## Standard Statement

The UNSW Data Classification Standard is a framework for assessing data sensitivity, measured by the adverse business impact a breach of the data would have upon the University. This standard for the University community has been created to help effectively manage information in daily mission-related activities.

Determining how to protect & handle information depends on a consideration of the information’s type, importance, and usage. The standards outline the minimum level of protection necessary when performing certain activities, based on the classification of the information being handled.

The classification applies to University employees (faculty, staff, student employees) and other covered individuals (e.g., affiliates, vendors, independent contractors, etc.) in their handling of University data, information and records in any form (paper, digital text, image, audio, video, microfilm, etc.) during the course of conducting University business (administrative, financial, education, research or service).

**Responsible Executive:** Director, Business Reporting & Intelligence, & Data Governance (BRIDG)

**Responsible Office:** Business Reporting & Intelligence, & Data Governance

**Contact:** Kate Carruthers, Deputy Director, Data Governance Office
  k.carruthers@unsw.edu.au

## Purpose

- **Area covered:** This Standard is University-wide

## Scope

- **Version:** 1.0
- **Approval date:** 11 March 2016
- **Effective date:** 1 March 2016
- **Next review date:** March 2019

**This standard applies to all data or information that is created, collected, stored or processed by the UNSW, in electronic or non-electronic formats.**

This Standard applies to all faculty, staff and third-party agents of the University as well as any other University affiliates who are authorised to access UNSW data.

### Are Local Documents on this subject permitted?

- Yes
- Yes, subject to any areas specifically restricted within this Document
- ✗ No

## Standard Process and Actions

### 1. Responsibilities

- Data owners are responsible for appropriately classifying data.
- Data stewards are responsible for labelling data with the appropriate classification and applying required and suggested safeguards.
- Data users are responsible for complying with Data Governance Policy, related Standards and Guidelines.

### 2. Classifications
All data at the University shall be assigned one of the following classifications. Collections of diverse information should be classified as to the most secure classification level of an individual information component with the aggregated information.

<table>
<thead>
<tr>
<th>Data Classification</th>
<th>Description</th>
<th>Example Data Types</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Highly Sensitive</strong></td>
<td>Data that if breached owing to accidental or malicious activity would have a high impact on the University’s activities and objectives. This label describes the Intended audience from a restricted UNSW organisational unit or external perspective. Dissemination is based on strict academic, research or business need.</td>
<td>Data subject to regulatory control Medical Children &amp; Young persons Credit Card Research Data (containing personal medical data)</td>
</tr>
<tr>
<td><strong>Sensitive</strong></td>
<td>Data that if breached owing to accidental or malicious activity would have a medium impact on the University’s activities and objectives. This label describes the Intended audience from a restricted UNSW organisational unit or external perspective. Dissemination is based on strict academic, research or business need.</td>
<td>Student and Staff HR data Organisational financial data Exam material Exam Results Research Data (containing personal data)</td>
</tr>
<tr>
<td><strong>Private</strong></td>
<td>Data that if breached owing to accidental or malicious activity would have a low impact on the University’s activities and objectives. This label describes the Intended audience from a broad UNSW organisational unit or external perspective. Dissemination is based on academic, research or business need.</td>
<td>Business unit process and procedure Unpublished Intellectual property ITC system design &amp; configuration information</td>
</tr>
<tr>
<td><strong>Public</strong></td>
<td>Data that if breached owing to accidental or malicious activity would have an insignificant impact on the University’s activities and objectives. This label describes the Intended audience.</td>
<td>Faculty and staff directory information Course catalogues Published research data</td>
</tr>
</tbody>
</table>
### Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Approved by</th>
<th>Approval date</th>
<th>Effective date</th>
<th>Sections modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>President and Vice-Chancellor</td>
<td>11 March 2016</td>
<td>1 March 2016</td>
<td>New Standard</td>
</tr>
</tbody>
</table>

### Supporting Information

#### Parent Document (Policy)
Data Governance Policy

#### Supporting Documents
Data Handling Guideline

#### Related Documents
Nil

#### Superseded Documents
This is a new Standard

#### File Number
2016/09759

#### UNSW Statute and / or Regulation
Any variation to Policy or Procedure must remain consistent with the parent statute or regulation
Nil

#### Relevant State / Federal Legislation
Nil

### Accountabilities

#### Responsible Officer
Director, Business Reporting & Intelligence, & Data Governance

#### Contact Officer
Deputy Director, Business Reporting & Intelligence, & Data Governance

### Further Information

#### Key words for search engine
Data Governance, Data