## Standard Statement

### Purpose

The purpose of this Standard is to establish minimum requirements related to the handling and protection of UNSW 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) all UNSW Information Resources.
- c) any device connecting to a UNSW network or used to access UNSW Digital Information.
- d) all UNSW owned, controlled, or leased locations where UNSW Digital Information is hosted, located, or used.
- e) all UNSW Digital Information.

### Are Local Documents on this subject permitted?

- ☐ Yes, however Local Documents must be consistent with this University-wide Document
- ☒ No
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 the Confidentiality Risk Rating).

<table>
<thead>
<tr>
<th>Digital Information</th>
<th>Low Confidentiality Risk Rating</th>
<th>Medium Confidentiality Risk Rating</th>
<th>High Confidentiality Risk Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research related UNSW Digital Information</td>
<td>Consists of ONLY:</td>
<td></td>
<td>Consists of:</td>
</tr>
<tr>
<td></td>
<td>Public UNSW Digital Information,</td>
<td></td>
<td>Sensitive UNSW Digital</td>
</tr>
<tr>
<td></td>
<td>OR</td>
<td></td>
<td>Information related to more</td>
</tr>
<tr>
<td></td>
<td>Private or Sensitive</td>
<td></td>
<td>than or equal to 1,000</td>
</tr>
<tr>
<td></td>
<td>UNSW Digital Information</td>
<td></td>
<td>individuals,</td>
</tr>
<tr>
<td></td>
<td>related to less than 1,000</td>
<td></td>
<td>AND</td>
</tr>
<tr>
<td></td>
<td>individuals.</td>
<td></td>
<td>Highly Sensitive UNSW</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Digital Information related to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>less than 1,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>individuals,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>AND</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>has no other requirement</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>for high security.</td>
</tr>
<tr>
<td>All other UNSW Digital Information</td>
<td>Consists of ONLY:</td>
<td></td>
<td>Consists of:</td>
</tr>
<tr>
<td></td>
<td>Public UNSW Digital Information,</td>
<td></td>
<td>More than 10,000 records of</td>
</tr>
<tr>
<td></td>
<td>OR</td>
<td></td>
<td>Sensitive UNSW Digital Information,</td>
</tr>
<tr>
<td></td>
<td>Less than 1,000 records of</td>
<td></td>
<td>OR</td>
</tr>
<tr>
<td></td>
<td>Private or Sensitive</td>
<td></td>
<td>More than or equal to 1,000</td>
</tr>
<tr>
<td></td>
<td>UNSW Digital Information</td>
<td></td>
<td>records of Private or Sensitive</td>
</tr>
<tr>
<td></td>
<td>related to more than 10,000</td>
<td></td>
<td>UNSW Digital Information,</td>
</tr>
<tr>
<td></td>
<td>records of Highly Sensitive</td>
<td></td>
<td>AND</td>
</tr>
<tr>
<td></td>
<td>UNSW Digital Information</td>
<td></td>
<td>Less than 1,000 records of</td>
</tr>
<tr>
<td></td>
<td>related to more than or equal</td>
<td></td>
<td>Highly Sensitive UNSW</td>
</tr>
<tr>
<td></td>
<td>to 1,000 individuals,</td>
<td></td>
<td>Digital Information,</td>
</tr>
<tr>
<td></td>
<td>OR</td>
<td></td>
<td>OR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>has a contractual requirement,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>external partner, or regulatory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>requirement for high security.</td>
</tr>
</tbody>
</table>

Table 1 - Confidentiality Risk Rating
2. Additional Controls

2.1. UNSW Information Resources storing, processing, or transmitting UNSW Digital Information must also comply with the Cyber Security Standard – Risk Management regardless of whether they are non-production use.

3. UNSW Digital Information Handling

3.1. Protection at Rest

(a) Storage volumes containing High Confidentiality Risk Rated UNSW Digital Information must:
   i. be encrypted at rest (including when backed up or archived), in accordance with Appendix A - Approved Algorithms and Protocols.
   ii. have any encryption keys managed in accordance with the key management requirements in Appendix B - Key and Certificate Management Requirements.

