Cyber Security Standard – Data Security

Version	Approved by	Approval date	Effective date	Next full review
X.X		XX Month Year	XX Month Year	Month Year

Standard Statement

Purpose	The purpose of this Standard is to establish minimum requirements related to the handling and protection of digital information consistent with data classification, cyber security risk rating, as well as applicable laws, regulations, standards, and contractual obligations.	
Scope	This Standard applies to: a) any person that creates, stores, processes, or transmits UNSW Digital Information. b) any Information Resource that creates, stores, processes, or transmits UNSW Digital Information, including any device connecting to a UNSW network or used to access UNSW digital information. c) all UNSW owned, controlled, or leased locations where UNSW digital information is hosted, located, or used. d) all UNSW Digital Information.	
Are Local Documents on this subject permitted?	☐ Yes, however Local Documents must be consistent with this University-wide Document	☒ No

Standard

1. Confidentiality Risk Rating

1.1. Any **user that handles (creates, controls, stores, processes, or transmits) UNSW Digital Information must:**

(a) classify the **UNSW digital information in accordance with the *UNSW Data Classification Standard*, and in consultation with the Data Controller.**

(b) determine the confidentiality risk rating associated with the UNSW digital information based on the below table (utilising the data classification to determine risk rating).

Digital Information	Low Confidentiality Risk Rating	Medium Confidentiality Risk Rating	High Confidentiality Risk Rating
All UNSW digital information	Consists of ONLY: ***public*** digital information OR Less than 1000 records of ***private*** or ***sensitive*** digital information	Consists of: More than or equal to 1000 records of private or ***sensitive*** digital information AND Less than 1000 records of ***highly sensitive*** digital information AND has no other requirement for high security	Consists of: More than 10,000 records of ***sensitive*** digital information OR More than or equal to 1,000 records of ***highly sensitive*** digital information OR Has a business requirement, external partner, or regulatory requirement for high security

Table 1 - Confidentiality Risk Rating

2. Additional Controls

2.1. Additional controls not specified in this standard may be applicable.

(a) Information Resources storing, processing, or transmitting UNSW digital information must also comply with the *Cyber Security Standard – Risk Management* and *Cyber Security Standard – End User Computing*, regardless of whether they are non-production use.

3. Digital Information Handling

3.1. Data Creation

(a) Digital Information must only be created in accordance with the *Enterprise Data Governance Framework* and all applicable legal or regulatory requirements.

3.2. Data Access

(a) Access to Digital Information must only be granted on a “least privilege” and “need to know” basis, and in accordance with the *Cyber Security Standard – IT Access Control* and *Cyber Security Standard – Logging and Monitoring*.

3.3. Data and Storage Services

(a) Data Services and Storages Services must comply with the *Cyber Security Standard – Risk Management* and section 3.5 - Data Jurisdictions.

(b) High confidential risk rated digital information must:

i. be encrypted at rest (including when backed up or archived), in accordance with the *Approved Algorithm and Protocol List* (see *Appendix A*).

ii. have encryption keys managed in accordance with the key management requirements in *Appendix B.*

3.4. Data Storage (Portable Storage)

(a) Portable storage devices storing high confidentiality risk rated digital information must be:

i. encrypted in accordance with the Approved Algorithm and Protocol List (see Appendix A).

ii. transported by registered mail, commercial courier or another person approved by the Data Controller.

iii. sanitised using one of the approved methods in Appendix C, prior to any offsite maintenance.

(b) Portable storage devices storing medium confidentiality risk rated digital information must be password protected or physically secured when unattended.

(c) Portable storage devices with an unknown source or origin must not be used.

3.5. Data Jurisdictions

(a) Arrangements with IT Hosting Services (Data Centres, SaaS, IaaS, PaaS), Data Services, and Storage Services that handle UNSW digital information regardless of jurisdiction, must comply with the *Cyber Security Standard – Vendor Risk Management*.

(b) Where UNSW digital information is a UNSW Record as per the *UNSW Recordkeeping Standard*, it must be handled in accordance with applicable legal and regulatory requirements, including ensuring the digital information is always under the control of the Data Owner, or delegate, and ensuring its safekeeping, preservation, and due return.

