# Cyber Security Policy

# Section 1 - Purpose and Context

(1) The purpose of this policy is to identify and outline the steps that are taken to ensure that malicious intrusion (including those associated with foreign interference) or accidental compromise of the security of Western Sydney University (the University) Information Technology (IT) Digital Services is prevented, reduced and managed.

(2) This policy applies to the University and any entity or person associated with the University authorised for the use of Digital Services including internet and email.

(3) Within Cyber Security Assurance and Operations, lead by the Chief Information and Security Officer, different sections are given responsibility for the controls necessary for the University's Cyber Security. For the purpose of expediency of language within this policy, CISO is used as a cover-all term for the department and the appropriate sections within it.

(4) This policy is to be read in conjunction with the following University policies and guides:

a. Acceptable Use of Digital Services Policy;
b. Digital Information Security Policy;
c. Email and Internet Policy;
d. Media, Social Media and Public Commentary Policy;
e. Password Protection Guide;
f. Privacy Management Plan; and
g. Privacy Policy.

# Section 2 - Definitions

### Terms and Acronyms

(5) The following definitions apply for the purposes of this policy:

a. Authorised User: a person who is an enrolled or attending student, a current employee, or a formal supplier, affiliate or associate of the University who is granted access and provided with authentication credentials by the University. Eduroam users are also Authorised Users.
b. Confidential and Sensitive Material: any information or material that a person knows or ought reasonably to know is confidential or sensitive, including but not limited to:
    i. The personal information of staff or students
    ii. Student, staff or research subject health information
    iii. Unpublicised financial information
    iv. Unpublicised strategic, legal, or research information
    v. Any data that could compromise any facet of the University, including reputation
c. CISO: Chief Information and Security Officer;

d. Cyber Security Event: any actual or suspected breach, threat, event, risk, vulnerability, or security weakness relating to University Digital Services.
e. Cyber Security Incident: any Cyber Security Event that has been determined as a genuine breach in Cyber Security.
f. Digital Services: synonymous with IT Resources, all services (e.g. data, voice, video) delivered through electronic means. This includes the capture, storage, retrieval, transfer, communication and/or dissemination of information electronically and the technologies used in support of these activities. Such technologies encompass systems, software, hardware, communications and network facilities. The method of delivery may be hosted within University IT facilities, externally or a combination. They may be paid or free, subscribed or purchased, provided through a cloud or as a managed service. (Ref. Criminal Code Act 1995, Division 92)
g. Foreign Interference: Foreign interference occurs when activities are carried out by, or on behalf of a foreign actor, which are coercive, covert, deceptive or corrupting and are contrary to Australia's sovereignty, values and national interests.
h. ISMS: Information Security Management System
i. ITDS: Information Technology and Digital Services, when used in this policy may mean the entire department, or a group within the department.
j. IT Resources - refer to Digital Services.
k. IT Service Desk: a team within ITDS, established to be the first point of call for staff and students, for all IT matters.
l. Malware: malicious software or code; software programs designed to damage or do other unwanted actions that are put onto the University's Digital Services without permission that do not serve a function to the University's business, and are often designed to actively work against it.
m. MOE: Managed Operating Environment, where the University's computers all make use of the same baseline software suite supporting Digital Services. This includes the patches, updates, and software installed, and the administration systems used.
n. Phishing: a form of social engineering, commonly an email or telephone call, designed to convince Authorised Users to provide information about or access to a Digital Service; believing the source of the message to be genuine, or originating from within that Digital Service.
o. Remote Desktop Software: an application, protocol, or other software solution that allows a computer or similar device to connect to the University's hardware or network without being on-site. This does not include the University's Wi-Fi network, which is only broadcast on-site.
p. Social Media: means any facility for online publication and commentary through and on the internet, including, but not limited to, blogs, wikis, pod casts, forums, video and photo posts, RSS, social bookmarking, and any social networks or networking sites including, but not limited to, Facebook, LinkedIn, Twitter, Pinterest, Instagram, Google+ and Flickr.
q. Spam: unsolicited commercial email.

# Section 3 - Policy Statement

(6) The University is committed to ensuring information security by preventing unauthorised access to, and modification or impairment of, its Digital Services and the information stored within them; through a combination of preventative measures, Cyber Security Incident Management, and the participation of all Authorised Users in ensuring that security measures are not undermined. [Ref. Cybercrime Act 2001, section 476.2]

(7) The University recognises foreign interference as a specific subset of cyber threat which is guarded against by instilling a positive security culture, embedding security awareness and decision making practices into all aspects of the University, as well as implementing preventative measures and risk mitigation practices.

(8) The University acknowledges that a strong security culture requires all Authorised Users to be trained in and be aware of their Cyber Security responsibilities.

