GRIFFITH UNIVERSITY

Procedure

Information Security Classification

1.0 Purpose

This procedure outlines information security classification requirements for both digital and physical University information and should be read in conjunction with the Information Governance and Management Framework and Information Management Policy.

The objectives of this procedure are to:

- provide guidance for consistent evaluation of Griffith information assets and applying the appropriate security classification.
- ensure Griffith's information security classifications are based on risk and are informed by confidentiality, integrity and availability requirements.
- protect and manage Griffith's information assets in accordance with relevant policies and regulatory requirements.

2.0 Scope

This procedure applies to:

- information/data that is created, collected, stored or processed by Griffith University, regardless of digital or physical format.
- information asset owners and information asset custodians who are responsible for classification and control of University information assets.
- users of the information for any relevant and responsible purposes, including sharing or processing the information.
- Information Service Providers who are designing or administering University information-related Information and Communication Technology (ICT) solutions and information systems.
- Information Management and Information Governance Specialists who develop and maintain information governance and information management frameworks, policies, procedures, and practices and who have responsibility for managing classified information assets over time.

Refer to Section 4.3 Roles and Responsibilities in the Information Governance and Management Framework for further details

3.0 Procedure

Information assets are valuable resources which must:

- be handled with due care and in accordance with authorised procedures.
- be made available and accessible only to staff who have a legitimate 'need-to-access' to fulfil their official University duties or contractual responsibilities.
- only be released or operated in accordance with the policies, legislative requirements, and directives of authorised Griffith University management (as outlined in Section 4.3 Roles and Responsibilities of the Information Governance and Management Framework).

A key aspect of managing information assets is to ensure they are assessed, identified and labelled with an appropriate information security classification commensurate with their value and risk. This classification can then be used to guide the implementation of security and other mechanisms to control this information from being leaked, manipulated, or becoming unavailable. Classification extends across three pillars.

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Refers to limiting the access to information to authorised persons for approved purposes.	Refers to the assurance that information has been created, amended or deleted only by the intended authorised means and is correct and valid.	Refers to allowing authorised persons to access information for authorised purposes at the time they need to do so.
Considers the risk associated with unauthorised or inappropriate disclosure, use or release.	Considers the risk associated with its reliability, or the impact of unauthorised changes to the information.	Considers the risk associated with not being available to authorised users.

Information assets should be classified and secured based on the value of the content, not the format (e.g. electronic versus physical), location, or the University's organisational structure. A "common sense" approach should apply when considering a more restrictive security classification, as doing so may adversely interfere with other critical functions, such as information sharing.

3.1 Classification scheme

The University uses Confidentiality, Integrity and Availability to help determine the appropriate security classification for information. This model is aligned with the University's risk matrix in assessing consequence and impact of the risk.

Consequence / Impact Risk Assessment Matrix					
Risk	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Descriptor	Some loss but immaterial. Existing controls & procedures should cope with event or circumstance	Consequences of event can be readily absorbed with management effort to minimise the impact	Significant event or circumstance that can be managed under normal conditions	Critical event or circumstance that can be endured with proper management	Critical event/circumstance with potentially disastrous impact on business sustainability
Confidentiality	OFFICIAL (PUBLIC)	OFFICIAL (INTERNAL)	SENSITIVE	PROTECTED	ABOVE PROTECTED [1]
Integrity	LOW	MEDIUM	MEDIUM	HIGH	HIGH
Availability	LOW	MEDIUM	MEDIUM	HIGH	HIGH

3.1.1 Confidentiality labels

UNOFFICIAL

Impact if compromised	Compromise of information confidentiality would be expected to have **no impact**. This information does not form part of official University business.
Examples include, but are not limited to	▪ Photos of a personal event shared using Griffith infrastructure (e.g. photos from a family wedding). ▪ Email to family/friends about events outside of Griffith business activities (e.g. arrangements for the weekend, home electricity bill, personal bank statement). Staff should consider acceptable use of Griffith resources before using for transmission or storage of unofficial information.