(c) UNSW digital information that contains personal information or health information about an individual must be handled in accordance with applicable legal and regulatory requirements including ensuring the digital information is not transferred outside New South Wales (NSW) or not transferred to a Commonwealth agency unless:

i. the recipient is in a jurisdiction that upholds principles for fair handling of digital information substantially like NSW. Generally, this applies to most OECD* countries.

ii. a risk assessment is conducted, including consultation with the Chief Information Security Officer, Chief Data and Analytics Officer, Records, and Legal, before any digital information is transferred.

3.6. Data Transmission

(a) Transmission of UNSW digital Information must only occur in accordance with any relevant *Data Sharing Agreement* with the Data Controller.

(b) Medium and High confidentiality risk rated digital information (including any authentication data) must be:

i. encrypted in transit when transmitted through public or untrusted networks in accordance with the *Approved Algorithm and Protocol List* (see *Appendix A*).

ii. have encryption keys managed in accordance with the key management requirements in *Appendix B.*

(c) Digital information transmitted to an Information Resource with a lower cyber security risk rating (determined using the *Cyber Security Standard – Risk Management*) must be masked or sanitised to maintain the lower risk rating of the destination.

(d) Where technically possible, any data decryption in transit (for the purposes of traffic inspection and analysis of malicious activity) must be applied at the network firewall or load balancer level.

3.7. Data Retention and Data Disposal

(a) UNSW digital information that is a UNSW Record and is retained in a UNSW System of Record must:

i. be done so in accordance with the *UNSW Recordkeeping Standard* and after appraisal from the Data Controller.

ii. only be destroyed in accordance with the *UNSW Recordkeeping Standard*, and after approval from the UNSW Records & Archives unit.

(b) Digital information that is no longer required must be deleted using one of the Approved Deletion Methods in *Appendix C.*

3.8. Compliance

(a) All UNSW digital information (regardless of the confidentiality risk rating) may have legal, regulatory, standards or contractual compliance obligations. These may include, for example, critical infrastructure asset reporting obligations, mandatory data breach reporting obligations, industry obligations or codes, such as PCI-DSS, data use agreements, or participant consent agreements that Faculty, Researchers or Divisions may be bounded by.

(b) When faced with two sets of data security requirements (e.g., one from UNSW and one from another entity), both sets of requirements must be used, and the most stringent of the controls applied.

(c) All cyber security events including non-compliance with UNSW policies and standards must be reporting to the UNSWIT Service Desk.

4. Exemptions

(a) Any exemption or deviation from this Cyber Security Standard must be approved in accordance with the *Cyber Security Standard – Framework Exemption*, including a mandatory risk assessment and agreed compensating controls.

5. Appendix A – Approved Algorithm List

5.1. Insecure protocols must not be used, such as Telnet, FTP, HTTP, LDAP, SMB v1/v2, SNMP v1/v2. Secure encrypted alternatives such as SSHv2, TLS, and SFTP/FTPS, HTTPS, LDAPS, SMB v3, SNMP v3, S/MIME, IPsec, WPA2, WPA3 must be used.

5.2. Users must ensure Information Resources use the below cryptographic algorithms, key sizes, or protocols when encryption is required for digital information at rest or in transit:

Cryptographic Algorithms /Protocols	Key Size/Versions (minimum)	Permitted uses	Applicability
Advanced Encryption Standard (AES)	256 bits	*Encryption* Must not be used in Electronic Code Book (ECB) Mode.	*Symmetric Encryption*
Rivest-Shamir-Adleman (RSA)	2048 bits (Refers to the size of the modulus used in the RSA calculation)	*Key Distribution* *Digital Signatures*	*Asymmetric Encryption/public key*
Secure Hash Algorithm (SHA)	SHA-256 and SHA-512 Block Size	*Hashing*	*Digital Signing*
Transport Layer Security (TLS)	TLS v1.2 or 1.3 New implementations must use TLS 1.3	*Server-side and client-side Transport Layer Security (TLS)*	*Data In Transit - Application Level*
Elliptic Curve Digital Signature Algorithm (ECDSA)	P-256, P-384, or P-521 curves	*Digital Signatures*	*Asymmetric Encryption/public key*

Table 2 - Approved Algorithm and Protocols List

5.3. If any other cryptographic algorithms or protocols are required to be used in or by an Information Resource, encryption or key exchange must be consistent with current industry best practices such as the National Cyber Security Center (NCSC), the Australian Cyber Security Centre (ACSC), NIST, or SSL Labs. (The latest versions of these publications must be used).

