Information Security - Data Classification Procedure and Standards

Section 1 - Purpose

(1) The purpose of this Procedure is to facilitate the application of appropriate data security controls to University data and assists data Owners and Custodians to determine the level of classification required to protect data for which they are responsible.

(2) This Procedure is referenced from, and should be applied in conjunction with the Cyber Security Policy.

(3) This Procedure is closely aligned with the 2015 New South Wales Government Digital Information Security Policy 'Compliance with Minimum Controls Core Requirement as recommended for universities by the New South Wales Government ICT Strategy and draws from the following guidelines for the Information Security Industry standards:

a. AS/NZS ISO/IEC 27005:20011 Information technology — Security techniques — Information security risk management
b. AS ISO/IEC 27002:2015 Information technology — Security techniques — Code of practice for information security controls.

(4) This Procedure outlines the steps required to classify and secure data within their span of control, according to the prescribed minimum standards for data protection.

SCOPE

(5) The scope of this Procedure applies to all persons who use University IT facilities and / or have access to University data.

(6) Based on the data classification, the Owner is required to implement appropriate security measures to protect the data consistent with the minimum security standards included in this document. Data that is classified as confidential has more stringent requirements than Controlled and Published classifications.

(7) Data that is personal to the User of a University IT Resource and is stored, processed, or transmitted on that IT Resource as a result of incidental personal use is not considered University data. However, University data stored on non-university IT facilities must be verifiably protected according to the minimum security standards.

Section 2 - Policy

(8) Refer to the Cyber Security Policy.

Section 3 - Procedures

Part A - Responsibilities and Required Actions

Responsibilities of the Chief Information Officer

(9) The Chief Information Officer will consult with Faculties and Offices to jointly agree on who Owners and Custodians of University data shall be.

Responsibilities of the Owner

(10) The Owner of a data repository is the authoritative head of the respective Faculty, School, or Office within the University. The Owner is the person responsible for the business use of the information in the data repository. Where appropriate, Ownership may be shared by persons of different areas within the University.

(11) The Owner (or delegated representatives) are responsible for and authorised to:

a. approve access to the data repository and formally assign a custodian for it;
b. determine the value of the data;
c. specify and establish data control requirements and communicate these to custodians and users;
d. specify appropriate controls, based on risk assessment, to protect the University's information resources from unauthorised modification, deletion, or disclosure;
e. controls shall extend to information resources outsourced by the University;
f. confirm that controls are in place to ensure the accuracy, authenticity, and integrity of data;
g. confirm compliance with applicable IT security controls;
h. review the access rights of users depending on security risk management decisions;
i. complete an annual return to the Chief Information Officer for consolidation and certifying that their responsibilities under the Cyber Security Policy have been met;
j. promulgate data classifications, minimum security standards, procedures and business rules for data handling to their functional areas including Custodians and Users of the data;
k. conduct audits to review the classification of data on an annual basis to ensure currency of the data categories and that relevant procedures have been followed; and
l. maintain an up to date Data Classification Register for their functional area.

(12) Any deviation from the Standards for Data Protection will require a waiver in the form of written approval from the Owner. The waiver will be recorded on the Owner's Data Classification Register.

Responsibilities of the Custodian

(13) The Custodian is responsible for and authorised to:

a. carefully consider the information they are working with and to discharge their responsibilities in accordance with the Minimum Security Standards (Part C of this Procedure);

b. implement the controls specified by the Owner(s);
c. provide physical and procedural safeguards for the data;
d. assist Owners in evaluating the cost-effectiveness of controls and monitoring;
e. implement monitoring techniques and procedures for detecting, reporting; investigating incidents; and
f. custodians must not transfer or store Critical Information in email, Microsoft Word / Excel etc. unless the manner of doing so meets the storage and transmission requirements stipulated in the Standards for Data Protection.

(14) Advice relating to Custodian should be sought from the Chief Information Officer.

Responsibilities of the User

(15) The User of a data repository can be an individual or an automated application or process that is authorised by the Owner to access the data in accordance with the Owner's procedures and business rules. A User is any person who has been authorised by the Owner of the data repository to read, enter, or update data. The User is the single most effective control for providing adequate data security.

(16) Users have the responsibility to:

a. carefully consider the information they are working with and to discharge their responsibilities in accordance with the Minimum Security Standards (Part C of this Procedure).

b. use the data repository only for the purpose specified by the Owner;
c. comply with IT security controls established by the Owner;
d. prevent disclosure of confidential or sensitive information; and
e. custodians must not transfer or store Critical Information in email, Microsoft Word / Excel etc. unless the manner of doing so meets the storage and transmission requirements stipulated in the Standards for Data Protection.

(17) Advice relating to User Responsibilities should be sought from the Chief Information Officer.

Part B - Data classification Categories

(18) All University data that is stored, processed, or transmitted on University IT resources (or on other IT resources where University business occurs) must be classified into one of three categories:

a. Confidential;
b. Controlled; or
c. Published.