OFFICIAL (PUBLIC)

Impact if compromised	Information where an accidental or malicious breach would have an **insignificant impact**. The information is authorised for public access, however may not necessarily be released into the public domain.
Examples include, but are not limited to	▪ University strategic plans & annual reports ▪ Brochures and other promotional materials or information ▪ Published research data or open research data ▪ Released media announcements ▪ Program and Courses Catalogue ▪ Research profiles of academics including contact information as published in Griffith Experts ▪ Historical photos or documents (e.g.: Griffith Archive) authorised for release ▪ University campus maps ▪ University policies and procedures published in the Policy Library ▪ Research achievements and rankings

[1] National security information and systems above PROTECTED must be dealt with according to the arrangements outlined in the Memorandum of Understanding on the Protection of National Security Information between the Commonwealth and States and Territories.

OFFICIAL (INTERNAL)

Impact if compromised	Information where an accidental or malicious breach would be **unlikely to cause harm** to the University, another organisation or an individual if released publicly. The information has a restricted audience, and access must only be authorised based on academic, research or business need. This is the default classification for all information except for research project information and research data.
Examples include, but are not limited to	▪ Course material and other learning management system content ▪ Financial data and transaction information (e.g. invoices, purchase orders, budgets) ▪ Operational plans for business areas ▪ Routine business information ▪ Committee agendas and minutes which do not contain or relate to sensitive information of individuals/research (e.g. Academic Committee) ▪ Staff phone book (where information has not been publicly released) and organisational charts Examples of research-related information which does not contain sensitive information (e.g. personal information about individuals, commercial-in-confidence, 3rd party copyrighted material etc) which may be downgraded to this classification include: ▪ Data from sensors, cameras, records ▪ Data from instruments and imaging systems ▪ Drafts of research publications ▪ Suitably de-identified aggregated research data (e.g. incidents of disease in a geographic area by age groups).

SENSITIVE

Impact if compromised	Information where an accidental or malicious breach could **reasonably be expected to cause harm** to the University, another organisation or an individual if released publicly. The information has a restricted audience, and access must only be authorised based on **strict** academic, research or business need. This is the default classification for all research project information and research data unless reclassified in consultation with the lead researcher.
Examples include, but are not limited to	▪ Committee agendas and minutes which contain or relate to sensitive information of individuals/research (e.g. Human Research Ethics Committee, Promotions Committees) ▪ Research project information including aspects of ethics approvals and management of the research project ▪ Research data (unless classification is changed) ▪ Student information including personal information, progress and assessment results ▪ Staff personal information / human resources data relating to employment and payroll

- Staff name, role and email address for certain positions which may be considered a heightened target/risk
- Tax File Numbers
- Biometric information of individuals
- Credit card details
- Alumni information
- Health, medical and counselling patient files
- Intellectual property including trade secrets/other commercially sensitive IP
- Personal information about any individual collected and held by the University (e.g. as part of a research project, collected during University recruitment events etc)
- Master sets of exam papers
- Donor information
- Information provided to the University as commercial-in-confidence

PROTECTED

Impact if compromised	Information where an accidental or malicious breach could **reasonably be expected to cause serious harm** to the University, another organisation or an individual if released publicly. The information has a restricted audience, and access must only be authorised based on **very strict and limited** academic, research or business need.

National Security Information (NSI)

The University's confidentiality labelling schema does not deal with the classification of National Security Information (NSI) or systems; however, it integrates with the broader Australian Government approach and has been included in the Risk Assessment Matrix for Consequence/Impact (refer Table 1) for context. The source of most NSI is the Australian government, and the Information Creator is likely to aware of the classification and handling control requirements.

3.1.2 Integrity labels

Refers to the assurance that information has been created, amended or deleted only by the intended authorised means and is correct and valid.

Low	The unauthorised modification or destruction of information could be expected to have a **limited** adverse effect on University operations, University assets, or individuals.
Medium	The unauthorised modification or destruction of information could be expected to have a **serious** adverse effect on University operations, University assets, or individuals. It could be easily detected and recovered.
High	The unauthorised modification or destruction of information could be expected to have a **severe** adverse effect on University operations, University assets, or individuals. It would cause significant embarrassment and disruption and might be difficult to detect.