(9) The University aims to maintain an appropriate level of Cyber Security to ensure the confidentiality, integrity, and availability of all Digital Services.

## Preventative Measures

(10) Preventative measures are in place to provide security controls around the University's Digital Services. These include the following:

a. Firewall: The University uses firewall hardware and software to log and protect internet and network usage, including connectivity of all Authorised Users and Digital Services, to prevent known threats and vulnerabilities from being exploited. The strength and configuration of the firewall used is based around industry standards to ensure the quality of protection on all University Digital Services. [Ref. ISO 27002 section 13.1.2; ISM Controls 1528, 1194, 0639].
b. Blocking of websites: The University blocks certain website URLs, as their content is considered unsafe, unacceptable, or would put people, Digital Services, or the University at risk. This includes, but is not limited to, malicious, gambling, pornographic, or terrorist content. [Ref. ISO 27002 section 12.2.1; ISM Control 0959].
c. Blocking of applications: The University occasionally places a throttle or limit on the internet traffic to certain high-bandwidth streaming applications to prevent an unnecessary drain on University Digital Services. [Ref. ISO 27002 section 12.1.3].
d. Antivirus software: The University uses antivirus software to ensure the confidentiality, integrity, and availability of its Digital Services and to detect any malware or similar malicious code. Where possible, its source is traced. The strength of the antivirus software and the regularity that it is set to scan is based around industry standards. [Ref. ISO 27002 section 12.2.1; ISM Controls 1288].
e. Automated Spam and Phishing detection: The University uses systems that detect spam, phishing messages, and other malicious email entering and leaving its email servers, in order to protect against Spam, Phishing attempts and viral outbreaks. The configuration of this software is adjusted to cater for new types of Spam, Phishing attempts and other forms of malicious email when CISO is made aware of them. As such, reporting of suspicious activity is still a vital part of this process. For more information on security and awareness in relation to email, see the Email and Internet Policy. [Ref. Spam Act 2003, section 4; Workplace Surveillance Act 2005, section 17.2; Telecommunications Act 1997, section 113; ISO 27003 section 13.2.3; ISM Controls 1234 & 0264].
f. Password strength: The University requires a certain level of complexity in all Authorised Users' passwords, to ensure that access to Digital Services is within industry standards. See the Digital Information Security Policy and the Password Protection Guide for more information or advice on password requirements. [Ref AAF Federation Rules section 8.7; ISO 27002 section 9.2.4; ISM Control 1546].
g. Identification and management of technical vulnerabilities: The University uses a range of tools to identify, monitor and manage vulnerabilities on its Digital Services. Vulnerabilities will be assessed for their risk to University operations and managed accordingly. [Ref: Higher Education Standards Framework (Threshold Standards) 2021, section 6.2.1e; ISO 27002 section 12.6.1; ISM Controls 1163].
h. Cryptography: The University procures digital certificates using a bona fide and valid Certificate Authority (CA), and ensures that cryptographic certificates are issued and managed as required. [Ref. ISO 27002 section 10; ISM Controls pages 123-127].
i. Awareness Information: The University provides awareness information and training relating to Cyber Security, Phishing, and Good Practices. This information is available on the University website and by following #SecurityCorner on Yammer.
j. Monitoring of logs: CISO conducts routine monitoring of Digital Services and logs related to those services. This monitoring may reveal signs of external interference, including foreign interference, which is handled in accordance with the Cyber Security Incident Management Process.

# Section 4 - Procedures

## Responsibility of All Users

(11) Cyber Security Events or breaches of security controls must be reported to the IT Services Desk immediately, even if only suspected. [Ref. ISO 27002 section 7.2.2; ISM Control 0252].

(12) Any and all remote desktop software presents a significant threat to the security of the University's Digital Services. As such, the CISO(or nominee) must first authorise and approve any software solution that provides remote access, in order to ensure the confidentiality, integrity and availability of University Digital Services (see the Digital Information Security Policy for more details). [Ref. ISO 27002 section 6.2.2; ISM Control 1272].

(13) When using or accessing University Digital Services from off-site, using a University or personal device, be aware of the inherent risks to the privacy of confidential and sensitive information kept in those services. All remote access provisions are expected to be used for University business only, and certain controls will need to be in force at all times:

a. Ensure the device used to access University Digital Services is up-to-date and virus free, and will not circumvent or compromise the security controls the University places around its Digital Services. Refer to the Acceptable Use of Digital Services Policy for information on using personal devices [Ref. ISO 27002 section 16.1.1.; ISM Control 1398];
b. An appropriate level of care and caution is exercised to prevent unauthorised access to any and all Digital Services (see the Digital Information Security Policy for more information);
c. An appropriate level of care and caution is exercised to maintain the security of confidential and sensitive information, to protect the privacy of all Authorised Users and the University (see the Privacy Policy for more information); and
d. Be aware that where remote access to University Digital Services is provided, such access is subject to the Acceptable Use of Digital Services Policy, and all other relevant University policies. All use of the University's Digital Services is logged and may be subject to routine reviews. [Ref. ISO 27002 sections 11.2.6, 11.2.8; ISM Control 0528].