(19) To classify data, Owners must start by understanding the classifications. There are specific laws and regulations that govern some kinds of data. Additionally, there are situations where Owners must consider whether the confidentiality, integrity, or availability of the data is a factor. Finally, consideration must be given to the storage of data on more than one medium, such as moving data between computers by flash drive, for example. If only the primary IT facility is considered to be confidential, but not the secondary computer or the transfer media, the secondary computer could put University data at risk because it would not be adequately protected.

(20) For the intent and purpose of this Procedure, data can be categorised as one of the following three categories:

Confidential Data

a. is subject to restrictive regulatory obligations in relation to the access, distribution, retention and / or destruction of data;
b. where unauthorised disclosure would seriously impact the University and / or its partner organisations;
c. that is protected specifically by Commonwealth or State law or by University rules and regulations; and
d. where data is protected by any known law or regulation, but which must nevertheless be protected due to contractual agreements or to maintain confidentiality (e.g. Non Disclosure Agreements, Memoranda of Understanding, Service Level Agreements, Grants or Funding Agency Agreements etc.).

(21) Examples of confidential data are:

a. Credit card numbers - are often the target of internet theft;
b. Tax file numbers - are required by the Australian Tax Office to be stored and used securely. Failure to adopt appropriate measures could see the University in breach of its legal obligations;
c. Health Information - is highly sensitive and subject to a number of statutory controls, including, but not limited to the Privacy Act 1988 and the Health Records and Information Privacy Act 2002. The accidental disclosure of health information could result in significant adverse press for the University and fines for breaches of data confidentiality requirements;
d. Reportable Police Information (incidents and violations); and
e. Information classified by Human and Animal Ethics Committees.

(22) Confidential data must be protected by applying the appropriate Minimum Security Standards.

Controlled Data

a. where unauthorised disclosure may adversely impact the University and / or its partner organisations;
b. where access is limited to a selected group or process; and
c. where data not otherwise identified as confidential but which is releasable in accordance with certain legal provisions (e.g. contents of specific e-mail, date of birth, salary, etc.) Such data must however, be appropriately protected to ensure a controlled and lawful release.

(23) Examples of controlled data are:

a. financial information that is not subject to regulatory compliance requirements and hence classified as confidential;
b. committee meeting minutes;
c. student evaluation of teaching survey results;
d. research datasets; and
e. communications with research partners.

(24) Controlled data must be protected by applying the appropriate Minimum Security Standards.

Published Data

a. data not otherwise identified as Confidential or Controlled and is made available or released to the general public; and
b. where no adverse effects are expected to result from the wide circulation of this data.

(25) Examples of Published data are:

a. the University home page;
b. Faculty course lists and the University Handbook; and
c. research achievements and rankings.

(26) Published data must be protected by applying the appropriate Minimum Security Standards.

Part C - Minimum Security Standards

(27) This section lists the minimum standards that should be applied to Confidential, Controlled and Published data

categories.

(28) Notwithstanding these minimum standards, data Owners and Custodians are expected to use their professional judgment in managing risks to the data repositories they own and support. IT security controls should be proportional to the confidentiality, integrity, and availability profiles of the data.

Data Backup

Ref No	Minimum Requirements	Confidential	Controlled & Published
a	System administrators should establish and follow a procedure to carry out regular system backups.	Required	Recommended
b	Backups must be verified at least quarterly, either through automated verification, through customer restores, or through trial restores.	Required	Recommended
c	Systems administrators must maintain documented restoration procedures for systems and the data on those systems.	Required	Recommended

Change Control

Ref No	Minimum Requirements	Confidential	Controlled & Published
a	There must be a change control process for systems configuration. This process must be documented.	Required	Recommended
b	System changes should be evaluated prior to being applied in a production environment. Patches must be tested prior to installation in the production environment if a test environment is available. If a test environment is not available, the lack of patch testing should be communicated to the service subscriber or data customer, along with possible changes in the environment due to the patch.	Required	Recommended

Computer Virus Protection

Ref No	Minimum Requirements	Confidential	Controlled & Published
a	Anti-virus software must be installed and enabled.	Required	Required
b	Install and enable anti-spyware software. Installing and enabling anti-spyware software is required if the machine is used by administrators to browse Web sites not specifically related to the administration of the machine.	Recommended	Recommended
c	Anti-virus and, if applicable, anti-spyware software should be configured to update signatures daily.	Required	Recommended

Physical Access

Ref No	Minimum Requirements	Confidential	Controlled & Published
a	Systems must be physically secured in racks or areas with restricted access. Portable devices shall be physically secured if left unattended.	Required	Recommended

Ref No	Minimum Requirements	Confidential	Controlled & Published
b	Backup media must be secured from unauthorised physical access. If the backup media is stored off-site, it must be encrypted or have a documented process to prevent unauthorised access.	Required	Recommended
c	Repairs to storage devices must be undertaken onsite and under supervision of Information Technology staff.	Required	Recommended