5.4. Key Agreement and Authentication principles.

(a) Key exchanges must either use Diffie Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH) cryptographic algorithm, with a key size in accordance with *Table 3*.

Cryptographic Algorithms / Protocols	Key Size/Versions (minimum)
Elliptic Curve Cryptography (ECC)	224 bits (Refers to the minimum order of the base point on the elliptic curve)
Diffie-Hellman	2048 bits
Internet Key Exchange (IKE)	Version 2
Rivest-Shamir-Adleman (RSA)	As mentioned in *Table 2*

Table 3 - Minimum requirements for Key Agreement and Authentication Algorithms

(b) Where SSL certificates are used for client authentication, endpoints must be authenticated before the exchange or derivation of session keys.

5.5. Certificate Authorities

(a) External facing Information Resources transmitting Medium and High confidential risk-rated digital information must use SSL/TLS certificates signed by a known, trusted Certificate Authority.

(b) Non-public facing Information Resources may use an Internal Certificate management service.

6. Appendix B - Key Management Requirements

6.1. Business Owners must ensure cryptographic key management procedures are documented and implemented for high confidentiality risk-rated Information Resources within their area of accountability.

6.2. For IaaS or PaaS, the key management functions of the cloud service provider may be used where the service is compliant with section 6.3.

6.3. Cryptographic keys must be:

(a) generated in an isolated environment that only authorised personnel can access.

(b) secure, with the level of protection required in *Table 2 & Table 3*.

(c) access controlled by the relevant Information Service Owners.

(d) restricted to the fewest number of custodians necessary.

(e) be different for each environment.

(f) under the full control of a key custodian from issuance to installation.

(g) distributed securely - Electronic distribution of keys must only be undertaken via encrypted channels such as TLS1.2+, SSHv2 etc. Alternatively, the key material can be encrypted under a secret or key only known to authorised parties (e.g., GPG or password encrypted).

(h) stored securely (e.g.: using a hardware security module, storing in a database, stored in a separate access-controlled server etc.) in the least number of locations, with a level of protection at least as high as the security level provided by the keys (e.g., AWS Key Management Service).

(i) backed up to an encrypted container and stored separately.

(j) changed at least annually or when the key is considered weakened or suspected of being compromised.

6.4. Default vendor keys must never be used.

6.5. Retired keys must be decommissioned if no longer required. Any keys retained after retiring or replacing must not be used for encryption operations.

6.6. Master Encryption Keys (MEK), and Key Encryption Keys (KEK) must be stored separately from the keys they protect.

6.7. The loss or disclosure of keys must be reported and managed in accordance with the *Cyber Security Standard – Incident Management.*

7. Appendix C – Approved Data Deletion Methods

7.1. For high confidentiality risk rated digital information:

(a) where connected to a Windows OS based Information Asset, delete using the Sdelete command, with parameter “-p3” (3 overwrite passes).

(b) where connected to a MacOS based Information Asset, deleted using Disk Utility, with Security Option 3 (DOE-compliant 3 pass secure erase).

(c) where connected to other platforms, delete using a method compliant with US DoD 5220.22-M Wiping Standard or US DoE 3-pass secure erase.

(d) digital Information storage in servers and workstations can be purged, degaussed, shredded, or otherwise destroyed using approved third-party providers. Destruction certificates must be obtained and provided to the Data Controller.

7.2. For medium confidentiality risk rated digital information, delete using the above methods, however 1 pass is permitted (Sdelete with parameter “-p1”, or Disk Utility with Security Option 2).

