THE UNIVERSITY OF NOTRE DAME AUSTRALIA

Procedure:

Information Management

Effective: 9 April 2024

Audience: employees, students

Policy category: management
Policy sub-category: information management and privacy

Key words:	Cybersecurity, data, information, information security
Procedure Owner:	Chief Information Officer
Responsible Officer:	Director, Cybersecurity and Business Partners
Review Date:	August 2025

Fremantle Broome Sydney

Contents

1 PURPOSE

1.1 This procedure supports the *Policy: Information and Information Technology* by stating requirements for:

1.1.1 classifying information created or received by the University of Notre Dame Australia (the University)

1.1.2 managing university information to which access is restricted

1.1.3 ensuring the quality of data on university systems, and

1.1.4 assessing and managing breaches of the confidentiality and/or security of information held by the University.

1.2 The Interpretation and definitions section at the end of this procedure:

1.2.1 states requirements for interpreting this procedure and

1.2.2 explains its hierarchical relationship with other policy documents in the University's *Policy Framework*.

2 ENDORSEMENT/APPROVAL PATHWAY

2.1 This procedure can only be changed (other than an administrative change as defined in the *Policy Framework*) if the Data Governance Group endorses the change for the Chief Information Officer's approval.

3 CHIEF INFORMATION OFFICER'S INSTRUCTIONS

3.1 Various sections of this procedure provide for the Chief Information Officer (CIO) to maintain instructions to ensure security of the University's information.

3.2 Users of university information systems and of devices provided by the University will follow the CIO's instructions.

4 RELATED POLICIES AND REGULATIONS

4.1 This procedure should be read alongside the *Policy: Information and Information Technology*, which it supports.

4.2 The *Procedure: Information Technology* states requirements for ensuring the security and appropriate use of the University's information systems.

4.3 The *Policy: Critical Incident Management* and *Procedure: Critical Incident Management* state requirements for managing critical incidents, which include serious breaches of information security.

5 CLASSIFICATION OF INFORMATION

5.1 All information held by the University will be classified as having one of the classifications in the following table.

Classification	Risk	Examples	Access
Public	Insignificant	• approved media releases • graduate lists • information for prospective students • information for prospective donors • research outputs already published • public access staff directory information.	Information or Data can be published externally without restriction.
Internal	Low	• committee papers that don't contain commercial-in-confidence information or other sensitive information • curriculum information intended for enrolled students • operational instructions intended for staff • research outputs not yet published • data provided by an external organisation on condition that it is only for use within the University.	Access restricted to: • Staff or students as relevant. • Access is only available to persons who have, as relevant, a staff or student account to access university information.
Sensitive	Medium	• committee papers that contain commercial-in-confidence business information or other sensitive information • personal information of staff or students other than health information • student results • university budget/expenditure information	Access restricted to • Staff who need the information to carry out their role. • Staff who have access to the relevant information system.

Classification	Risk	Examples	Access
		• commercial-in-confidence business information • data provided by an external organisation on condition that its use within the University is restricted to certain groups of staff or for certain purposes • information gathered or generated in research.	
Highly sensitive	High	• contracts • credit card information • health/medical information of staff or students • information generated in handling appeals, complaints and disciplinary proceedings • course experience and experience of teaching survey results that identify individual staff or include students' comments on teachers or courses • legal advice • equity information of individual students • research information that identifies research subjects or cultural information shared with researchers by members of a traditional Aboriginal or Torres Strait Islander community • information the release of which might cause reputational damage to the University	Access restricted to • Staff who need the information to carry out their role. Additional precautions are taken to ensure only authorised staff access this information: for example, the information: • is accessed only from certain computers • cannot be stored on portable devices.

5.2 The Chief Information Officer, in collaboration with business owners of enterprise information systems, will maintain detailed instructions for staff on:

5.2.1 what kinds of information fall under each of the four classifications

5.2.2 restrictions on use, communication and storage of sensitive and very sensitive information, and

5.2.3 secure methods for sharing sensitive and very sensitive information.

5.3 The business owner of an enterprise information system will maintain instructions for users of the system on how to classify information they create or change in the system.

5.4 Staff who operate an enterprise information system (as opposed to merely using it) will:

5.4.1 ensure users of the system follow the instructions on classifying information, and

5.4.2 correct the classification of any information on the system that has been classified incorrectly.