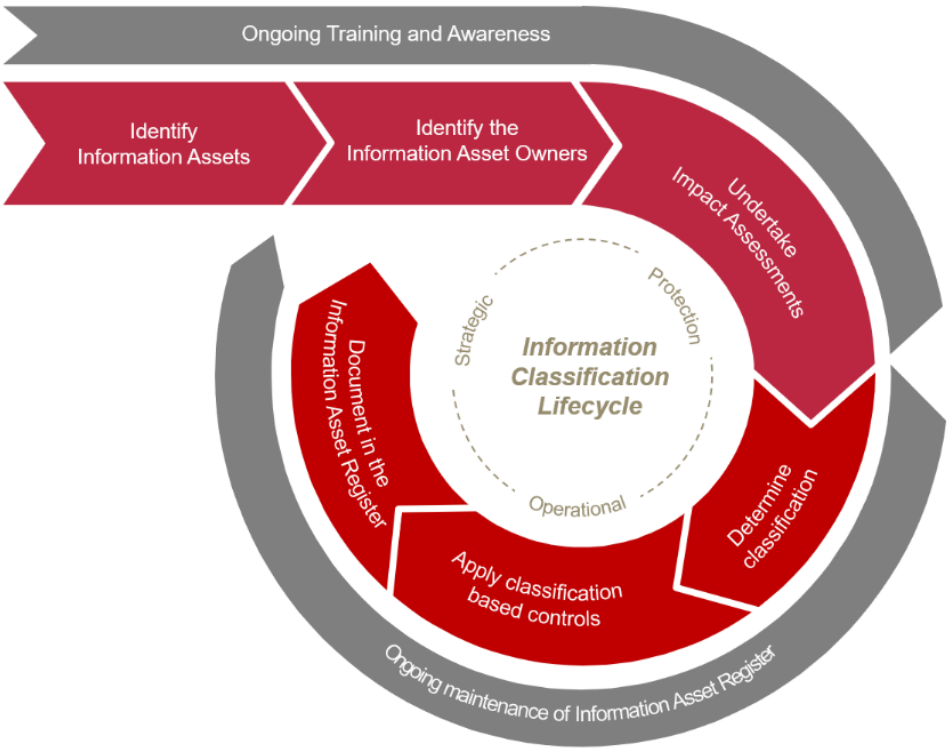
3.1.3 Availability labels

Refers to allowing authorised persons to access information for authorised purposes at the time they need to do so.

Low	The disruption of access to or use of information or an information system could be expected to have a **limited/minor** adverse effect on University operations, University assets, or individuals for an extended period (i.e. “best-effort” recovery).
Medium	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on University operations, University assets, or individuals and recovery must be achieved in a period measured in days (typically 3 business days or less).
High	The disruption of access to or use of information or an information system could be expected to have a **severe** adverse effect on University operations, University assets, or individuals and recovery must be achieved in a period measured in hours (typically same business day).

3.2 Information classification lifecycle

The assessment of information security is a living process; that is, that information security classifications need to be periodically re-assessed to ensure the required level of ongoing protection.



3.2.1 Identify information assets and Information Asset owners

An information asset is an identifiable collection of information, defined and managed as a single unit so it can be understood, shared, protected and utilised effectively. It is recognised as having value for the purpose of enabling the University to perform its business functions and supporting processes.

A Critical Information Asset (i.e., Crown Jewel) is an unstructured or structured information asset, which if compromised, degraded, rendered unavailable for an extended period or destroyed, would have a major to catastrophic impact (as defined in the Enterprise Risk Management Framework) on the viability and sustainability of the University.

The Information Asset Owner (or delegate) should classify information assets at the earliest opportunity and as soon as they are aware of the sensitivity of the information asset.

3.2.2 Undertake impact assessment and determine classification

A range of factors are considered when determining the correct information security classification levels and may include legislation, regulation, policy, contractual or other pre-determined means.

The Risk Assessment Matrix for Consequence/Impact (Figure 1) should be used to assess the impact of the information asset being compromised for confidentiality, integrity and availability, and to guide the determination of the information security classification. Apply the highest security classification level to an information asset prescribed by the impact assessment.

Information may be reclassified if its confidentiality changes, or if the information was incorrectly classified. Any protective marking must be amended to indicate the new classification.

Additional threat and risk assessment activities may be undertaken by Digital Trust where an information asset is identified as critical.

