Information Security Classification Framework

Approving authority	Chief Digital Officer
Approval date	15 January 2019
Advisor	Manager, Information Management, Digital Solutions Manager, Cybersecurity, Digital Solutions
Next scheduled review	2022
Document URL	https://policies.griffith.edu.au/pdf/Information Security Classification Framework.pdf
TRIM document	2019/0000082
Description	This document provides a framework for the classification of information assets that are identified across the University, enabling the appropriate level of control and governance over such assets. This document forms part of the University's Information Security Management System (ISMS) operated by Digital Solutions (DS). The ISMS is a collection of activities and processes that identify, assess and mitigate risks associated with the availability, confidentiality and integrity of Griffith University's information assets.

Related documents

- Information Security – Handling Controls Matrix
- Information Security Policy and Security Schedules
- Information Asset Register (Public Access) | Information Asset Register (Internal Access)
- Statement of Applicability
- Risk Treatment Plan
- Information Security Risk Management Framework
- Information Security Management System Operating Model
- Data Handling Controls
- Threat and Risk Assessment Reporting
- Recruitment and Section Policy
- Code of Conduct
- Purchasing Policy
- Business Continuity Management and Resilience Framework
- Risk Register
- Enterprise Information Systems Policy

1. DEFINITIONS

Available from the Glossary on the Information Management Framework website: http://www.griffith.edu.au/information-management-framework/glossary

The following definitions apply to this document in addition to those outlined in the Glossary:

- The terms **data** and **information** are used interchangeably. This scope of this definition includes both structured and unstructured data, meaning data in a structured format such as databases, system and log files; as well as unstructured data which can include a range of sources such as various document types, blogs, emails, social media etc. Both data types involve content in various lifecycle phases such as when stored, processed, or transmitted by technology and communication systems or by manual systems;

- **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;
- **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;
- **Data at rest (DAR)** is data residing on a storage medium and not actively moving between devices or networks, e.g. data stored on a hard drive, laptop, server, flash drive, within a cloud service, or archived/stored in some other way; and
- **Data in transit (DIT)** is data which is actively moving from one location to another across a network. Data in transit does not include data which has been stored on a flash drive and being carried from one location to another – this is data at rest. An example of data in transit would be data submitted on a website or an email in transit.

2. PURPOSE

The purpose of the document is to:

- Identify the roles and responsibilities that relate to the appropriate classification and use of information assets;
- Outline the classification scheme that applies to information assets based on their content;
- Detail the nature of each level outlined in the scheme;
- Provide a framework for the classification of the University's information assets into distinct categories based on the impact the asset would have to the University should it be compromised;
- Provide guidance on the interpretation of information security principles and the rationale for applying a security classification;
- Define characteristics that should be considered for each classification level;
- Outlines an overview of relevant access controls that may apply to an information asset; and
- Outlining training and awareness requirements for those responsible for this document.

This document should be read in conjunction with the *Information Security Policy* and its accompanying *Security Schedules* and other associated policies/standards as outlined above.

3. OBJECTIVE

The objective of this classification framework is to ensure that all information assets which belong to the University – physical or digital – have an appropriate information security classification applied. This classification can then be used to guide the implementation of appropriate security and other mechanisms to control this information from being leaked, manipulated or becoming unavailable.

A holistic, risk-based approach will consider the impact a compromise to the information asset might have on the University's broader profile. By following this framework, the University will also conform to the *Information Security Policy* and associated *Security Schedules*.

4. AUDIENCE

The target audience of this document is all Griffith University staff concerned with information security classification or anyone seeking information regarding the appropriate use and management of information assets based on its classification.

5. SCOPE STATEMENT

This classification framework addresses the governance requirements of all University information assets, both physical and digital, across all delivery mechanisms including both online and physical services and provides direction for determining the relevant security classification. A single framework for all delivery mechanisms is vital as services and information are increasingly offered on multiple channels.

Where third parties are involved with the delivery of services that handle information assets, these information assets must also be appropriately classified. Other security functions that are not directly related to the information security classification of information assets are outside the scope of this framework.

Individuals to be covered by this Framework include (but are not limited to) Griffith University employees, students, contractors or third-party agents providing services on behalf of the University.

All University technology assets including University-owned mobile devices have the potential to store corporate information assets and fall within the scope of this policy. University-owned devices, as well as personally-owned mobile devices (BlackBerry, iOS devices, Android, Windows, etc.), which are used to access corporate information must also be appropriately protected.

6. ROLES AND RESPONSIBILITIES

Each Griffith University user is responsible for protecting the information assets they generate, hold or control. This may include responsibility for:

- Classifying and applying the appropriate protective security marking when preparing documents, content or data;
- Ensuring the document, content or data is afforded the protection required by the marking;
- Denying access to other staff who do not have a ‘need-to-know’; and
- Not seeking access to information which they do not 'need-to-know'.

All Griffith University users are responsible through their day-to-day operations to report any situation where they suspect the security of University information may be at risk to the Manager Risk and Compliance, Digital Solutions. e.g. if a User finds sensitive information on a website that he or she feels shouldn’t be accessible, that situation should be reported. This includes reporting actual or suspected breaches and/or vulnerabilities in the confidentiality, integrity or availability of University information.

The roles & responsibilities associated with information security classification are detailed below.