6 SECURITY OF UNIVERSITY-PROVIDED DEVICES AND SOFTWARE, AND REMOVABLE STORAGE MEDIA

6.1 The Chief Information Officer (CIO) will maintain instructions for staff to ensure:

6.1.1 the security of university-provided mobile phones and tablet computers (mobile devices)

6.1.2 the security of personal computers in university workplaces

6.1.3 the security of removable digital storage media

6.1.4 that staff maintain information security in their use of software provided by the University.

6.2 A staff member who uses their own mobile device to access a university information system is expected to take the security precautions required in the CIO's instructions to ensure the security of university-provided mobile devices.

7 PHYSICAL SECURITY OF INFORMATION

7.1 Where an office or work area contains information classified as internal, sensitive or very sensitive, the supervisor of the office or work area will ensure it is not left unattended and unlocked.

8 DECOMMISSIONING OF DIGITAL STORAGE DEVICES

8.1 The Chief Information Officer will maintain instructions for staff to ensure that, before digital storage devices that contain licensed software and/or university information pass out of the University's control, the devices are:

8.1.1 reliably erased, or

8.1.2 destroyed.

9 RETURN OR DELETION OF INFORMATION WHEN STAFF LEAVE THE UNIVERSITY

9.1 The Pro Vice-Chancellor, People and Culture will ensure that the process to offboard staff who are leaving the University requires that they confirm that they have:

9.1.1 returned to the University any hard copy or physical information that is classified as internal, sensitive or very sensitive, and

9.1.2 deleted from all their own computers, mobile devices and removable digital storage

media, any data that is classified as internal, sensitive or very sensitive.

10 INFORMATION SECURITY BREACHES – ASSESSMENT AND ASSIGNMENT

10.1 An information security breach is the suspected or actual release of information classified as internal, sensitive or very sensitive:

10.1.1 to people not authorised to have access to the information, and/or

10.1.2 so that the information is or may be circulating outside the control of the University.

10.2 Where a staff member becomes aware of a possible or actual information security breach, they will initiate the following reporting and assessment process.

10.2.1 The staff member will:

10.2.1.1 immediately report the breach to the IT Service Desk, and

10.2.1.2 as soon as practicable, report the breach to their supervisor.

10.2.1.3 These reports will include the type of data involved and the context, cause and extent of the breach.

10.2.2 The IT Service Desk will raise a ticket for the incident and immediately:

10.2.2.1 inform the Chief Information Officer (CIO) and IT Security Lead, and

10.2.2.2 take whatever remedial action the IT Service Desk can.

10.2.2.3 The IT Service Desk's record of such tickets is the University's register of information security breaches and how they have been managed.

10.2.3 The staff member's supervisor will assess the breach to determine whether an information security breach has in fact occurred.

10.2.3.1 If they conclude that a breach has occurred or may have occurred, the supervisor will immediately contact the IT Security Lead, by phone and email (itsecuritylead@nd.edu.au), to provide:

- a description of the breach
- details of any action they have taken to address the breach and its outcome, and
- advice on whether further action is needed.

10.2.4 The IT Security Lead will:

10.2.4.1 assess the seriousness of the breach in consultation with the relevant directors and manager(s) of the Office of Information Technology (OIT); they may also consult the Legal Office; and

10.2.4.2 keep the CIO informed of the assessment process and resulting assessment.

10.2.5 As an outcome of this assessment, the CIO may decide that the breach:

10.2.5.1 can be handled by the OIT, or

10.2.5.2 is serious enough to initiate the critical incident management process.

10.2.6 If the CIO considers that the breach needs to be managed by the critical incident management process, they will initiate that process.

11 INFORMATION SECURITY BREACHES – MANAGEMENT

11.1.1 Each information security breach will be managed by:

11.1.1.1 assessing the risks of the breach and

11.1.1.2 deciding what actions are needed to mitigate those risks.

11.1.2 To achieve this, the Office of Information Technology will take the following four steps:
- 11.1.2.1 contain the breach and do a preliminary assessment
- 11.1.2.2 evaluate the risks of the breach
- 11.1.2.3 notify those who need to be aware of the breach, then
- 11.1.2.4 prevent future breaches.
- 11.1.2.5 Where the first three of these steps are taken, they should be taken at the same time or close together.
- 11.1.2.6 Depending on the breach, not all these steps may be needed, some steps may be combined or other actions specific to the breach may be needed.