3.2.3 Apply classification-based controls

The Classification label informs the minimum handling requirements for information/data/records regardless of format. These controls may change as information moves through its lifecycle but should be planned for in advance where possible. Refer to the Information and Data Protection Standards (Griffith staff only).

3.2.4 Document in the Information Asset Register

The University maintains an Information Asset Register (IAR) to record the confidentiality rating and other key metadata associated with the information asset.

3.3 Recording and reporting

Information assets are maintained in the Information Asset Register. Relevant reporting on the status of the Information Asset Register will be provided to governance bodies.

3.4 Transitional arrangements

These information security classification labels and associated protection standards will not be applied retrospectively and will be reviewed/updated when information systems/solutions are reviewed. The following tables illustrate the mapping of the legacy information security classification labels for future reference.

3.4.1 Confidentiality: Mapping legacy labels to current labels

PREVIOUS	CURRENT
Public	Official (Public)
Private	Official (Internal)
Private (labelled) Sub-labels included: - Private (PII) - Private (IP) - Private (Inv/Legal) - Private (PCI)	Sensitive (*note there are no sub-labels in this classification*)
Protected	Protected

3.4.2 Integrity: Mapping legacy labels to current labels

PREVIOUS	CURRENT
Uncontrolled	Low
Accurate	Medium
Trusted	High
Highly Trusted	High

3.4.3 Availability: Mapping legacy labels to current labels

PREVIOUS	CURRENT
Level 1	Low
Level 2	Low
Level 3	Medium
Level 4	Medium
Level 5	High

4.0 Definitions

For the purposes of this procedure and related policy documents, the following definitions apply:

Data refers to raw, unorganised facts such as numerical figures, words or characters. This term may occasionally be used interchangeably with the term 'information'.

Information refers to a combination of data elements which is processed, structured, or presented in a given context to make it meaningful and useful. This term may occasionally be used interchangeably with the term 'data'.

Information creators means those staff who capture or create information either entering Griffith or generated by Griffith and are responsible for:

- classifying and labelling with protective markings (if required and where possible)
- managing and storing the information commensurate with its information security classification in accordance with the Information and Data Protection Standards (Griffith staff only).

Information governance is a collection of policies, practices and processes that provides a formal framework to establish decision rights and apply control through defined roles and responsibilities for the management of information and data assets throughout their lifecycle.

Information management is a collection of capabilities delivered through people, processes and technology to ensure the confidentiality, integrity, availability, quality and security of our information and data assets throughout their lifecycle.

Information security classification is a process where the creator of information assesses the sensitivity and importance of the information and assigns a label to the information so that it can be managed or stored with consideration to its sensitivity and importance.

Information users are responsible for:

- using the information assets for their approved purpose and in compliance with relevant information-related legislation, policies, procedures and guidelines, and in using the information asset, doing so ethically and securely to ensure compliance with the confidentiality requirements of the information.
- providing feedback to the relevant Information Owner (e.g.: potential breaches, integrity or quality issues).

Protective Marking is a physical or electronic label attached to information to indicate the Security Classification that is assigned.

University information is any information (irrespective of format) created, received or managed by Griffith University staff, associates, contractors, volunteers or students in connection with their employment, business dealings, research or studies at the University.

5.0 Information

Title	Information Security Classification Procedure
Document number	2021/0000109
Purpose	This procedure outlines information security classification requirements for both digital and physical University information and should be read in conjunction with the Information Governance and Management Framework, Information Management Policy and Information and Data Protection Standards (Griffith staff only).
Audience	Staff
Category	Operational
Subcategory	Information Management
UN Sustainable Development Goals (SDGs)	This document aligns with Sustainable Development Goal: 16: Peace, Justice and Strong Institutions
Approval date	3 May 2022
Effective date	3 May 2022
Review date	2025
Policy advisor	Head of Information Management and Solutions
Approving authority	Chief Digital Officer

6.0 Related Policy Documents and Supporting Documents

Legislation	Information Privacy Act 2009 (Qld)
Policy	Information Governance and Management Framework

	Information Management Policy Information Security Policy
Procedures	Information and Data Protection Standards (Griffith staff only) Information Security Procedure (Griffith staff only)
Local Protocol	Information Asset Register
Forms	N/A