Role	Responsibility
Chief Digital Officer	The Chief Digital Officer (CDO) is responsible for the establishment and maintenance of a robust framework for the management of Griffith University's information risk. The CDO will also be responsible for overseeing the University's information management and cybersecurity programs.
Manager, Information Management	The Manager, Information Management, is responsible for the implementation and operation of the information governance policies, procedures, standards and frameworks under the remit of Digital Solutions.
Information Asset Custodian	The Information Asset Custodian is responsible for: ▪ Safe custody, transport and storage of information assets. ▪ Data capture controls and overall data architecture. ▪ System-based data processing controls. ▪ Ensuring IT policy and process considers data quality impacts and controls, particularly when applying changes and enhancements to IT systems. ▪ Testing of data quality impacts when applying system changes. ▪ Data validation and data lifecycle management jointly in consultation with the Information Asset Owner and Information Management.
Information Asset Owner	The Information Asset Owner is responsible for: ▪ Regular monitoring and reporting on data quality. ▪ Development of formal benchmarking/data metric reports to track data quality. ▪ Identification and management of data quality improvement opportunities. ▪ Identification and escalation of data quality issues for resolution. ▪ Undertaking a championing role in data quality forums. ▪ Managing staff data quality issues arising from quality monitoring and exception reporting. ▪ Joint responsibility for data validation and information/data lifecycle management with the Information Asset Custodian and Information Management. *Further information on the Information Asset Owner's roles & responsibilities have been provided in Section 6.1.*
Information Asset Steward	The Information Asset Steward is responsible for: ▪ Ensuring alignment with overall risk approach, policy and controls. ▪ Ensuring auditability of data. ▪ Ownership of data assurance program. ▪ Risk input and advice on data quality issues. ▪ Oversight of data lifecycle management.
Manager, Cybersecurity	The Manager, Cybersecurity is responsible for: ▪ Data access controls and security controls. • Data publication to external stakeholders and the management of associated data cleansing activities.
Advisory Groups	There are several advisory groups which provide a forum for executive consideration of University-wide information management and information technology activities (e.g. Change Advisory Board (CAB), Solution Architecture Board (SAB), Information & Technology Architecture Board (ITAB), Information Security, Risk and Compliance Committee etc.).

Role	Responsibility
	Specific oversight responsibilities for these advisory groups that relate to the implementation of the University's Information Security Classification include: • Reviewing and recommending actions to implement Data Classification; • Analysing the business impact of proposed control applications on the University; • Approving proposed actions/implementations; • Serving as a champion for accepted actions within respective business units;
Internal Audit	Internal Audit is responsible for providing some independent assessment of the effectiveness of the University's processes for managing particular areas of business risk. The scope of Internal Audit's risk-based program is agreed as part of an Annual Internal Audit Plan which is approved by the Audit Committee.
Griffith University Users	During day-to-day operations, if a Griffith University User comes across a situation where they suspect the security of University information might be at risk, it should be reported to Manager, Risk and Compliance, Digital Solutions e.g. if a User comes across sensitive information on a website that he or she feels shouldn't be accessible, that situation should be reported. This includes reporting actual or suspected breaches and/or vulnerabilities in the confidentiality, integrity or availability of University information.

6.1 INFORMATION ASSET OWNER

The role of the Information Asset Owner is one of the most crucial when it comes to the classification of information assets. Information Asset Owners are typically senior-level employees of the University who oversee the lifecycle of one or more pieces/collections of information. As the responsibilities of the Information Asset Owners are vast, they have been called out separately. These responsibilities are detailed below.

Responsibility	Description
Assigning an appropriate classification to University information assets	Ensuring that information assets have been classified based on its sensitivity, value and criticality to the University.
Assigning day-to-day administrative and operational responsibilities for information management to custodians	Information Asset Owners assign administrative and operational responsibility to specific employees or groups of employees. In some situations, multiple custodians may share responsibilities. Information Asset Owners should understand the delineation of these shared responsibilities where they arise.
Approving procedures related to day-to-day administrative and operational management of University information	Information Asset Owners must review and approve any procedures developed by the Information Asset Custodian with respect to processing information assets. Information Asset Owners should consider the classification of the information and associated risk tolerance when reviewing and approving procedures. For example, the management of high risk and/or highly sensitive information may warrant more comprehensive documentation and, similarly, a more formal review and approval process.

Responsibility	Description
	Further information on procedures for control are provided in the *ISMS Operating Model*.
Determining the appropriate criteria for obtaining access to information	Information Asset Owners are accountable for who has access to information assets - this does not imply that they are responsible for the day-to-day provisioning of access. It is better practice for Information Asset Owners to define a set of rules that determine who is eligible for access based on the individuals position within the University e.g. a simple rule may be that all students are permitted access to their own transcripts or all employee members are permitted access to their own health benefits information. These rules should be documented in a manner that is easily understood by and available to those handling the information assets.
Ensuring that Information Asset Custodians implement reasonable and appropriate security controls to protect the confidentiality, integrity and availability of University information	The *Information Security – Handling Controls Matrix* provides guidance on implementing reasonable and appropriate security controls based on three classifications of information: PUBLIC, PRIVATE and PROTECTED. [Note that there may be further sub-labels applied to information classified as PRIVATE based on sensitivity.] Information Asset Owners should be familiar with the security classification requirements of the information they are responsible for maintaining and ensure all Information Asset Custodians are also aware of, and can demonstrate compliance with, these requirements.
Understanding and approving how University information is stored, processed and transmitted by the University and by third-parties of the University	To ensure reasonable and appropriate security controls are implemented, Information Asset Owners must understand how information is stored, processed and transmitted. This can be accomplished through regular reviews of the University's *Risk Register.* In situations where University information is being managed by a third-party, the contract or service level agreement should include documentation of how this information will be stored, processed and transmitted in accordance with University requirements.
Defining risk tolerance and accepting or rejecting risk related to security threats that impact the confidentiality, integrity and availability of the University's information	Information security requires a balance between security, usability and available resources. Risk management plays an important role in establishing this balance. Understanding the classification of information are being stored, processed and transmitted will allow Information Asset Owners to better assess risks. Understanding legal obligations and the cost of non-compliance will also play a role in this decision making.