(b) UNSW Digital Information copied to an UNSW Information Resource with a lower Cyber Security Risk Rating must be masked or sanitised, in order to maintain the Cyber Security Risk Rating of the destination.

3.2. Creation

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

3.3. Access

(a) Access to UNSW Digital Information must only be granted on a “least privilege” and “need to know” basis, and in accordance with the Cyber Security Standard – Identity and Access Management.

3.4. Portable Storage

(a) Portable storage devices storing High Confidentiality Risk Rated UNSW Digital Information must be:
   i. encrypted in accordance with Appendix A - Approved Algorithms and Protocols List.
   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 – Approved Data Deletion Methods, prior to any offsite maintenance.

(b) Portable storage devices storing Medium Confidentiality Risk Rated UNSW 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. Jurisdiction

(a) Where UNSW Digital Information is a UNSW Record as defined in the UNSW Recordkeeping Standard, it must be handled in accordance with applicable legal and regulatory requirements, including ensuring the UNSW Digital Information is always under the control of the Data Controller, or delegate, and ensuring its safekeeping, preservation, and due return.

(b) UNSW Digital Information that contains personal information or health information about an individual must not be transferred outside New South Wales (NSW), or to a Commonwealth agency, unless a privacy impact assessment is conducted to ensure that the transfer is compliant with all applicable privacy laws (such assessment should include consultation with the Chief Information Security Officer, Chief Data and Analytics Officer, Records, and Legal & Compliance before any UNSW Digital Information is transferred).

3.6. Transmission

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

(b) Medium Confidentiality Risk Rated UNSW Digital Information (including any authentication data) must be:
i. encrypted in transit when transmitted through public or untrusted networks in accordance with Appendix A - Approved Algorithms and Protocols.

(c) High Confidentiality Risk Rated UNSW Digital Information (including any authentication data) must be:
   i. encrypted in transit when transmitted through public or untrusted networks and public cloud environments in accordance with Appendix A - Approved Algorithms and Protocols.
   ii. have encryption keys managed in accordance with the key management requirements in Appendix B - Key and Certificate Management Requirements.

3.7. Retention and 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) UNSW Digital information that is no longer required must be deleted in accordance with Appendix C – Approved Data Deletion Methods.

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) the most stringent of the controls must be applied.

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 Algorithms & Protocols

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, and WPA3 must be used.

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

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

*Table 2 - Approved Algorithms and Protocols*

5.3. If any other cryptographic algorithms or protocols are required to be used in or by an UNSW 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.

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

*Table 3 - Minimum requirements for Key Agreement and Authentication Algorithms*
6. Appendix B - Key and Certificate Management Requirements

6.1. Business Owners must ensure cryptographic key management procedures are documented and implemented for High Confidentiality Risk-Rated UNSW Information Resources within their area of responsibility.

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, storing 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 when the key is considered weakened, has reached its crypto-period or is suspected of being compromised.

6.4. Default vendor keys must not 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.

6.8. Certificate Authorities

(a) External facing UNSW Information Resources transmitting Medium and High Confidentiality Risk-Rated UNSW Digital Information must use SSL/TLS certificates signed by a known, trusted Certificate Authority.
(b) Non-public facing UNSW Information Resources may use an Internal Certificate management service.

7. Appendix C – Approved Data Deletion Methods

7.1. For High Confidentiality Risk Rated UNSW Digital Information:

(a) where connected to a Windows OS based UNSW Information Asset, delete using the Sdelete command, with parameter “-p3” (3 overwrite passes).
(b) where connected to a MacOS based UNSW Information Asset, delete 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) UNSW Digital Information storage in servers and workstations must be purged, degaussed, shredded, or destroyed. If a secure destruction service is used, a destruction certificate must be obtained and provided to the Data Controller.