11.1.3 To contain the breach and make a preliminary assessment:
- 11.1.3.1 For a physical breach, alert Campus Security.
- 11.1.3.2 If the breach has resulted from a cyber-attack, it may be continuing: in this case, the IT security team will ensure no more information is released.
- 11.1.3.3 Any evidence should be preserved that may help identify the cause of the breach and/or inform corrective action.
- 11.1.3.4 The preliminary assessment should address the following questions:
  - What steps have already been taken to contain, assess and remedy the breach?
  - What information does the breach involve?
  - What caused the breach?
  - What is the extent of the breach?
  - What harm could arise to persons whose information was released?
  - What other harm might the breach cause?
  - How can the breach be contained?

11.1.4 Where a data breach has involved the release of personal information so it is beyond the control of the University, and there is a risk of harm to the persons whose information has been released, the Chief Information Officer (CIO) will ensure the breach is reported to the Office of the Australian Information Commissioner.

11.1.5 Where a cyber-attack has breached security of an information system, the CIO will report the breach to the Australian Cyber Security Centre.

12 ROLES AND RESPONSIBILITIES

12.1 The *Policy: Information and Information Technology* states general responsibilities of everyone who uses a university information system.

12.2 All staff

12.2.1 A staff member will notify the IT Service Desk as soon as they become aware of:
- 12.2.1.1 a breach of information security, or
- 12.2.1.2 that someone has gained access to university information they are not authorised to access.

12.2.2 Staff will follow any instructions maintained by the Chief Information Officer for secure use of software, personal computers, mobile devices and tablets provided by the University.

12.3 Business owners of information systems

12.3.1 The business owner of an information system will, where an Office of Information Technology audit recommends improvements to the system's security, implement the recommendation in the time frame stated in the audit report.

12.3.2 In addition, the business owner of an enterprise information system will:

12.3.2.1 define processes for access to the system, to ensure

- data quality and
- correct use to 9inimize security risks, and

12.3.2.2 maintain a document of security risks/mitigations for the system

12.4 Chief Information Officer

12.4.1 The Chief Information Officer will:

12.4.1.1 in collaboration with business owners of enterprise information systems, maintain detailed instructions for staff to ensure information security of these systems in matters such as:

- developing software for them
- managing them
- passwords and other credentials for access to them
- protecting against loss of their data
- security patches to them, and
- use of cloud computing services for university information, and

12.4.1.2 maintain instructions for staff to ensure

- secure use of university-provided software, personal computers, mobile devices and tablets, and
- reliable erasure or destruction of university digital storage devices that contain licensed software and/or university information, before these pass out of the University's control, and

12.4.1.3 assess the seriousness of breaches of information security that are reported to the IT Service desk and where appropriate initiate the critical incident management process.

12.4.2 See also the responsibilities of the Office of Information Technology below.

12.5 Director, Analytics, Planning and Reporting

12.5.1 The Director, Analytics, Planning and Reporting will lead, advise on and coordinate data quality improvement, in collaboration with business owners of enterprise information systems.

12.6 Finance Office

12.6.1 The Finance Office will, in collaboration with the Legal Office and Office of Information Technology, ensure that:

12.6.1.1 information technology procurement minimises risks to information security, and

12.6.1.2 third-party information systems used by the University meet the same standards of information security as the University's internal information systems.

12.7 IT Security Lead

12.7.1 The IT Security Lead will promptly investigate breaches of information security reported to the IT Service Desk, keeping the Chief Information Officer informed of the investigation and their conclusions.

12.8 Legal Office

12.8.1 The Legal Office will, in collaboration with the Finance Office and Office of Information Technology, ensure that:

12.8.1.1 information technology procurement minimises risks to information security, and

12.8.1.2 third party information systems used by the University meet the same standards of information security as the University's internal information systems.