It is understood that the person assigning an appropriate classification to the asset may be a delegate of the process such as; solution architecture, information management or cybersecurity stakeholders. Where this exists, the Information Asset Owner must accept and sign off on the applicable risk to the asset (i.e.: where required data handling controls are not implemented, or to ensure responsibility for business-level controls are adhered to (e.g.: password management and so on).

The Enterprise Information Systems Policy provides details on the responsibilities of the Business Owner, Information System Custodian, Information System Provider and Information System User. It is acknowledged that the Information Asset roles detailed in this Framework are complementary to these roles.

7. CLASSIFICATION GUIDANCE

This section is used to determine the information classification requirements for Griffith University information assets. Information assets are valuable resources which must:

- Be handled with due care and in accordance with authorised procedures;
- Be made available/accessible only to people who have a legitimate 'need-to-access' to fulfil their official duties or contractual responsibilities; and
- Only be released or operating in accordance with the policies, legislative requirements and directives of authorised Griffith University management (as outlined within the Roles and Responsibilities section of this document).

Information and operational assets typically fall into three broad categories:

- Assets intended for public use/consumption;
- Routine assets without special sensitivity or handling requirements; and
- Assets which, because of the adverse consequences of unauthorised disclosure and use, or legislative obligations require additional controls to protect its confidentiality, integrity and availability and/or handling requirements.

Classification extends across confidentiality, integrity and availability of assets for the University. Each of these three pillars are assessed to ensure the classification of the assets are done so in a way that is meaningful to the University:

Confidentiality	Risk of unauthorised/inappropriate disclosure or release **of information assets to stakeholders that are not authorised**
Integrity	Risk to information quality through manipulation and/or destruction
Availability	Risk to information not being available to authorised users, such as service disruption and unavailability

It is essential that the University is aware of the value of the information contained in the information assets it possesses and executes responsibility to protect and manage such assets.

Information is to be classified and appropriately secured based on the content, not its format (e.g. electronic versus physical), location, or the University's organisational structure.

A "common sense" approach should be followed when applying a more restrictive security classification, as doing so interferes with some other critical functions, such as a desirable process of information sharing.

7.1 CONFIDENTIALITY LABELS

An information security confidentiality assessment examines the impact to the University should the information be inappropriately released. The information security (confidentiality) level applied to a document or data element flags how access to the information should be restricted and the efforts that should be made in doing so.

This following classification framework for confidentiality prescribes that information stored by the University is classified into the following levels:

- **PUBLIC**: Information and systems are classified as Public if they are not considered to be Private or Protected, and:
    - The information is intended for public disclosure/consumption; or
    - The loss of confidentiality, integrity, or availability of the information or system would have no adverse impact on our mission, safety, finances or reputation.
- **PRIVATE**: Information and systems are classified as Private if they are not considered to be Protected, and
    - The information is not generally available to the public; or

- The loss of confidentiality, integrity, or availability of the information or system would have a mildly adverse impact on our mission, safety, finances, or reputation.

Note: Labels may be applied to specified subsets of information that may be identified as having a special or legislated need for handling, but do not meet the requirements of the Protected classification. These labels are only used for information in the PRIVATE classification and may be used to compartmentalise information and aid in assigning access and technical controls.

- **PROTECTED**: Information and systems are classified as Protected if:
  - Specific protection of the information is required by law/regulation; or
  - The loss of confidentiality, integrity, or availability of the information or system would have a significant adverse impact on our mission, safety, finances, or reputation or result in damage/distress to students, staff or other individuals.

By default, all information (created or received by the University) will be understood to be classified as PRIVATE. This is based on the type of information within the University that is not publicly accessible and should therefore be controlled to a certain extent. In determining the appropriate level of classification, there is a requirement to balance between the protection of such information from harmful disclosure/possible misuse and disseminating it widely enough for effective utilisation. Because some information can be valuable, access to it should be controlled both within the University as well as outside it. Such information is restricted and is subject to specific handling instructions. The higher the classification, the more stringently access is controlled and limited. Refer to the Information Security – Handling Controls Matrix for guidance.

The protections given to information assets marked as PRIVATE and PROTECTED aims to limit both its availability and access to it. The barriers to access include:

- Limiting access to those who have a demonstrated need-to-know;
- Implementing strict procedures for any transmission, transfer or movement of the information;
- Establishing protected storage requirements; and
- Documenting and implementing appropriate destruction/disposal procedures.

The following section provides an overview of each of different classification tiers.

7.1.1 PUBLIC

This classification is applied to information that has been authorised by the Information Asset Owner for unrestricted access and circulation, such as via publications or web sites.

