# Information Security Classification Procedure

# Section 1 - Purpose and Scope

(1) This Procedure outlines information security classification requirements for information at The University of Queensland (UQ) and should be read in conjunction with the Information Management Policy and Information Governance and Management Framework. This Procedure applies to:

a. All information that is created, collected, stored or processed by UQ, in electronic or physical formats.
b. Individuals creating or accessing UQ's information, including (but not limited to) students, staff, contractors and consultants, visitors, title holders and third parties.

(2) This Procedure aims to:

a. Provide a consistent approach for the management of UQ information.
b. Provide guidance for evaluating UQ information and applying the appropriate security classification.
c. Protect and manage UQ information in accordance with relevant UQ policies and procedures and regulatory requirements.

# Section 2 - Process and Key Controls

(3) Information Stewards must set or endorse an overall information security classification for each information entity they are assigned to.

(4) The UQ community must classify information at the time of creation or capture, according to section 3 of this Procedure and direction from the relevant Information Steward.

(5) UQ information must be managed appropriately in accordance with its information security classification, in compliance with the Data Handling Procedure.

(6) For Microsoft 365 documents and emails, staff must ensure the correct sensitivity label is applied in accordance with the relevant information security classification. If not updated, the 'OFFICIAL' label will be applied by default. Read more about sensitivity labels.

# Section 3 - Key Requirements

### Information Security Classifications

(7) The UQ community is responsible for applying information security classifications to UQ information they create or capture.

(8) Information security classifications are based on confidentiality and ensures the information is only accessible to authorised individuals. Individuals must consider the risks associated with unauthorised or inappropriate disclosure of the information.

*This document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to refer to The University of Queensland's Policy and Procedure Library for the latest version.*

(9) All information at the University must be assigned one of the classifications in the table below. If a collection of information contains elements with different security classifications, the collection should be classified and handled based on the highest (most confidential) classification level of information within the collection.

(10) For more examples and guidance regarding information security classification, visit the data at UQ webpage.

| Information security classification | Description | Examples |
|---|---|---|
| **UNOFFICIAL** | Information that is not related to UQ study or work. | • Personal holiday itinerary<br>• Email for personal dinner reservation |
| **PUBLIC** | Information that if lost, or accessed or disclosed without authorisation, either accidentally or due to malicious activity (data breach), would have an insignificant impact.<br>The information is authorised for public access – however it may not be made available to the public. | • University strategy<br>• Published course outline<br>• Academic calendar<br>• Published research data<br>• UQ staff contact information (name, UQ email, UQ phone) |
| **OFFICIAL (Default for all information)** | Information that if subject to a data breach, would be unlikely to cause harm to UQ, another organisation or an individual if released publicly.<br>The information has a restricted audience, and access must only be authorised based on academic, research or business need (e.g. specific teams). | • UQ student contact information (name, UQ email, UQ phone)<br>• Organisational unit processes and procedures<br>• Team leave calendar |
| **SENSITIVE (Default for research projects)** | Information that if subject to a data breach, could reasonably be expected to cause harm to UQ, another organisation or an individual if released publicly.<br>The information has a restricted audience, and access must only be authorised based on strict academic, research or business need (e.g. specific individuals or groups). | • Student and staff personal information (e.g. Tax File Numbers, passport details, address, bank account details)<br>• Organisational financial data<br>• Exam material<br>• Exam results<br>• Unpublished research data |
| **PROTECTED** | Information that if subject to a data breach, could reasonably be expected to cause serious harm to UQ, another organisation or an individual if released publicly.<br>The information has a restricted audience, and access must only be authorised based on very strict academic, research or business need (e.g. only the individuals required). | • Medical data<br>• Personal data regarding persons under the age of 18<br>• Credit card data<br>• Commercially significant research results<br>• National security information |

## Additional or Alternate classifications

(11) Additional or alternate security classifications and controls may apply to information as part of the terms of a contract or agreement (e.g. data sharing agreement).

### Research projects

(12) Staff (including contractors) and HDR candidates must adhere to the research data management classifications and controls that are specified in the relevant contractual agreements or ethics approvals.

(13) They must also define additional or alternate classifications and associated controls in a research data management plan (to be stored in UQRDM) for the following types of information:

a. National security information: if staff create or capture information that if subject to a data breach, would damage the national interest or have national security implications, additional classifications and controls may apply. Refer to the Australian Government Protective Security Policy Framework.
b. Defence Industry Security Program (DISP): If staff capture or create information as part of a DISP research project, alternate security classifications and controls apply. Contact Research Ethics and Integrity for more

information.

(14) See the Research Data Management Policy for more information.

### Information Reclassification

(15) Information security classifications must be periodically reviewed in line with clause 22 (Manage and Maintain) of the Data Handling Procedure. Information must also be reclassified if its confidentiality changes, or if the information was incorrectly classified. Reclassified information must be managed in accordance with its new classification in compliance with the Data Handling Procedure.

# Section 4 - Roles, Responsibilities and Accountabilities

(16) The roles below are a summary of key information governance and management roles and responsibilities. Refer to the Information Governance and Management Framework for a comprehensive list.

