TRIM Access and Security Policy

March 2022 – This document is rescinded and replaced by the Records Management Policy and Records Management Procedure.

Section 1 - Purpose

(1) This document sets out Charles Sturt University's policy in relation to the creation, evaluation, dissemination and exploitation of information with Charles Sturt University's Records Management System, TRIM. This Policy aims to assist Charles Sturt University (the University) to operate effectively and efficiently, to comply with legislation and good practice, and to safeguard its information assets against loss by theft, fraud, malicious or accidental damage, or breach of privacy or confidence.

Scope

(2) This Policy applies to all members of the University community who have access to TRIM.

Section 2 - Glossary

(3) For the purpose of this Policy:

a. Records - a record is information created, received and maintained by Charles Sturt University and its employees in the transaction of official business or conduct of affairs, and kept as evidence of such activity.
b. Confidential Records - are sensitive information which if disclosed could cause harm to the University and sensitive information about University employees or students. Accessibility is usually to a selected group.
c. Imaged Records - are records communicated and maintained by means of electronic equipment.
d. Strictly Confidential Records - are records that would cause severe financial loss, harm or embarrassment to the University, its staff and/or students. Accessibility is usually restricted to one group.
e. State Records - means records created by public offices in NSW (including universities) are State records under the State Records Act 1998 (NSW), and subject to the provisions of both the State Records Act 1998 and the State Records Amendment Act 2005 (NSW).
f. State Archives - means a State record that State Records NSW has control of under the State Records Act 1998.
g. TRIM - is the records management software used to capture corporate records of Charles Sturt University.
h. Unclassified Records - means information which is available to the general community.

Section 3 - Policy

Part A - Responsibilities

(4) The misuse and abuse of information may have serious implications for the University's reputation. In some cases the individual processing the information has a personal legal liability in addition to the liability of the University. The University will produce guidelines for processing of information where specific liabilities may arise, but the University expects all those handling information on its behalf to do so in a responsible manner.

(5) The University and individuals as information providers and users have responsibilities to manage the access to and the security of information, within laws, policies, guidelines and codes of practice. The University Records Manager has overall responsibility for recordkeeping and use. There will be a custodian (normally the person who created or commissioned the information or a nominee) for each item of information created or held by the University and its members who are responsible for ensuring its integrity and accuracy, for legal compliance, and for determining access rights. Each individual is responsible for his or her actions and should not take any action which they know to be outside the law or in breach of the University policies, guidelines or codes of conduct. Heads of Departments are responsible for the implementation and monitoring of the Policy within their departments, and for ensuring that those for whom they are responsible, including visitors and contractors, are aware of the Policy and associated guidelines.

(6) Mechanisms will be provided by the University Records Manager where appropriate to help ensure that information may be used only within the laws or regulations pertaining to it for those records held in TRIM.

Part B - Principles

(7) Charles Sturt University has adopted the following principles which support this Policy:

a. Information captured with TRIM will be protected in line with relevant laws, legislation and University policies, notably those relating to data protection, privacy and freedom of information.
b. Information that falls under relevant legislation must be secured according to the appropriate level of availability: Unclassified, confidential and strictly confidential.
c. Information should be available to all who have a legitimate need and authority for that information.
d. Integrity of information must be maintained; information must be accurate, complete, timely and consistent with other information.
e. All who have access to information have a responsibility to handle it appropriately according to its security classification.
f. Nominated staff of the University are responsible for ensuring that appropriate procedures and systems for the processing and holding of information are in place and are effective.
g. Information will be protected against unauthorised access, inappropriate for its security classification.

Part C - Access

Rights of Access

(8) The University will provide easy access to information to enable those operating on its behalf to undertake their duties effectively; this information will include information generated and owned by the University as well as appropriate external information. In addition, the University will provide access to internal information to external bodies and individuals under the terms of the Freedom of Information Act and to those with whom the University has statutory or contractual commitments. The University will protect the rights of individuals in relation to access to personal and/or sensitive data held by the University. Physical and/or electronic access control systems will be provided to ensure that access to personal and/or sensitive information is available only to authorised individuals. The University will ensure that clear guidelines are provided on the deployment of personal and/or sensitive information and will provide training in their deployment.

Constraints on Access

(9) In addition to the legal constraints on access to specific items of information, the University has developed policies and guidelines to ensure confidentiality, to reflect best practice, and to maintain sensitive information.

Part D - Security

Security Classification

(10) All information entered in TRIM is automatically secured to the individual's business unit. If information entered falls under legislation for privacy, confidentiality protection, etc. then TRIM users must enter access controls, security levels and/or caveats appropriate for that record.

Rights to Security

(11) The University is committed to providing a secure environment in which information can be accessed and processed. Subject to disclosure under court order, data subjects have legal rights to confidentiality of information held about them by the University, and personal or sensitive information will be available only to those authorised.

Data Security

(12) The custodian of the information has a duty to ensure data security through appropriate procedures and mechanisms, which provide controlled access to the information only to appropriately authorised people. S/he must ensure, insofar as is possible, the accuracy and currency of information, and must take reasonable steps to maintain data integrity for information held in physical or in electronic form.

Computer and Network Security

(13) The University will take reasonable steps to ensure the integrity of its computer systems and data communication network.

Section 4 - Procedures

(14) Nil.

Section 5 - Guidelines

(15) Nil.

Status and Details

Status	Current
Effective Date	22nd May 2014
Review Date	31st January 2018
Approval Authority	Vice-Chancellor
Approval Date	30th April 2014
Expiry Date	Not Applicable
Unit Head	Natalie Nixon University Secretary
Author	Shelley McMenamin
Enquiries Contact	Vanessa Salway Manager, Policy and Records