Whilst PUBLIC information has no confidentiality requirements it is still important to ensure its accuracy and completeness (integrity) prior to release. For example, information published on a publicly accessible web site must be protected from being tampered with.

Information should be specifically classified as PUBLIC before release. Publishing of PUBLIC information for external consumption should be approved by the relevant Information Asset Owner.

Information which is released with the intention to be consumed as Open Data (information that has been deemed to be freely available for use, re-use and redistributed by anyone) also falls within the PUBLIC classification. Open Data facilitates interoperability and the ability of diverse systems and organisations to work together.

7.1.2 PRIVATE

This is the default classification applied to all information assets managed by the University. Access to information under this classification should be open to all University employees and relevant external third-parties (e.g. consultants, contractors, researchers, etc.) as required by their scope of work.

Because applying a security classification makes information more expensive to handle, store and transmit, a decision to further mark PRIVATE information with a label (see

below) should be undertaken in conjunction with the Information Asset Owner and/or the Information Management or Cybersecurity teams.

7.1.2.1 PRIVATE (LABELLED)

Where sensitive information assets with a PRIVATE classification require additional protection – where misuse of the information might cause harm to the University, other entities, members of staff or students – a label may need to be applied. Sensitive information should be designated (where possible) using the following four labels.

- PRIVATE (PCI)

  This label relates specifically to the Payment Card Industry Data Security Standard (PCI DSS) and processing of payment cards of individuals.

- PRIVATE (PII)

  The Personally Identifiable Information (PII) label is used for information that is personally identifiable in alignment with the definition in Section 6 of the Privacy Act and includes health information. Personal information is defined in section 6 of the Privacy Act 1988 as 'information or an opinion... about an individual ... whose identity is apparent, or can reasonably be ascertained, from the information or opinion'.

- PRIVATE (IP)

  The Intellectual Property (IP) label is used for information that relates to the protection of the University's intellectual property, including information related to the non-disclosure of other's intellectual property, often marked as commercial-in-confidence.

- PRIVATE (Inv/Legal)

  The Investigation/Legal Privilege label is used for information that relates to investigative or legal privilege activities undertaken by or involving the University. This includes investigation/case matters related to internal audit activities, the investigation of misconduct by staff or students including grievances, internal audit investigations or investigations by external entities such as the Crime and Corruption Commission.

Many types of labelled PRIVATE information can be shared within the University, especially within designated communities of practice.

7.1.3 PROTECTED

The highest security classification available within the University is PROTECTED. It requires a substantial degree of protection, as misuse of the information could be reasonably expected to cause serious harm to the University, other entities, and members of staff or students. Comparatively, very little information belongs in this category and this classification is used with restraint.

Examples of information which could fall into this category are:

- Highly sensitive communications between the University and Government agencies;
- Executive Management or Council matters of a highly sensitive nature;
- Litigious or law enforcement information, the loss and/or compromise of which would seriously jeopardise the University;
- Significant inquiries or investigations that are likely to cause serious harm to individuals, groups or the general community (e.g. Crime and Corruption Commission enquiries);

- Highly sensitive financial and economic information, the release of or premature release of which could give a significant unfair advantage to any person or entity (e.g. acquisitions, take-overs, etc.)
- Information dealing with major fraud inquiries;
- Highly sensitive litigation cases;
- Compilations of information which individually may be classified PRIVATE (Labelled) or lower, but which collectively should be classified PROTECTED.

Access to information under this classification is generally restricted to a small number of users (e.g. highly sensitive Council matters may only be accessed by the members of University Council).

7.2 INTEGRITY LABELS

An information security integrity assessment examines the impact to the University should the information be inappropriately manipulated or destroyed. The information security (integrity) level applied to a document or data element flags how access to the information should be restricted and the efforts that should be made in doing so.

This following classification framework for integrity prescribes that information stored by the University is classified into the following levels:

- **UNCONTROLLED:** Information and systems are classified as **Uncontrolled** if they are not considered to cause an impact to the University if they are manipulated or destroyed
- **ACCURATE:** Information and systems are classified as **Accurate** if they are considered to cause a minor or insignificant impact to the University if they are manipulated or destroyed
- **TRUSTED:** Information and systems are classified as **Trusted** if they are considered to cause a moderate or major impact to the University if they are manipulated or destroyed
- **HIGHLY TRUSTED:** Information and systems are classified as **Highly Trusted** if they are considered to cause a catastrophic impact to the University if they are manipulated or destroyed

By default, all information (created or received by the University) will be understood to be classified as ACCURATE. This is based on the type of information within the University being associated with a level of trust. In determining the appropriate level of classification, there is a requirement to balance between the protection of such information from harmful manipulation and modification and disseminating it widely enough for effective value realisation. Because some information can be valuable, it should be monitored, and enforcement should be put in place both within the University as well as outside it. Such information is restricted and is subject to handling instructions. The higher the classification, the more stringently access is controlled and limited. Refer to the *Information Security – Handling Controls Matrix* for guidance.

7.3 AVAILABILITY LABELS

An information security availability assessment examines the impact to the University should the information be rendered unavailability. The information security (availability) level applied to a document or data element flags how access to the information should be restricted and the efforts that should be made in doing so.

By default, all information (created or received by the University) will be understood to be classified as LEVEL 2/3. This availability assessment should be used to identify the criticality of services to the University in the event of a disaster. It results in the assignment of a Disaster Recovery and determination of Recovery-Time Objectives (RTO) and Recovery Point of Objective (RPO).