12.9 Office of Information Technology

12.9.1 The Office of Information Technology will:

12.9.1.1 lead, advise on and coordinate information security improvements

12.9.1.2 maintain an inventory of university information systems with their security risks and mitigations of these risks

12.9.1.3 conduct regular information security audits of university information systems and make recommendations to improve their security

12.9.1.4 where it considers that a university information system cannot be made secure, collaborate with the business owner of the system to find an alternative system

12.9.1.5 provide ongoing training on information security for staff

12.9.1.6 in collaboration with the Finance Office and Legal Office:

- ensure that information technology procurement 10inimizes risks to information security, and
- ensure that third party information systems used by the University meet the same standards of information security and confidentiality as the University's internal information systems.

12.10 Pro Vice-Chancellor, People and Culture

12.10.1 The Pro Vice-Chancellor, People and Culture will ensure that the offboarding process for staff who are leaving the University requires them to confirm that they have returned hard copy university information to the University and have deleted digital university information from their computers, mobile devices and removable digital storage media.

12.11 Staff who operate an enterprise information system

12.11.1 Staff who operate an enterprise information system (as opposed to staff who merely use the system) will:

12.11.1.1 ensure access is managed in accordance with the processes for access to the system

12.11.1.2 ensure users comply with information security processes for the system

12.11.1.3 cleanse data entered by other staff in the system to ensure its quality is high

12.11.1.4 ensure information created in the system is correctly classified.

12.12 Staff who use an enterprise information system

12.12.1 Staff who use an enterprise information system will:

12.12.1.1 keep their password strong and their password and other access credentials secret

12.12.1.2 follow the processes set by the business owner of the system for access to it and to maintain its information security, and

12.12.1.3 if they create or change data in the system:

- follow the processes set by the business owner of the system to ensure the quality of the data, and
- classify the data correctly.

13 INTERPRETATION AND DEFINITIONS:

13.1 Interpretation

13.1.1 The following rules of interpretation apply to this procedure:

13.1.2 The University's *Policy Framework* sets out the hierarchy of the University's policy documents.

13.1.3 Should any provision in this procedure be inconsistent with a provision of a document higher in the University's hierarchy of policy documents as stated in the *Policy Framework*, the higher document prevails and overrules this procedure to the extent of the inconsistency.

13.1.4 This procedure must be read alongside other closely-related policy documents:

13.1.4.1 the policy that it supports, identified in the Purpose section

13.1.4.2 closely-related policies and regulations listed in the Related policies and regulations sections

13.1.4.3 the *Code of Conduct (Staff)* and *Code of Conduct (Students)*, which include a requirement to comply with policy documents of the University, and

13.1.4.4 any other documents listed in the Related documents section.

13.1.5 Where this procedure uses:

13.1.5.1 the verbs 'will' or 'must', it states a requirement

13.1.5.2 the phrases 'cannot', 'must not' or 'only [position title] can', it states a prohibition

13.1.5.3 the words 'include', 'includes; or 'including' followed by a list, the words 'without limitation' are taken to follow immediately

13.1.5.4 the phrase 'for example' or 'such as' followed by a single instance or list, the instance or list is not exhaustive

13.1.5.5 the phrases 'described in', 'set out in', 'specified in' or 'stated in', it will be read as if the words 'expressly or impliedly' appeared immediately before them;

13.1.5.6 the singular, it also means the plural, and vice versa

13.1.5.7 any gender, it includes the other genders, and

13.1.5.8 a reference to a statute, ordinance, code or other law, it includes regulation, by-laws, rules and other statutory instruments under it for the time being in force and consolidations, amendments, re-enactments, or replacements of any of them.

13.2 Definitions

13.3 For the purpose of this procedure, the definitions stated in the Definitions section of the *Policy: Information and Information Technology* apply.

13.4 The following additional definitions apply to this procedure:

13.4.1 ***Third party information system*** means an information system hosted by an external organisation, used to create, manage or store information of the University.

13.4.2 ***Equity information*** means students who belong to one of the following groups: students with disability, Aboriginal and Torres Strait Islander students, students from low socioeconomic status locations, students from regional and remote parts of Australia, students from non-English speaking backgrounds, and students who are first in their family to attend university, etc.

Version	Date of approval	Approved by	Amendment
1	2 August 2022	Vice Chancellor	Effective date – new procedure.
2	9 April 2024	Chief Information Officer	Minor amendment to define student equity data and include as an example of Highly Sensitive Data.