Accountabilities	
Responsible Officer	Chief Information Security Officer (CISO)
Contact Officer	Head of Cyber Security Strategy & Governance
Supporting Information	
Legislative Compliance	Privacy and Personal Information Protection Act 1998 (NSW) (the "PPIP Act") Health Records and Information Privacy Act 2002 (NSW) (the "HRIP Act"). State Records Act 1998 (NSW) Security of Critical Infrastructure Act 2018 Security Legislation Amendment (Critical Infrastructure Protection) Act 2022
Parent Document (Policy)	Cyber Security Policy
Supporting Documents	Enterprise Data Governance Framework Data Governance Policy Research Data Governance & Materials Handling Policy Research - Handing Research Material & Data Procedure UNSW Recordkeeping Standard. Cyber Security Standard – Network Security Cyber Security Standard – Logging and Monitoring Cyber Security Standard – Vendor Risk Management Cyber Security Standard – Incident Management. Cyber Security Standard – Risk Management Cyber Security Standard – End User Computing Cyber Security Standard – IT Access Control
Related Documents	UNSW Records Appraisal Procedure Australian Code for the Responsible Conduct of Research (2007) NSW Government State Records General retention and disposal authorities [https://www.records.nsw.gov.au/recordkeeping/rules/general-retention-and-disposal-authorities] PCI DSS Compliance – Electronic Media Destruction Data Retention Procedure - https://www.gs.unsw.edu.au/policy/documents/dataretentionprocedure.pdf UNSW Data Classification Standard
Superseded Documents	Data Handling Guidelines
File Number	[For Governance Use]

Definitions and Acronyms	
Area of Accountability	Any area where a person has strategic, structural, operational, or financial control over an 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. Note: The Business Owner of an Information Service may be in the UNSWIT unit or any other organisational unit.

Data	Has the meaning defined in the UNSW Data Classification Standard.
Data Controller	Means Data Owner or Data Controller as defined in the UNSW Data Governance Framework.
Data Service	Means an Information Service that provides any handling of digital information.
Digital information	Means information or Data that is in a digital or electronic form and is stored, processed, or transmitted within an Information Service or Information Asset.
External Systems or External Service	Means an Information Resource that is external to the UNSW network, is not an End User Device, and may be provided access through the UNSW's internet facing firewall.
Health Information	As defined in the HRIP Act.
Information Asset	Means any hardware (including IoT devices), software, cloud-based services, communication devices, networks, that is owned by UNSW or provided by UNSW to users.
Information Asset Owner	Means the person who is accountable for the day-to-day operation and protection of an Information asset.
Information Resource	Means any Information service, Information asset or digital information.
Information Service	Means any business or technology function provided by UNSW or its partners, 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.
Information Service Owner	Means the person responsible for defining, operating, measuring, and improving an Information service and associated cyber security controls. Also known as "System Owner".
Isolated Environment	Mean an environment where cryptographic keys are generated and only accessible to authorised personnel. Generally, this is a separate key management server from the environment/server where the encryption keys are used.
Non-Production Purposes	Means any purpose other than production (live) use, such as development, system testing, pre-production, integration testing, user acceptance testing, performance testing, staging, or other such use.
Personal Information	As defined in the HRIP Act.
Portable Storage	Means an Information Asset that has the primary purpose of storage of digital information.
Storage Service	Means an Information Services that has the primary purpose of storage of digital information.
Trusted Certificate Authority (CA) / Certificate Management service	Means a trusted entity that issues Transport Layer Security (TLS) certificates for organisations that request them. This can be an external CA or an Internal Certificate Management Service.
UNSW Information Asset	Means any Information Asset owned, leased, operated, or provided by any UNSW unit or partner to users.

UNSW Information Resource	Means any Information Resource that is owned, leased, operated, or provided by any UNSW unit or partner to users.
UNSW Information Service	Means any Information Service that is owned, leased, operated, or provided by any UNSW unit or partner to users.
UNSW Supplier	UNSW supplier is a supplier that has been qualified following an approved UNSW Procurement process and approved by Strategic Procurement to supply specific goods, services, infrastructure, and capital works to UNSW based on UNSW needs. As a result, a supplier has entered into a UNSW Contract with UNSW to supply specific goods, services, infrastructure and capital works (e.g.: office supplies). To be approved by Strategic Procurement as a UNSW supplier, evidence of a competitive sourcing activity process or approved sourcing strategy must be provided.
Untrusted Network	refers to networks that do not belong to UNSW or are outside UNSWs ability to control or manage.
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 the UNSW, including any use before, during and after any formal relationship exists.

Revision History

Version	Approved by	Approval date	Effective date	Sections modified
#.#	[to be completed]	[to be completed]	[to be completed]	[to be completed]