- **LEVEL 1:** Information and systems are classified as Level 1 if they are not considered to cause an impact to the University if they are unavailable for a period of time.

- **LEVEL 2:** Information and systems are classified as Level 2 if they are considered to cause a minor impact to the University if they are unavailable for a period of time.
- **LEVEL 3:** Information and systems are classified as Level 3 if they are considered to cause a moderate impact to the University if they are unavailable for a period of time.
- **LEVEL 4:** Information and systems are classified as Level 4 if they are considered to cause a major impact to the University if they are unavailable for a period of time.
- **LEVEL 5:** Information and systems are classified as Level 5 if they are considered to cause a catastrophic impact to the University if they are unavailable for a period of time.

8. CLASSIFICATION PROCESS

This section details the security classification process, which is described diagrammatically below. It is necessary to ensure that the process is understood to be a living process, that is, that information security classifications need to be periodically and regularly reassessed, and that the application of this process on a one-off basis may not provide the required level of ongoing protection.

Each of the steps identified in Figure 1 - Classification Process is expanded in more detail in the following sub-sections.

Whenever information is generated, consideration should be given as to whether it requires additional protection (i.e. the business value may not be high, but the misuse of the information could lead to serious repercussions). Classification should occur the moment information has been identified as being at risk, which may occur before drafting commences if the subject area or sources of information are particularly sensitive.

If an information collection contains items which have been restricted (such as sections, quotes, or tables), the whole collection must be assigned the classification carried by the highest classified item. An information collection that simply makes a reference to restricted information does not necessarily require a higher classification, depending on the content and context.

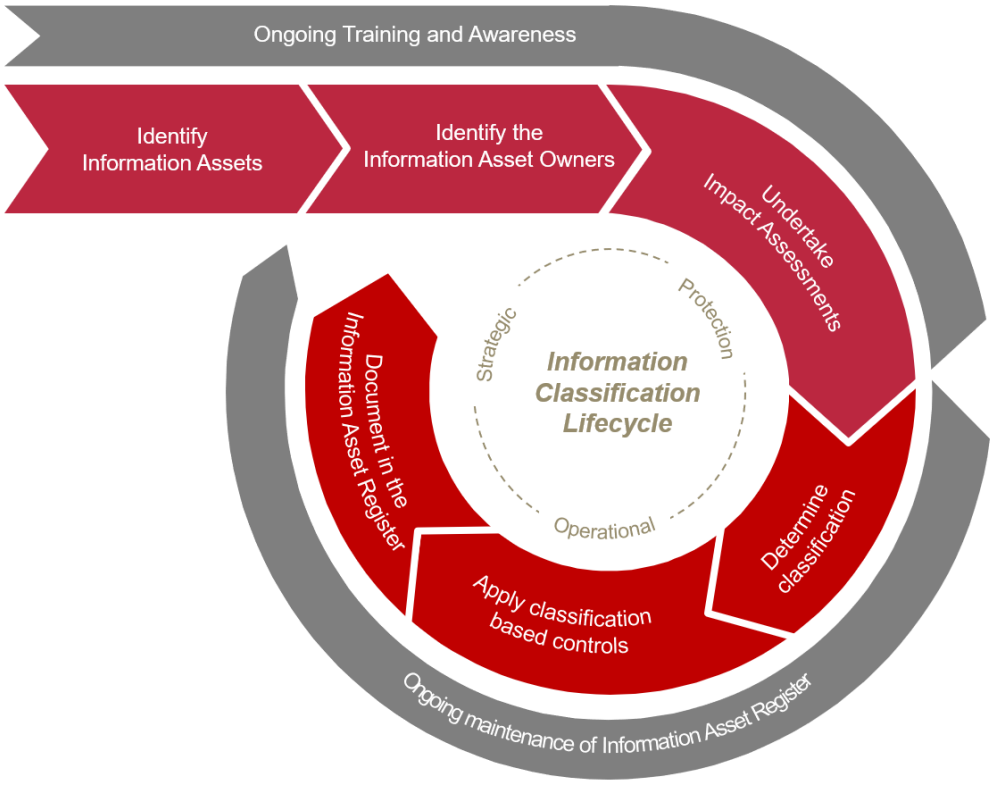

Figure 1 - Classification Process

8.1 IDENTIFY INFORMATION ASSETS

Information assets are defined as an identifiable collection of information/data, stored in any manner and recognised as having value for the purpose of enabling Griffith University to perform its business requirements.

Examples of information assets include, but are not limited to:

- records regardless of format (e.g.: email, documents, images)
- rows in a database
- tables or figures within a document
- whole database tables
- collections of data objects about a single logical entity or concept such as 'customer'
- content identified through a Uniform Resource Locators (URLs) or Uniform Resource Identifiers (URIs)
- metadata about other information assets.

Information spanning multiple media types or formats must ensure classification requirements are applied to all types or formats, to ensure overarching classification control is maintained.

If any information assets exist that are not stored in paper-based or electronic formats (such as photographs or test samples), they should still be classified using the classification scheme, but may require additional policies to ensure consistent evaluation and application.

