019*
	Acceptable Use of ICT Resources Policy 2019
	Privacy Policy 2017
	Recordkeeping Policy 2017
	Risk Management Policy 2019

Risk Management Framework

Organisational Resilience Framework

Privacy Procedures 2018

Payment Card Industry Data Security Policy 2019

AMENDMENT HISTORY

Provision	Amendment	Commencing