Records Management - Security Procedure

Section 1 - Introduction

(1) Commonwealth and Northern Territory Government legislation requires that all members of the University community are responsible for proper records management and must contribute to the 'corporate memory' through compliance with University Records Management policies, procedures and guidelines.

(2) The security of University records refers to the practice of creating, storing, using and making records available securely, with due regard to permitting access to those members of the University community with a genuine need to know the information contained within the records and who have the proper authority to access them.

Section 2 - Compliance

(3) This is a compliance requirement under the Information Act 2002.

Section 3 - Intent

(4) This document applies to all members of the University community. It is intended to identify what issues should be considered with regard to the security of a University record.

Section 4 - Relevant Definitions

(5) In the context of this document:

a. Archiving means the process of taking records that are no longer actively utilised and separating them from active records. For hard-copy records this usually means moving them to an offsite storage facility. For digital records archiving may involve updating the status, moving the record to a separate data storage medium or compression of the data;
b. Metadata means key information identified about a record and used to discover and identify records;
c. Record means:
    i. recorded information in any form (including data in a computer system) that is required to be kept by a public sector organisation as evidence of the activities or operations of the organisation, and includes part of a record and a copy of a record; and/or
    ii. information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business;
d. Register means Register of Systems Approved for the Management of University Records;
e. Security Classification means a structured approach to manage access to records by members of the University community who have the appropriate authorisation to do so; and
f. University Community means officials and individuals carrying out University business. This includes, but is not limited to, all staff members, researchers, peer reviewers, students, volunteers, consultants, agents and contractors.

Section 5 - Procedures

(6) University records must be kept secure to prevent inappropriate access by persons without correct authorisation and potential misuse. To ensure this is possible, records must be kept in an approved system listed on the Register of Systems Approved for the Management of University Records (henceforth known as the Register) and managed consistently and systematically.

Approved Systems for Security of University Records

(7) All systems on the Register must have workflow processes in place to ensure records are kept secure, including but not limited to:

a. secure login credentials and processes around access to the approved system; and
b. additional levels of security may be applied to specific records within the system. This includes both electronic records and metadata relating to hard-copy records. This is referred to as access control, with the level of access being identified by a security classification. Access to these restricted records is limited to a subgroup of authorised people.

(8) These workflow processes must be reviewed regularly to ensure that the level of access granted to staff remains appropriate.

Security of Hard-Copy Records

(9) To ensure that hard-copy records being held within the University community are retained securely, the University community must:

a. capture the records in line with the Records Management - Capturing Procedure; and
b. ensure records are stored in line with the security classification of the approved records management system for that record. University records must not be able to be physically accessed by people who do not have access to the systems in which they are stored.

(10) Alternatively records must be forwarded to the Records and Archives for secure long-term storage.

(11) Access to archived hard-copy records must be requested through the University's Records and Archives. The Records and Archives must ensure enforcement of the appropriate security restrictions when accessing records from archive storage.

Freedom of Information

(12) If a request for freedom of information (FOI) is made that involves a University record, the assessment on whether the information within the record/s is pertinent to the request, must be assessed in accordance with the Information Act 2002. The Information Act 2002 does not recognise security classification as a justification for withholding information. Freedom of information requests are managed by Governance (governance@cdu.edu.au).

Review of Security Classification

(13) Records must be allocated security classification appropriate to the content. Members of the University community must have uninhibited access to the records that they require to undertake their work. This will avoid security classifications being ignored or over-ridden because they are inappropriate.

(14) If a member of the University community considers that the security classification of a record is inappropriate, a request must be raised with the person/s responsible for maintaining the record, to review the classification.

Records and Archives

(15) The Records and Archives is responsible for ensuring that processes and tools are in place to confirm that University records are kept securely by all members of the University community.

(16) The Records and Archives of the University is responsible for:

a. managing the University's Electronic Document and Records Management System and the administration of that system;
b. assessing systems and work processes for managing University records;
c. maintenance of the Register of Systems Approved for the Management of University Records;
d. conducting regular auditing on records management processes across the University;
e. managing the storage of archived, hard-copy University records;
f. developing and reviewing University Records Disposal Schedules;
g. managing the application of retention and disposal of University records; and
h. providing advice on how to implement new processes that involve the management of University records.

Status and Details

Status	Historic
Effective Date	15th January 2022
Review Date	14th January 2023
Approval Authority	Vice-Chancellor
Approval Date	20th December 2021
Expiry Date	20th April 2022
Responsible Executive	Fiona Coulson Deputy Vice-Chancellor Academic
Implementation Officer	Cheryl Dias Information Management Coordinator +61 8 89467069
Enquiries Contact	Cheryl Dias Information Management Coordinator +61 8 89467069