8.2 IDENTIFY THE INFORMATION ASSET OWNERS

The University is responsible for ensuring that information assets have an information security classification that is authorised by the Information Asset Owner, and that an Information Asset Custodian who is responsible for implementing and maintaining information assets according to the rules set by the owner has been assigned. Information assets should be classified by the Information Asset Owner or delegate at the earliest possible opportunity and as soon as the originator or owner is aware of the sensitivity of the information asset.

8.3 UNDERTAKE IMPACT ASSESSMENTS

When determining the correct information security classification levels for an information asset or domain, a range of factors need to be considered. Where information assets can be security classified according to legislation, regulation, policy, contractual or other pre-determined means, it should be so classified. For example, breach of proper undertakings to maintain the confidentiality of information provided by third parties and breach of statutory restrictions on the management and disclosure of information need to be considered, and these may influence the final security classification level.

Where the security classification cannot be so determined, the impact assessment matrix below, 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.

	Severity				
Impact Type	**Lowest**				**Highest**
Impact Severity	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Compliance with Legislation	Oversight on reporting activity that is under control. No penalty or imprisonment.	Minimal non-compliance to relevant legislation, within Group or Divisions. Breaches by an individual staff member. Penalty maybe incurred.	Non-compliance with legislation affecting other Group or Divisions. Possible closure of a course or Research Centre, penalty and/or imprisonment.	Non-compliance with legislation affecting Group or Divisions activities. Closure of several non-core operations. High possibility for individual/corporate penalty and/or imprisonment.	Non-compliance with legislation affecting closure of core Group or Divisions operations or key business activities and/or large penalty (individual/corporate) and/or imprisonment.
Damage to Reputation	Minimal adverse publicity in local press. Letters received and printed but no further action taken.	Adverse publicity in local/state press. Letters to the Editors, with follow up comments from the readership or interested parties.	Extended negative local/state, plus national media coverage. Requirement to manage key stakeholders.	Longer-term nationwide and international coverage. Need to increase focus on management of a broader group of stakeholders.	Extended negative national and international wide coverage. Requirement to implement a communication plan for all stakeholders.
Disruption to Established Routines and operations	No interruption to service. Inconvenience to localised operations.	Some disruption manageable by altered operational routine. Reduction in operational routine.	Disruption to a number of operational areas/campus. Closure of an operational area/campus for up to one day.	Several key operational areas closed. Disruption to teaching / course schedules or key business activities for up to one week.	Disruption to services causing campus closure or key business closure for more than one week.
Financial	Less than $1M.	$1M to $5M.	$5M to $20M.	$20M to $50M.	Greater than $50M.
General Environmental & Social Impacts	No lasting detrimental effect on the environment i.e., harm, nuisance, noise, fumes, odour or dust emissions of short- term duration.	Short term, detrimental effect on the environment or social impact, E.g. Minor discharge of pollutants within local neighbourhood.	Serious, discharge of pollutant or source of community annoyance within general neighbourhood that requires remedial action.	Long term detrimental environmental or social impact i.e., chronic &/or significant discharge of pollutant.	Extensive detrimental long-term impacts on the environment and community i.e., catastrophic &/or extensive discharge of persistent hazardous pollutant.
Work Health & Safety	Incident – no lost time. No injury.	Injury – no lost time. First aid required.	Injury – lost time compensable injury. Medical treatment required.	Fatality or serious injury/stress resulting in hospitalisation.	Multiple fatalities (not natural causes).
Management Time and Effort	Event absorbed by normal activity.	Management effort required to minimise the impact.	A significant event managed through normal practices.	A critical event, which with proper management can be endured.	Executive Management focus away from day to day key functions for extended periods.
Confidentiality Classification	**PUBLIC**	**PRIVATE**		[See labels information for this 1/3 of sliding scale]	**PROTECTED**
Integrity Classification	**UNCONTROLLED**	**ACCURATE**		**TRUSTED**	**HIGHLY TRUSTED**
Availability Classification	**LEVEL1**	**LEVEL 2**	**LEVEL 3**	**LEVEL 4**	**LEVEL 5**

8.4 DETERMINE INFORMATION SECURITY CLASSIFICATION

The highest security classification level prescribed by the impact assessment must be applied to an information asset.

The example in the table below outlines the analysis of an information asset, confidentiality impact assessment. In this example, the highest impact identified was moderate, and hence the information asset would be classified as PRIVATE. As mentioned earlier, regulatory or legislative issues may also impact on the security classification of the information and need to be considered at this point.

Consequence	Classification Impact Severity
Compliance with Legislation	None
Damage reputation	Moderate
Disruption to Established Routines and operations.	Moderate
Financial	Minor
General Environmental & Social Impacts	Minor
Work Health & Safety	Insignificant
Management Time and Effort	Minor

When an information asset is classified, it may be possible to determine a specific date or event, after which the consequences of compromise might change. An event may trigger an increase in the sensitivity of the information - for example a student application form may be PUBLIC when empty and PRIVATE (PII) when filled in.

8.5 APPLY CLASSIFICATION-BASED CONTROLS

Appropriate controls must be applied to ensure that protection is given to information assets commensurate with the security classification. It is important to note that not all controls need to be applied to each classification tier. The controls architecture must be applied to the extent that is appropriate to the classification of the information. These controls also include information/data processes such as destruction, retention, naming etc.

Controls per classification are presented as guidance in the *Information Security – Handling Controls Matrix*.

8.6 DOCUMENT IN THE INFORMATION ASSET REGISTER

The University maintains an Information Asset Register (IAR) to record the security classification of information assets. The level to which information assets should be captured and documented in this register is detailed in the *Information Security – Handling Controls Matrix*.

