Standard: Information and Data Classification

Purpose

The purpose of this standard is to operationalise the Data Governance Policy and Procedure through a framework for assessing information and data sensitivity, measured by the adverse business impact a breach of the information or data would have upon the University.

Definitions

A complete list of definitions relevant to this standard is contained within the Data Governance Policy and Procedure.

Standard

1. All information and data, whether created or collected, is allocated a classification so that it is managed, use and secured in a manner appropriate to its importance and sensitivity.

2. To ensure appropriate protection throughout its lifecycle, Data Domain Stewards are accountable for ensuring all information and data, within their data domain, is protected and classified when it is created, saved or completed, commensurate with its sensitivity and value.

3. Data Domain Stewards are responsible for setting the information and data classification scheme for their data domain at the lowest reasonable level in accordance with the classification table below:

<table>
<thead>
<tr>
<th>Classification</th>
<th>Description</th>
<th>Potential Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Information or data available and intended for the public consumption.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Examples include:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Policies and procedures</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Promotional publications and media</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Negligible adverse impact to the University if disclosed</td>
<td></td>
</tr>
<tr>
<td>Information and Data classifications</td>
<td>Internal</td>
<td>Sensitive</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>• information</td>
<td>Dissemination of this information or data would only be based on academic, research or business need but would have a broad internal audience.</td>
<td>Dissemination of this information or data would only be based on strict academic, research or business need and would have a limited audience.</td>
</tr>
<tr>
<td>• Degree information</td>
<td>Examples include:</td>
<td>Examples include:</td>
</tr>
<tr>
<td>• Published research outputs</td>
<td>• Documentation on most projects and processes</td>
<td>• Identifiable student data</td>
</tr>
<tr>
<td>• Public websites</td>
<td>• Aggregated information and trend analysis</td>
<td>• Identifiable staff data</td>
</tr>
<tr>
<td>• Annual Report (once approved for</td>
<td>• Unpublished research output</td>
<td>• Identifiable applicant data</td>
</tr>
<tr>
<td>publication by the Minister)</td>
<td>• De-identified record level data</td>
<td>• Financial data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Some research data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Small cohort demographic data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ITC system design and configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>May cause minor/low impact on the reputation of the University, other organisation or an individual if disclosed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Would cause medium impact to the University, staff or students if disclosed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>May cause minor/low impact on the reputation of the University, other organisation or an individual if disclosed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Would cause medium impact to the University, staff or students if disclosed</td>
</tr>
</tbody>
</table>
| Highly Sensitive | Information that, if disclosed without authorisation, could cause a severe degradation of core organisational capability or which is restricted under the Privacy Act 1988, is legally privileged or subject to other restricted legislation (for example, the Defence Trade Controls Act). Dissemination of this information or data would only be based on very strict academic, research or business need and would have a limited audience. Examples include:  
- Medical information  
- Legal information  
- Passport information  
- Personal financial details  
- Information related to minors  
- Multiple identifiable attributes like DOB and Address  
- Some research data, especially medical research data or national security related research data  
- Identifiable equity and disability data | Would cause a **high** impact (significant risks or liabilities) to the University, staff or students if disclosed. |

4. **Custodians** are responsible for applying required and suggested safeguards to protect information and data in accordance with its classification.

5. **Producers and users** are responsible for complying with this standard, and the *Data Governance Policy*. 
6. Each information and data classification requires different handling procedures that provide appropriate levels of protective security.

7. Sensitive and Highly Sensitive Information and Data require special handling requirements, especially during electronic transmission and physical transfer.

8. Data domain stewards, custodians, producers, and users need to ensure authorised access to Information and Data of different classification is appropriately managed.

9. For further information regarding information and data management and security, refer to Information technology security policy and Acceptable use of information technology policy.

10. Access may be given under relevant legislation such as Privacy, Archives, Freedom of Information, including restrictions as required under those Acts.
Document information

Title
Information and data classification

Document Type
Standard

Document Number
ANUP_6750451

Version
4

Purpose
To operationalise the data governance policy and procedure through a framework of the University for assessing information and its sensitivity.

Audience
Staff, Students

Category
Administrative

Topic
Governance & Structure

Subtopic

Effective Date
28 Oct 2022

Review Date
27 Oct 2023

Responsible Officer
University Librarian and Director, Scholarly Information Services

Approved By
Vice-Chancellor (eo.vc@anu.edu.au)

Contact Area
Library, Archives and University Records (director.sis@anu.edu.au)

Authority
Australian National University Act 1991
Archives Act 1983
Crimes Act 1914 (Cth)
Higher Education Support Act 2003
Electronic Transactions Act 1999
Education Services for Overseas Students Act 2000
Evidence Act 1995
Telecommunications Act 1997

Printed On
10 Aug 2023

Please ensure you have the latest version of this document from the Policy Library website before referencing this.