### Vice-Chancellor

(17) The Vice-Chancellor is accountable for ensuring the collection and management of UQ's information and records in accordance with relevant legislative, regulatory and policy obligations.

### Chief Information Officer (CIO)

(18) The CIO is accountable for developing, maintaining and implementing information management capabilities, policies, procedures and technical standards to protect UQ's information.

### UQ community

(19) Members of the UQ community are responsible for:

a. Classifying information in compliance with this Procedure and using sensitivity labels for Microsoft 365 documents and emails;
b. Reviewing information security classifications of documents, data sets and collaboration spaces periodically, as specified in clause 22 (Manage and Maintain) of the Data Handling Procedure; and
c. Managing information in line with its information security classification, in compliance with the Data Handling Procedure.

### Information Stewards

(20) Information Stewards are responsible for the following (for the information entity/entities they are assigned to):

a. Setting or endorsing an overall information security classification for each information entity; and
b. Providing advice and making decisions regarding day-to-day management of information.

### Senior Manager, Data Strategy and Governance

(21) The Senior Manager, Data Strategy and Governance is responsible for:

a. Maintaining and implementing this Procedure; and
b. Escalating high-rated risks to UQ committees requiring resolution as required.

*This document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to refer to The University of Queensland's Policy and Procedure Library for the latest version.*

**Data Strategy and Governance Team**

(22) The Data Strategy and Governance Team supports the Manager, Data Strategy and Governance to maintain and implement this Procedure. The team is also responsible for:

a. Reporting to UQ committees on information management compliance as required;
b. Delivering training and awareness regarding data handling principles and processes; and
c. Providing training and support for Information Domain Custodians and Information Stewards.

# Section 5 - Monitoring, Review and Assurance

(23) The Data Strategy and Governance team will:

a. Provide training and guidance material (including training for Information Domain Custodians and Information Stewards) and deliver awareness initiatives to the wider UQ community as required, to improve data literacy and awareness across UQ;
b. Report on information management risk and compliance to the IT Policy, Risk and Assurance Committee (IT PRAC) quarterly and to other UQ committees as required (including regarding the use of Microsoft 365 sensitivity labels), in alignment with the IT Governance and Management Framework;
c. Maintain and update the information entity catalogue to ensure its accuracy; and
d. Review and update this Procedure as required to ensure its accuracy.

(24) Staff must review the information security classification for of documents, data sets and collaboration spaces in compliance with clause 22 (Manage and Maintain) of the Data Handling Procedure.

# Section 6 - Recording and Reporting

(25) The Data Strategy and Governance team maintains UQ's information entity catalogue which records:

a. Information domains and information entities;
b. Information Leaders, Information Domain Custodians and Information Stewards assigned to each business area, domain and entity (respectively); and
c. information security classifications for each UQ information entity.

(26) For research projects, information management roles and responsibilities should be captured as a research data management record in UQ RDM. Research data management plans should also be stored in UQ RDM where possible.

# Section 7 - Appendix

## Definitions

| Term | Definition |
|---|---|
| Data | refer to the Information Management Policy. |
| Information | refer to the Information Management Policy. |
| Personal information | refer to the Privacy Management Policy. |
| Information entity | refer to the Information Management Policy. |

| Term | Definition |
|---|---|
| Information domain | refer to the Information Management Policy. |
| UQ community | refer to the Information Management Policy. |
| Data breach | where data is lost, or accessed or disclosed without authorisation, either accidentally or due to malicious activity. |
| Harm | refer to the Enterprise Risk Management Framework's risk matrix for examples of consequences and their rating (from insignificant to critical), noting that this does not typically cover consequences for individuals or other impacted organisations. Serious harm typically involves consequences rated as major and critical. The Office of the Australian Information Commissioner also provides guidance regarding serious harm in relation to personal data breaches. |

## Related Policies and Procedures

(27) Information Management Policy

(28) Information Governance and Management Framework

(29) Data Handling Procedure

(30) Cyber Security Policy

(31) Privacy Management Policy

(32) Research Data Management Policy.

## Supporting Material

(33) Queensland Government - Information Security Policy (IS18:2018)

(34) Queensland Government Information Security Classification Framework

(35) Queensland State Archives - Records Governance Policy

(36) Queensland State Archives - University Sector Retention and Disposal Schedule

(37) Queensland State Archives - General Retention and Disposal Schedule (GRDS).

*This document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to refer to The University of Queensland's Policy and Procedure Library for the latest version.*

## Status and Details

| | |
|---|---|
| **Status** | Historic |
| **Effective Date** | 9th January 2024 |
| **Review Date** | 9th January 2027 |
| **Approval Authority** | Chief Information Officer |
| **Approval Date** | 9th January 2024 |
| **Expiry Date** | 30th June 2025 |
| **Policy Owner** | Zoran Sugarevski<br>Chief Information Officer |
| **Enquiries Contact** | Information Technology Services |

*This document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to refer to The University of Queensland's Policy and Procedure Library for the latest version.*