The IAR is maintained by Information Management and aims to include all security classified information assets of the University. There are three (3) instances of the Information Asset Register:

- **Public -** This version of the IAR contains minimum metadata related to the University's Information Assets and is accessible to all members of the public as required under provisions of the Right to Information Act.
- **Internal -** This version of the IAR contains expanded metadata related to the University's Information Assets and is accessible to all staff of the University.
- **Administrative -** This version of the IAR contains all metadata related to the University's Information Assets and is accessible to Information Management staff.

The following minimum metadata about each Information Asset is to be recorded:

- name or unique identifier of asset or group of assets (e.g. a unique file number or name, data base name)
- description of information asset (i.e. what is it about)
- location of information asset, including the device/application on which it is stored
- Information Asset Owner
- Information Asset Custodian
- security classification of the information asset
- date of security classification with details of the authority of the classifier (e.g. who approved the classification)

- reason for the security classification of the information asset (particularly important to support review and reclassification of the information asset at a later time - should include legislative, regulatory, policy or other reference where applicable, or a copy of the impact assessment made)
- date to review security classification (if known).
- date range of the information asset (where relevant)
- disposal details where information has been disposed of.

The IAR is in and of itself an information asset. The IAR will be continually reviewed in that new information assets will be added as they become known.

9. CLASSIFICATION CONSIDERATIONS

9.1 CLASSIFICATION BY DOMAIN

It is often not practical to classify every information and operational asset, so a more appropriate method is to classify by domain. A domain in this context is any assets – logical or physical, people, process or technology – all subject to a common risk profile and set of security policies.

Information Asset Owners should assign a single classification to a collection of information that has a common purpose or function. When classifying a collection of information, the most restrictive classification of any of the individual information elements should be used e.g. if an information collection consists of a student's name, address and tax file number, the information collection should be classified as PRIVATE (PII) even though the student's name and student ID on their own is considered PRIVATE information. This helps to ensure consistency and reduce owner and user/editor workloads.

Creating conceptual domains that have security controls associated with them simplifies the process of protecting assets once they become a part of the domain. Domains allow the grouping of data and controls to be applied collectively to reduce the administrative overhead of classifying every individual data set. Domain-based classification ensures appropriate controls are applied across a set of data that share similar attributes or pose a similar set of risks to the business. The same principles of classification still apply – however classification is performed at a domain level rather than at a singular data set level.

9.2 TRAINING AND AWARENESS

The ongoing awareness of Griffith staff in the importance of classifying information is critical to the success of the University's overall security environment. All employees should have a clear understanding of the information security classification policies and procedures, their responsibilities, and the 'need-to-know' principle. Employees who create, process or handle security classified information assets should be aware of how to handle information in accordance with its classification.

9.3 MAINTENANCE OF THE INFORMATION ASSET REGISTER

As environments and circumstances change, Information Asset Owners should review security classifications to ensure that the protection being afforded is cost-effective and commensurate with the level of risk. Information Assets should be re-evaluated to ensure the assigned classification is still appropriate based on changes to legal and contractual obligations as well as changes in the use of the information or its value to the University. This evaluation should be conducted by the Information Asset Owner in conjunction with the Information Management or Cybersecurity team as part of the routine Information Asset Register management regime.

If an Information Asset Owner determines that the classification of a certain piece/collection of information has changed, an analysis of security controls should be performed to determine whether existing controls are consistent with the new classification. If gaps are found in existing security controls, they should be corrected in a timely manner, commensurate with the level of risk presented by the gaps.

Security classification makes information assets more expensive to handle, store and transfer, so it is important to ensure the information security classification is appropriate. This may require de-classifying information assets that are no longer sensitive or increasing the classification where the consequence of compromise has become more elevated.

Information Asset Owners should use the IAR to regularly review information asset security classifications.

9.4 DECLASSIFICATION OF INFORMATION

The security classification rated for an information asset may be downgraded when the reason for the higher classification no longer applies. Information assets should be reassessed by the Information Asset Owner. Should a decision be made to reclassify information, commensurate action should be taken in line with the controls that must be applied to appropriately protect this information.

9.5 DOCUMENT THE CAPABILITIES OF TECHNOLOGY AND APPLICATION SYSTEMS

The application of appropriate controls to information assets is generally documented through a solution architecture which is reviewed and approved at Solution Architecture Board. Where an application may not meet appropriate control measures commensurate to the security classification of the information asset, an exception is raised and considered by the Information & Technology Architecture Board (ITAB).

The capability of applications and systems to support different information security classification levels should be reviewed periodically, and when upgrades occur, to ensure controls are maintained.

10. INFORMATION SECURITY CONTROLS

The classification applied to a set of information will dictate the type of controls that should be applied. These controls are set out in the *Information Security – Handling Controls Matrix* and include both technical and non-technical controls. To summarise the controls, the following provides an overview of an appropriate multi-layered information protection control architecture.

10.1 INFORMATION HANDLING

As it is not feasible to allocate each staff member a security classification commensurate to their role, the principle of *Least Privilege* should be applied to ensure that each staff member only has access to data required to do their job. This should be enforced through a combination of appropriate classification and the relevant controls based on the classification.

