THE UNIVERSITY of ADELAIDE

Technology Services

Information Classification and Protection Guideline

Background and Purpose

The University generates, collects, processes and stores a large amount of information as part of its research, teaching, administrative, and other business activities. The University must protect the security of information in its custody in order to achieve its goals and to comply with laws and regulations. In the interests of efficiency and economy, the level of protection should be commensurate with the value of the information asset or the impact to the University if security is compromised.

This guideline provides a common framework for classifying the University's information assets in order to determine the appropriate level of security protection. The guideline has been developed to be sufficiently generic so that it can be applied to all areas within the University. Areas may choose to elaborate on this guideline to meet their specific needs.

Definitions

- **Information Security**: Security generally comprises three qualities: confidentiality, integrity and availability. A compromise in security implies a breakdown in one or more of the three qualities, namely: unauthorised disclosure, unauthorised modification, or inability to access, which may or may not result in permanent loss.
- **Information Asset**: Any piece of information, stored electronically, on paper or other media. This includes electronic files, databases, software applications, paper, and raw data.
- **Information Asset Owner**: A person who is ultimately accountable for the security of an information asset.
- **Information Asset Custodian** – A person or a team responsible for managing an information asset under the direction and delegated authority granted by the information asset owner.
- **Personal Information** has the same meaning as in the University's Privacy Policy and includes a person's name, address, date of birth, academic record, health information.
- **PSD**: Portable Storage Devices includes USB flash storage, removable hard disks, mobile phones, tablets, and laptop computers.
- **On-Premise Storage**: Storage hosted inside one of the University's data centres.
- ***SaaS*** – Software as a Service. Also known as a "cloud" application. Refers to software solutions that are hosted external to the University e.g., DropBox.

Scope of Applicability

This guideline applies to all staff, titleholders, contractors, visitors and students.

This guideline applies to all information assets generated by or on behalf of the University or otherwise within the University's custody, whether in electronic or physical form.

Information Classification

Information assets shall be classified according to the following classification scheme:

Class	Subtitle	Visual Cue	Definition and Examples
Class 3	Confidential		Significant consequences to the University (e.g. financial, reputational, legal, operational) if security of the information asset were to be compromised. Examples: Personal information (e.g. staff or student records, medical records), unpublished research data or intellectual property with commercial value, commercially sensitive information, information in respect of which the University has confidentiality obligations to a third party
Class 2	University Internal		Information that should not be made available for general public access, but which is not of the level of sensitivity as Class 3 as defined above. Examples: Unpublished research data without commercial value, general business records, teaching materials
Class 1	Public		Information authorised for unlimited public access and circulation. Loss of security has minimal adverse impact on the University. Examples: Published papers, information on websites, primary research data

Information Protection

The following table sets out the measures that should be taken to protect the security of information under each Class.

Class	Protection Guideline
 Confidential	***Use*** • Should have a designated owner and custodian • Should be managed through local University information asset register • Restrict access to persons who have a genuine need to know, and grant the minimum level of access required to perform required function • If electronic, require logon using unique ID and password at the minimum to access • If hardcopy, keep a record of any access or movement of the records • Custodian should perform periodic inventory of people with access • Custodian should keep an electronic log for all access, modifications and deletions • Should be labelled as confidential where practical • Confidentiality obligations must be reinforced to those who have access • If personal information, de-identify before use where practical ***Disposal*** • Paper-based documents must be cross-shredded or disposed using confidential disposal services • Electronic storage media must be destroyed safely in accordance with "National Institute for Standards and Technology's (NIST) Special Publication 800-88: Guidelines for Media Sanitization" • Permanent destruction of official records must be authorised (refer University Records Policy) ***Storage and Backup of electronic data*** • Should be stored using on-premise University-approved electronic storage • Should be encrypted on disk using a University approved encryption scheme

Class	Protection Guideline
	• Should be backed up on a daily basis • Must not be stored on portable storage devices (PSD) without encryption AND explicit approval of the owner • Should avoid use of off-premise "cloud" or SaaS application or storage. Where third party hosting is being contemplated, follow the *Third Party Hosting Security Guideline* • Must store non-electronic (printed) copies in locked cabinets ***Transmission*** • Must be encrypted during electronic transmission • Must not be faxed or sent over plaintext email
University Internal	***Use*** • Do not allow access to persons external to the University unless they have been authorised Must require logon using unique University ID and password at the minimum to access ***Storage and Backup of electronic data*** • Should be stored in a University-approved electronic storage • Should be backed up on a daily basis • Risks of using off-premise "cloud" or SaaS application should be considered carefully using The Third Party Hosting Security Guideline and Checklist. ***Transmission*** • Should be encrypted during electronic transmission where possible
Public	***Use*** • No restrictions ***Disposal*** • No restrictions, subject to compliance with University Records Policy ***Storage and Backup of electronic data*** • Should be backed up daily if it is the original copy ***Transmission*** • No restrictions

Related University Policies

This Guideline should be read and interpreted in conjunction with the following University policies.

IT Acceptable Use and Security Policy

All use of University ICT facilities must comply with the ITAUSP.

University Records Policy

Any information assets that are "official records" of the University as defined in the University Records Policy must be handled and disposed of in accordance with the University Records policy.

Privacy Policy

Any information asset that is deemed personal information as defined in the University Privacy Policy and Management Plan must be stored, handled and disposed of in accordance with the Policy.

Responsible Conduct of Research Policy

Any research data must be managed in accordance with the Responsible Conduct of Research Policy.

Research Data and Primary Materials Policy [Draft]

Any research data and primary materials must be handled in accordance with the Research Data and Primary Materials Policy.