System Hardening

Ref No	Minimum Requirements	Confidential	Controlled & Published
a	Systems must be set up in a protected network environment or by using a method that assures the system is not accessible via a potentially hostile network until it is secured.	Required	Recommended
b	Operating system and application services security patches should be installed expediently and in a manner consistent with change management procedures. Products that no longer receive security updates from the vendor (e.g. unsupported) are not authorised.	Required	Required
c	If automatic notification of new patches is available, that option should be enabled.	Required	Required
d	Services, applications, and user accounts that are not being utilised should be disabled or uninstalled.	Required	Recommended
e	Methods should be enabled to limit connections to services running on the host to only the authorised users of the service. Software firewalls, hardware firewalls, and service configuration are a few of the methods that may be employed.	Required	Recommended
f	Services or applications running on systems manipulating confidential data should implement secure (that is, encrypted) communications as required by confidentiality and integrity needs.	Required	Recommended
g	Systems will provide secure storage for Confidential data as required by confidentiality, integrity, and availability needs. Security can be provided by means such as, but not limited to, encryption access controls, file system audits, physically securing the storage media, or any combination thereof as deemed appropriate. Contracts with third-party providers must include appropriate standards for data protection and comply with privacy clauses in the Macquarie University Privacy Management Plan.	Required	Recommended
h	If the operating system supports it, integrity checking of critical operating system files should be enabled and tested. Third-party tools may also be used to implement this.	Required	Recommended
i	Integrity checking of system accounts, group memberships, and their associated privileges should be enabled and tested.	Required	Recommended
j	Whenever possible, all non-removable or (re-) writable media must be configured with file systems that support access control.	Required	Recommended
k	Access to non-public file system areas must require authentication.	Required	Required
l	Access to records and files must be restricted to specific job roles, and require authentication and password protection. Strong password requirements will be enabled, as technology permits, based on the category of data the account is allowed to access.	Required	Required
m	Apply the principle of least privilege to user, administrator, and system accounts.	Required	Recommended

Ref No	Minimum Requirements	Confidential	Controlled & Published
n	Transportable devices should be protected by a passcode and encryption (if available on the device) and stored in a secured (locked) location.	Required	Recommended

Security Monitoring

Ref No	Minimum Requirements	Confidential	Controlled & Published
a	If the operating system comes with a means to log activity, enabling and testing of those controls is required.	Required	Recommended
b	Operating system and service log monitoring and analysis should be performed routinely. This process should be documented.	Required	Recommended
c	The systems administrator must follow a documented backup strategy for security logs (for example, account management, access control, data integrity, etc.). Security logs should retain at least 14 days of relevant log information (data retention requirements for specific data should be considered).	Required	Recommended
d	All administrator or root access must be logged.	Required	Recommended

Transmission

Ref No	Minimum Requirements	Confidential	Controlled & Published
a	Data must be encrypted using an approved encryption method when transmitted over the Internet or unsecured communications channel.	Required	Recommended
b	Data must not be made available via the public Internet, the wireless network or by facsimile.	Required	Recommended
c	Transmission must only be by a dedicated secure link (e.g. credit card gateway) or transported by hand.	Required	Recommended

Disposal

Ref No	(29) Minimum Requirements	(30) Confidential	(31) Controlled & Published
a	Data must be removed before the storage device is retired or reused. If the data cannot be removed, the device must be destroyed.	Required	Recommended

Part D - Compliance

(32) If any of the minimum standards contained within this document cannot be met on systems manipulating Confidential or Controlled data, an Exception Process must be initiated that includes reporting the non-compliance to the Chief Information Officer, along with a proposed risk assessment and management plan. Non-compliance with these standards may result in revocation of system or network access, notification to supervisors and reporting to the Audit and Risk Committee.

Section 4 - Guidelines

(33) Nil.

Section 5 - Definitions

(34) Commonly defined terms are located in the University Glossary. The following definitions apply for the purpose of this Procedure.

a. ‘Custodian’ means an authorised person who is responsible for the collection, storage, or transmittal of electronic information.
b. ‘Data Classification Register’ means a table showing the functional areas of the University, the Owner of the data repository within the functional area and the data classification for the data in the data repository.
c. ‘Owner’ means an authorised person with the responsibility for coordinating the implementation of this Procedure within their functional area of the University (Education, Research, Administration etc.)
d. ‘User’ means an authorised person who accesses electronic information.

Status and Details

Status	Historic
Effective Date	22nd February 2021
Review Date	8th March 2021
Approval Authority	Vice-President, People and Services
Approval Date	21st June 2016
Expiry Date	28th April 2021
Responsible Executive	Nicole Gower Vice-President, Professional Services
Responsible Officer	Tim Hume Chief Information Officer +61 2 9850 1660
Enquiries Contact	Andrew Wan Chief Information Security Officer Information Technology