All staff who have access to data classified as PROTECTED should be documented and granted access based on a need-to-know status. When a decision is made to securely classify an information asset, a time limit for the classification should also be set. Information assets should be declassified or downgraded when protection is no longer necessary or is

no longer needed at the original level. It might be possible to determine a specific date or event that will allow the information asset to be declassified.

10.2 STORAGE AND TRANSIT PROTECTION

It is the responsibility of all staff to ensure that they are following the processes and procedures in place that are designed to protect the University's information assets. Information assets controlled/owned by the University shall be categorised using the scheme outlined in the previous sections. To ensure that this scheme is utilised at all times, processes will be integrated as part of day-to-day activities. Regardless of the information classification applied to any given information asset containing data, technical controls for protecting the data should be implemented. This applies to data in transit between devices as well as data at rest. Supporting technologies may include:

- Records management systems
- Data loss prevention (DLP) technology (e.g. USB drive rules)
- Information rights management (IRM) technology (email scanning restrictions)
- Hardware and software-based encryption (full-disk, database, file/folder)
- Virtual Private Network (VPN) connections across public and cross-zonal networks
- Centralised data element registry
- Physical validation and authorisation
- Centralised asset inventory

To ensure the ongoing compliance (both internally and externally), data classification audits and discovery activities shall be performed at regular intervals.

Maintaining adequate processing capacity is a key component to ensuring the integrity and availability of data regardless of its classification. Procedures and appropriately configured technology which support capacity planning and load balancing must be implemented and operational to ensure that capacity limits are not exceeded, leading to loss of availability and/or integrity of information.

10.3 USER ACCESS AND AUTHENTICATION

Whilst external threats pose a significant data risk to the University, it is also recognised that internal threats are also with risk. Processes should be implemented to ensure that access to information assets is appropriate and does not compromise their integrity.

For governing, controlling and monitoring user access, it is vital to ensure an appropriate Identity and Access Management strategy, architecture and processes are implemented.

10.4 DATA INTEGRITY CHECKING

The University has procedures to control the installation of software on systems and applications that store information assets. Restrictions may be imposed on generic users, preventing them from adding, modifying or removing programs as well as executing unauthorised code.

Periodic reviews shall be performed using integrity verification tools to detect unauthorised changes to software, firmware, and data. These tools should use a pre-defined standard operating environment as a benchmark and assess unexpected changes/deviations using a risk-based approach.

10.5 PHYSICAL SECURITY

Whilst data is generally considered in its digital form, it is important to ensure physical security is applied to classified information assets. Physical security provides the ability to restrict access to both digital and physical information assets and reduces the risk of unauthorised access and use. Generally, physical security controls applied to information assets include:

- Data classified as PRIVATE (Labelled) or PROTECTED is not left unattended.
- Controls to ensure use of printers/copiers is fit for purpose.
- Servers that store or transmit data are kept in a secured location.
- Visitor/Guest/3rd-Party access to physical buildings where information assets are kept is controlled and governed.

10.6 OPERATIONAL SECURITY

To ensure that information assets are protected from unauthorised use and disclosure, implemented controls will have ongoing monitoring, logging and auditing capability. This provides the University with the ability to track activity and identify malicious and anomalous use of PRIVATE and PROTECTED data. These monitoring activities will generally fall under an operational capability as part of ongoing security detection monitoring.

10.7 RETENTION REQUIREMENTS

Information, including storage media and system documentation, must be retained and disposed in a manner that preserves confidentiality of the data classified on such devices. Minimum retention periods are generally specified in relevant retention and disposal schedules issued by Queensland State Archives.

A key component of data retention includes the need for backups of information to be kept in the event that the primary source of data becomes corrupted, destroyed or otherwise unusable.

The University will make all reasonable efforts to ensure the data stored in its information systems environment (including computer servers, application systems and databases) is backed up using the most appropriate tools and techniques. Backups are performed to meet statutory requirements for the preservation of data, as well as providing a risk mitigation activity to cover the loss of data or failure of equipment.

Note: the specific data, applications and systems to be backed-up will be specified as part of the approved backup procedure. In addition, a system backup should be performed before and after major changes to the operating system, system software, or applications.

10.8 DISPOSAL/DESTRUCTION

Secure destruction of University information assets should be considered as part of an overall information life cycle and undertaken in compliance with the *Public Records Act 2002 (Qld)*.

When equipment/media is decommissioned, all potential storage must be sanitised utilising approved tools. Implementing these controls in conjunction with other data governance practice ensures that data is protected from the point of inception, over the course of its life (both when in transit and at rest) and upon its ultimate disposal.

10.9 DATA FLOW DIAGRAMS

A data flow diagram (DFD) maps out the flow of information for any process or system. It uses defined symbols like rectangles, circles and arrows, plus short text labels, to show data inputs, outputs, storage points and the routes between each destination.

It is recognised that they routine development of data flow diagrams would require a maturity and resource uplift for the University and as such is not currently mandated. As the University progresses in its maturity, the use of data flow diagrams will be prepared in accordance with a defined procedure and subject to periodic reviews, or, when significant changes are made to the configuration of Griffith University's network data flows. Mapping would be undertaken

using standardised templates and tools. Each data flow diagram will then be assigned a security classification based on the level of critical information that it could provide to a potential attack.

11. CONTROL EXCEPTION PROCESS

Refer to the *ISMS Operating Model* for guidance on the exception for applying the controls outlined in the *Information Security – Handling Controls Matrix*.