## Responsibilities of the University

(14) Through the Digital Security Steering Committee (DSSC), as established in the Digital Information Security Policy, defining and supporting a strong security culture.

(15) Through the Audit and Risk Committee (ARC) ensuring the University has effective cyber security and foreign interference controls in place to protect the University.

(16) Through the Office of Marketing and Communication, the review of digital material which can pose a risk to the University is performed as detailed in the Media, Social Media and Public Commentary Policy.

(17) Providing appropriate training and awareness campaigns created to educate Authorised Users around Cyber Security Events and issues, as well as foreign interference awareness, in order to improve the effectiveness of the reporting and response processes. [Ref. ISO 27002 section 16.1.3; ISM Controls 0252]

## Responsibilities of the CISO

(18) Authorising the appropriate section(s) within CISO to perform specific procedures for ensuring the University's Cyber Security, including those identified within this policy.

(19) All Cyber Security Events reported to CISO are evaluated to determine if a response is required. If a response is

required, the Event becomes a Cyber Security Incident and will be managed by the appropriate response team in accordance with the steps outlined in the Cyber Security Incident Management Process (KB0014354, available to CISO Staff Only). This will ensure a consistent and effective approach to the management of Cyber Security Incidents, CISO including communications, and that the collection and analysis of evidence from the Cyber Security Incident occurs without compromising the integrity of the investigation or the Digital Service/s. [Ref. ISO 27002 section 16.1, 16.1.2, 16.1.3; ISM Control 0043 & 0125]

(20) Logs are reviewed to identify and manage Cyber Security Incidents and/or breaches in the security of Digital Services, as well as create and manage records and documents associated with Cyber Security Incidents for further analysis. In the event of a breach in the University's Information Security, CISO will utilise the CISO Data Breach Incident Report Process (KB0014961, available to CISO Staff Only) to triage the event and notify appropriate parties within the University if personal data is involved, as defined in the Privacy Policy and Privacy Management Plan. [Ref. ISO 27002 16.1.5, 16.1.6; ISM Controls 0120 & 0133]

(21) Controls and other preventative measures are put in place to avoid Cyber Security Incidents, either as a result of experience from previous Cyber Security Incidents or as a countermeasure or deterrent to likely Cyber Security Incidents. These measures are documented and regularly reviewed to ensure their validity and reliability. [Ref. ISO 27002 section 16.1.6]

(22) Ensures the sharing of cyber intelligence with other Australian and New Zealand Universities and the Government to help build a common picture of interference threats across the sector and to share countermeasures, to the extent that it does not compromise the University’s security posture.

(23) Nominated members of ITDS and CISO actively participate in higher education sector and government cyber security exercises, as appropriate.

(24) In the event that a Cyber Security Incident is identified as originating from a state based foreign actor, escalation within and external to the University is considered appropriate in the interests of national security.

# Section 5 - Guidelines

(25) The University maintains a MOE to provide a consistent and secure IT environment across University Digital Services. This also allows the University to maintain better control over any technical vulnerabilities that are known, or that arise,  impacting that environment. All computers procured by the University following its typical procurement process will have an appropriate MOE in place by default, if possible. It is recommended that all University Digital Services are part of a MOE wherever possible.

(26) This Policy should be read in conjunction with the following:

a. The Australian Signal Directorate's Information Security Manual as maintained by the ACSC
b. AAF Federation Rules
c. Criminal Code Act 1995
d. Cybercrime Act 2001
e. Higher Education Standards Framework (Threshold Standards) 2021
f. Spam Act 2003
g. Telecommunications Act 1997
h. Workplace Surveillance Act 2005

(27) This policy makes reference to the International Standard for Information Security, AS/NZS ISO/IEC 27002, which can be accessed under "Standards On-line Premium (SAI Global)" via the alphabetical listing in the e-Resources

section of the University Library.

## Status and Details

| | |
|---|---|
| **Status** | Current |
| **Effective Date** | 21st February 2024 |
| **Review Date** | 3rd June 2024 |
| **Approval Authority** | Director, Governance Services |
| **Approval Date** | 21st February 2024 |
| **Expiry Date** | Not Applicable |
| **Unit Head** | Justin Lisle<br>Chief Information and Security Officer<br>justin.lisle@westernsydney.edu.au |
| **Author** | Nadia Taggart<br>Chief Information and Security Officer |
| **Enquiries Contact** | Justin Lisle<br>Chief Information and Security Officer<br>justin.lisle@westernsydney.edu.au |