CYBER SECURITY PROCEDURES 2019

Issued by:	Acting Chief Information Officer
Dated:	29 July 2019
Last amended:	
Signature:	
Name:	Caroline Hungerford

---

1 Purpose and application

(1) These procedures are to give effect to the *Cyber Security Policy 2019* ("the policy")

(2) These procedures apply to:

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

(b) all ICT resources.

(3) These procedures detail how the University will manage cyber security, cyber security risk, and cyber security incidents.

2 Commencement

These procedures commence on 1 August 2019.

3 Interpretation

(1) Words and phrases used in these procedures and not otherwise defined in this document have the meanings they have in the policy.

Note: See clause 6 of the policy.

(2) Technical standards must be read in conjunction with the *Cyber Security Standard – Glossary*

Note: See Technical Standards website

Head of Administrative Area	has the meaning given in the *University of Sydney (Delegations of Authority) Rule 2020*. At the date of these procedures this is: a senior staff member, outside a faculty or University school, whose position is declared as such by the Vice-Chancellor in writing and recorded as such in the relevant human resources recordkeeping systems.
high impact personnel	means any person that has a high cyber security risk as determined by, and notified to them by, the Head of Cyber Security.
cyber security control	means any management, operational or technical measure (including safeguards or countermeasures) put into place for cyber security.
high risk ICT service	means an ICT service that has been rated as high risk in accordance with the technical standards.
ICT asset owner	means the person who is accountable for the day to day operation and protection of an ICT service or associated ICT asset (also known as an ICT service lead).
ICT service owner	means the person responsible for defining, operating, measuring and improving an ICT service and associated cyber security controls (also known as ICT infrastructure service owner or ICT technical application owner).
privileged access	means access or administrative powers within an ICT service or ICT asset, above those of a normal user.

4 Managing cyber security risks

(1) The head of each organisational unit must:

(a) assign a business system owner for each ICT service or group of ICT services used by that unit;

(b) identify and manage cyber security risks within their unit, in accordance with the Risk Management Framework and all relevant technical standards.

(2) Business system owners must classify digital information held within ICT services within their remit, in accordance with all relevant technical standards.

(3) Technology risk owners and business system owners must:

(a) identify and manage cyber security risks within their remit, in accordance with the Risk Management Framework and all applicable technical standards; and

(b) review ICT services within their remit at least annually for compliance with the technical Standards; and

(c) report non-compliance to the Head of Organisational Unit and Head of Cyber Security in accordance with any applicable technical standards.

Note: See Technical Standards website and Risk Management Framework

(4) Business system owners, ICT service owners and ICT asset owners must obtain written approval from the Head of Cyber Security for:

(a) any exception to the technical standards;

(b) any cyber security control not covered by a technical standard;

(c) any work instruction or guideline for a cyber security control for which they are responsible; and

(d) any ICT service providing a cyber security control to other ICT services, that is operated outside the remit of the University's ICT unit.

5 Managing ICT Services

(1) Business system owners:

(a) are responsible for identifying and managing cyber security risks related to ICT services within their remit, in consultation with the Head of Cyber Security;

(b) may assign management of an ICT service or group of ICT services to an ICT service owner or retain the associated responsibilities in this procedure or the relevant technical standards.

(2) ICT service owners may assign ICT asset owners for day-to-day operation of an ICT service or associated ICT asset or retain the associated responsibilities in this procedure or the relevant technical standards.

ICT service owners and ICT asset owners must:

(a) classify;

(b) design;

(c) build;

(d) operate; and

(e) maintain

ICT services and ICT assets, and associated cyber security controls, in accordance with applicable technical standards.

Note: See Technical Standards website

6 Managing ICT vendors

(1) Technology risk owners, business system owners, and technology risk owners must:

(a) procure ICT services;

(b) manage third parties providing ICT services within their remit; and

(c) review cyber security risks and cyber security controls within ICT services provided by third parties annually

in accordance with applicable policy, procedures and technical standards.

Note: See *Procurement Policy 2019*; *Procurement: Purchase Order Procedures*; and *Procurement Sourcing Procedures*. See also *Technical Standards*

7 Access to ICT resources

(1) Heads of organisational units must:

(a) identify roles within their unit that have privileged access to high risk ICT services; and

(b) apply additional controls to any person in those roles, in accordance with the *Cyber Security Standard – IT Access Control*, prior to granting access.

(2) Technical standards may provide specific cyber security controls for ICT services related to high impact personnel.

Note: See Technical Standards website

(3) Business system owners must require all access to ICT services to be controlled in accordance with applicable technical standards.

Note: See Technical Standards website

(4) ICT service owners and ICT asset owners must only establish controls and operational processes which are consistent with applicable technical standards.

Note: See Technical Standards website

(5) All users must:

(a) access or operate ICT resources in accordance with the *Acceptable Use of ICT Resources Policy 2019* and

(b) store, process and transfer digital information in accordance with applicable technical standards.

Note: See Technical Standards website

8 Cyber security awareness and training

(1) Heads of organisational units must:

(a) require all unit staff and affiliates to participate in any Head of Cyber Security specified cyber security awareness training; and

(b) require that all technology risk owners, business system owners, ICT service owners and ICT asset owners within their unit undertake any additional training required to perform their cyber security related accountabilities and responsibilities, as identified by the Head of Cyber Security.

9 Managing cyber security incidents

(1) Any person noticing a cyber security event must report it as soon as possible to the University's Shared Service Centre or ICT unit Cyber Security Team.

Note: Physical security events, including theft of ICT assets, and non-digital information, should be reported to Campus Security.

(2) All communications to parties outside the University in relation to cyber security risks, cyber security controls or cyber security incidents must comply with applicable policies and technical standards.

Note: See *Public Comment Policy* and Technical Standards website

(3) Business system owners and ICT service owners must participate in any cyber security incident management training and testing conducted by the Head of Cyber Security.

10 Rescissions and replacements

This document replaces the *Information Security Policy*, which was adopted on 9 March 2010 and which is rescinded as from the date of commencement of this document:

NOTES

Cyber Security Procedures 2019

Date adopted:	29 July 2019
Date commenced:	1 August 2019
Original administrator:	Head of Cyber Security
Current policy owner:	Chief Information Officer
Review date:	1 August 2024
Rescinded documents:	
Related documents:	*Cyber Security Policy 2019*
	Acceptable Use of ICT Resources Policy 2019
	Privacy Policy 2017
	Recordkeeping Policy 2017
	Privacy Procedures 2018
	Risk Management Policy 2019
	Risk Management Framework
	Organisational Resilience Framework
	Payment Card Industry Data Security Policy 2019

AMENDMENT HISTORY

Provision	Amendment	Commencing
3	replace ‘University of Sydney (Delegations of Authority – Administrative Functions) Rule 2016’ with ‘University of Sydney (Delegations of Authority) Rule 2020	20 July 2023