Information Classification and Handling Procedure

Section 1 - Purpose

(1) This procedure establishes the University's information classification standards and the protection and handling requirements for information created, collected, stored or processed by or for Charles Sturt University (the University). It supports compliance with:

a. NSW Cyber Security Policy
b. NSW Government Information Classification, Labelling and Handling Guidelines
c. NSW Standard on Records Management
d. other legislative, regulatory or contractual obligations for handling University information.

Scope

(2) This procedure applies to:

a. University employees and any other individual or party that is authorised to access University information
b. University information in any format, including physical and digital formats, data sets and digital records.

Section 2 - Policy

(3) This procedure supports the Information Technology Policy and Records Management Policy.

Section 3 - Procedures

Part A - Information classification standards

(4) The information classification standards are used to assess the sensitivity and security needs of University information and ensure that it is labelled, handled, stored and disposed of correctly. Classifications are assigned based on the potential impact of unauthorised disclosure or loss.

(5) All University information must be assigned one of the classifications in the table below. The classification is:

a. based on the content or category of the information, not the format
b. based on a clear and justifiable need and not be unnecessarily high; the lowest appropriate classification should be applied
c. recorded in the information metadata, if the system allows, and/or in an information asset register or other system documentation.

(6) University information that is subject to third-party agreements or contracts (e.g. data sharing agreements) may require additional or alternate security classifications and controls.

Information classification labels

(7) See also Delegation Schedule A - Governance and Legal for information governance delegations and authorities to share or disclose University information.

Classification	Definition	Consequence of breach or loss*	Examples^	Handling guidelines
Highly sensitive	Information that could reasonably be expected to cause serious harm to the University, multiple individuals or another organisation if released publicly.	Major to catastrophic	Information subject to mandatory regulatory or legislative control Login and password information Individual's financial records (credit card data, tax file numbers, etc.) Highly sensitive business data, plans & strategies Medical records Research data containing medical data, identifiable personal/ child/young person information, or other restricted data)	1. Must only be collected and shared with University staff if necessary to enable the University to fulfil its lawful purposes and directly relates to an activity of the University. 2. Must be stored on systems and services endorsed for internal use by Division of Information Technology (DIT). 3. Seek guidance from DIT on secure methods for sharing highly sensitive information internally or externally. 4. Only share with third parties when accompanied by non-disclosure agreements (NDA) or where there are legal obligations to provide such information. Approval must be obtained from the relevant delegated officer 5. Additional security measures are required for the capturing, processing, and storing of highly sensitive information as outlined below.
Confidential, private	Information which if disclosed could reasonably be expected to cause harm to the University, an individual or another organisation if released publicly.	Moderate	Most student and staff personally identifiable records Exam materials Student assessment items and results, study plans, practicum placements, etc. Intellectual property Records of Council and Council committees Audit reports University financial information Payroll information In progress/unpublished research materials Legal professional privilege information Complaints and appeals	1. May be distributed to University staff who have a specific and appropriate need to receive the information. Information and fields must be limited to only that which is necessary. 2. May only be processed or stored on systems and services endorsed for internal use by DIT. 3. May only be shared with third parties when accompanied by NDAs or where there are legal obligations to provide such information.

Classification	Definition	Consequence of breach or loss*	Examples^	Handling guidelines
Internal	Proprietary information that is only available to current staff or students of the University. Information that if breached would be expected to cause no or minimal harm to the University, an individual or another organisation if released publicly. Default for most University information.	Minor	Teaching materials Internal procedures and work instructions System design and configuration Project documentation Records of academic governance committees and management committees	1. May be distributed to University staff using systems and channels endorsed for internal use by DIT. 2. May be shared with third parties with approval from the relevant delegated officer (and accompanied by an NDA).
Public	The information is intended for public disclosure or consumption. Its availability to the general community would be beneficial to the University. Requires no special protection or rules for use and may be freely disseminated.	Insignificant	Course offerings University contact information Recruitment, advertised positions General information about the University University policies Published research information Open access information under the GIPA Act	1. May be distributed without restriction.

* Refer to Appendix 1 - University risk matrix of the Risk Management Guidelines to determine the potential consequence a breach or loss may cause to students, staff or other individuals, or to University objectives, safety, finances or reputation.

^ Examples are indicative only. A higher or lower classification may be more appropriate based on the risk assessment. The lowest appropriate classification should be applied.

Additional requirements for handling highly sensitive information

(8) When collecting, processing, storing, and distributing highly sensitive information:

a. Highly sensitive information is stored on University systems that require multi-factor authentication for remote access.
b. Access to highly sensitive information is restricted on a need to know basis. User access reviews are performed on a periodic basis to validate user profile and access rights.
c. Encryption and/or password protection is used when distributing highly sensitive information via email, removable media, or cloud storage.
d. Sharing highly sensitive information outside of the University requires approval from the relevant delegated authority which owns the data. In accordance with the University's Third Party Risk Management Guidelines, when sharing highly sensitive information with third parties, a contractual agreement must be in place and must include provisions for security, data breach notification, retention and disposal of the information in accordance with the University's Privacy Management Plan.

Government classification alignment

(9) The University's information classification supports compliance with NSW Cyber Security Policy (item 3.3). The

Information Classification Schedule demonstrates the alignment with the dissemination limiting markers (DLMs) and security classifications used by the NSW Government Information Classification, Labelling and Handling Guidelines and Commonwealth government Protective Security Policy Framework.

Part B - Information breach procedures

(10) A suspected or known breach or loss of University information must be reported as soon as possible:

a. For staff: report to the IT Service Desk
b. For students/HDR candidates: report to Student Central.

(11) Where the breach involves personal information, the Information Technology Procedure - Personal Data Breach will apply.

(12) Breaches of this procedure or information handling requirements will be managed under the Information Technology Procedure - Acceptable Use and Access.

Section 4 - Guidelines

(13) Information Security Guidelines

Section 5 - Glossary

(14) In this procedure:

a. Information asset – means a body of data, information or records defined and managed as a single unit so it can be understood, shared, protected and managed efficiently.
b. University information (also University record) – under the State Records Act 1998 (NSW), means any data, information or record, in any format or medium, made and kept or received and kept, by any person in the course of the exercise of official functions in the University, or for any purpose of the University, or for the use of the University.

Section 6 - Document context

Compliance drivers	NSW Cyber Security Policy
Review requirements	As per Policy Framework Policy
Document class	Management

Status and Details

Status	Current
Effective Date	17th December 2024
Review Date	17th December 2029
Approval Authority	Chief Operating Officer
Approval Date	17th December 2024
Expiry Date	Not Applicable
Unit Head	Helen Jessop Chief Information and Digital Officer
Author	Vanessa Salway Manager, Policy and Records
Enquiries Contact	Division of Information Technology +61 2 63386260