7.2. For Medium Confidentiality Risk Rated UNSW Digital Information, delete using the above methods, however, 1 pass is permitted (Sdelete with parameter ”-p1”, or Disk Utility with Security Option 2).
### Accountabilities

<table>
<thead>
<tr>
<th>Responsible Officer</th>
<th>Chief Information Security Officer (CISO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Officer</td>
<td>Head of Cyber Security Strategy &amp; Governance</td>
</tr>
</tbody>
</table>

### 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 – Risk Management
- Cyber Security Standard – Identity and Access Management
- Cyber Security Standard – Framework Exemption

#### Related Documents
- PCI DSS Compliance – Electronic Media Destruction
  
  **Data Retention Procedure**
- UNSW Data Classification Standard

#### Superseded Documents
- Data Handling Guidelines
- ITSS_02 IT Security Standard – Data Security

### Definitions and Acronyms

#### Area of Responsibility
- means any area where a person has a direct or delegated responsibility to manage an 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. Note: The Business Owner of a UNSW Information Resource may be in the UNSW IT unit or any other organisational unit.
<table>
<thead>
<tr>
<th><strong>Cyber Security Risk Rating</strong></th>
<th>A risk rating for a UNSW Information Resource determined in accordance with the Cyber Security Standard – Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data</strong></td>
<td>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 Standard this term includes all institutional data including research, administrative, and learning and teaching artefacts.</td>
</tr>
<tr>
<td><strong>Data Controller</strong></td>
<td>means Data Owner or Data Controller as defined in the UNSW Data Governance Framework.</td>
</tr>
<tr>
<td><strong>Data Service</strong></td>
<td>means an Information Service that provides any handling of Digital Information.</td>
</tr>
<tr>
<td><strong>Digital Information</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>External Systems or External Service</strong></td>
<td>means a UNSW 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.</td>
</tr>
<tr>
<td><strong>Health Information</strong></td>
<td>as defined in the HRIP Act.</td>
</tr>
<tr>
<td><strong>Infrastructure as a Service (IaaS)</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Information Asset</strong></td>
<td>means any hardware (including IoT devices), software, cloud-based services, communication devices, or network</td>
</tr>
<tr>
<td><strong>Information Asset Owner</strong></td>
<td>means the person who is responsible for the day-to-day operation and protection of a UNSW Information Asset.</td>
</tr>
<tr>
<td><strong>Information Resource</strong></td>
<td>means any Information Service, Information Asset or Digital Information.</td>
</tr>
<tr>
<td><strong>Information Service</strong></td>
<td>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); (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, and (c) system administrative tools that are used to support IT infrastructure services. Also known as ICT service, IT service, or system.</td>
</tr>
<tr>
<td><strong>Information Service Owner</strong></td>
<td>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”.</td>
</tr>
<tr>
<td><strong>Isolated Environment</strong></td>
<td>means 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.</td>
</tr>
<tr>
<td><strong>Non-Production Purposes</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
OECD Member Country

means Australia, Austria, Belgium, Canada, Chile, Czechia, Colombia, Costa Rica, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States.

Personal Information

as defined in the Privacy and Personal Information Protection Act (PPIP) Act.

Health Information

as defined in the Health Records and Information Privacy Act (HRIP) Act.

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 possibly configuration settings for the application-hosting environment.

Portable Storage

means a portable 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.

Storage Volume

means physical or logical data storage container provided by a drive, storage array or cloud storage service.

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 Digital Information

means Digital Information that is owned by UNSW or under 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 Resources 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.

UNSW Supplier

as defined in the UNSW Procurement Procedure.

Untrusted Network

refers to communications networks that do not belong to UNSW or are outside UNSW’s 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

<table>
<thead>
<tr>
<th>Version</th>
<th>Approved by</th>
<th>Approval date</th>
<th>Effective date</th>
<th>Sections modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Vice-President, Finance and Operations</td>
<td>7 June 2016</td>
<td>7 June 2016</td>
<td>This is a new document</td>
</tr>
<tr>
<td>2.0</td>
<td>Vice-Chancellor</td>
<td>18 November 2022</td>
<td>18 November 2022</td>
<td>Full review and title change</td>
</tr>
</tbody>
</table>