Data Classification and Handling Policy and Standard

Section 1 - Executive Summary

(1) The University of Newcastle routinely gathers, stores, processes, communicates, and disposes of information. That information must be protected from unauthorised disclosure, damage and loss. At the same time, information must be readily available to those who need it.

(2) Establishing an information classification scheme and the controls appropriate for each classification level is essential for protecting information throughout its lifecycle.

(3) Formalising information classification and protection requirements also enables the University to meet it’s legal obligation to manage personal information in accordance with the Privacy and Personal Information Protection Act 1998 No 133, the Health Records and Information Privacy Act 2002 No 71, the State Records Act 1998, and the University's Privacy Management Plan.

Section 2 - Purpose

(4) This document articulates the University's Information Classification Scheme for information assets and the controls that should be implemented at each classification level.

(5) The appropriate information classification level is determined by the Information Owner and reflects the value and sensitivity of the information and the impact to the University in the event that the information is compromised.

(6) A compromise of information is any loss in the confidentiality, integrity, or availability of that information.

Section 3 - Scope

(7) This Policy and Standard applies to all information created, processed, stored, or communicated by the University.

Section 4 - Audience

(8) All University staff, students, volunteers, vendors, and members of advisory and governing bodies, in all campuses and locations of the University and at all times while engaged in University business or otherwise representing the University.

Section 5 - Information Classification

Principles

(9) The information classification and protection principles of the University are:

a. information is an important asset of the University;
b. the University uses classifications to define the acceptable use and handling of information;
c. information classifications take into account:
    i. the broader goals of the University relating to the generation and sharing of information;
    ii. the value of information to the University; and
    iii. the risks associated with sharing information.
d. Information Owner's are responsible for determining the value of information, assigning classification labels and overseeing the protection of information throughout its lifecycle; and
e. information within systems must be managed to ensure the confidentiality, integrity, and availability of that information, and to meet the University's legal and regulatory responsibilities.

(10) These principles apply to the creation, storage, processing, and communication of all University information and assets, regardless of physical or logical location, storage medium, technology used, format, or the purpose(s) they serve.

(11) Any disputes regarding the appropriate classification of information will be resolved by the Legal and Compliance team.

Information Classification Requirements

(12) Information assets must be classified in terms of legal requirements, sensitivity, criticality, and risk to the University.

(13) If information assets are subject to classification, they must be classified upon their creation by the Information Owner.

(14) If information is received from an external source, the information must be classified by the Information Custodian.

(15) Information assets must be re-classified by the Information Owner upon significant change in legal requirements, sensitivity, criticality, or risk to the University.

(16) Information assets should only be stored, processed, and communicated on system(s) designed to support the classification level and appropriate management of that information.

(17) Information assets must be classified using the University's Information Classification Scheme, which is described in Table 1.

Table 1 – The University of Newcastle Information Classification Scheme

IMPACT TYPE	**SEVERITY**			
	Lowest	<------>		**Highest**
Impact	**Insignificant to Minor**	**Moderate**	**Major**	**Severe**
Security – What advantage does this information provide?	Little or no advantage.	Might provide some advantage.	Definite advantage.	Significant advantage.
Likelihood of malicious persons searching for this information.	Low or no likelihood.	Low	Medium	High
If this asset or information is disclosed, stolen or lost.				

Provision of business operation and service.	Some localised inconvenience, but no impact to the University. Disruption to operations with no permanent or significant effect on University.	Some impact on the University's operational performance. Less impact on strategic goals in the medium term.	Significant effect on operational performance.	Achievement of operational and strategic goals in the medium term jeopardised. Existence of the University under threat.
Compliance / Legal	Breach of legislation, contract, rule or policy that does not have any penalty or litigation impact. Breach of legislation, contract, rule or policy that may have an impact on the relationship with the third party or the legislator, but no long lasting effect. No litigation or prosecution and/or penalty. Regulatory consequence limited to standard inquiries.	Breach of legislation, contract rule or policy leading to escalated legal enquiries. Regulatory or legal consequence limited to additional questioning or review by legislator.	Breach of legislation, contract, rule or policy leading to possible legal action. Possible litigation or criminal prosecution and/or penalty. External enquiry or regulatory review and/or possible negative sanction by a regulatory body.	Breach of legislation, contract, rule or policy leading to significant and costly legal action with widespread potential impact for the University. Litigation or criminal prosecution and/or substantial major negative sanction by a regulatory body.
Employees / WHS	No impact to employees / WHS	Continuity of employment concerns across the University. WHS incident requiring significant medical attention. WHS event reported and investigated.	Significant (up to 15%) loss of staff contained to one college / division. Widespread damage to staff morale. WHS event causing serious injury, or negative environmental impact, and the relevant external authority notified.	Significant loss of staff extending to the entire University (over 15%). WHS event causing serious permanent injury, death or environmental. Impact leading to costly action and widespread impact on the University and/or senior staff.
Financial	Less than 1% of budget or up to $25K. 1 to 2% of budget or $25-50k.	2-5% budget or $250k – 1m.	5-10% budget or $1-5m.	Over 10% of budget or over $5m.
Reputation	No impact to reputation.	Student and/or community concern. National media coverage and external criticism. Reputation impacted with some stakeholders.	Loss of student confidence in a School or College. Sustained adverse national media and public coverage. Reputation impacted with a significant number of stakeholders. Breakdown in strategic and or business partnership.	Loss of student confidence in the University. Reputation and standing of the University affected nationally and internationally. Serious public outcry and/or international coverage. Reputation impacted with majority of key stakeholders. Significant breakdown in strategic and or business partnerships.

Service Levels	Loss of less than one day's teaching, research and/or business functions. Loss of one full day of teaching, research and/or business functions.	Loss of 1-7 days of teaching, research and/or business functions.	Loss of two weeks to two months of teaching, research and/or business functions.	Loss of over two months of teaching, research and/or business functions.
Example information types	College and staff directory information. Course catalogues. Published research data. Course descriptions.	Business unit process and procedure. Unpublished intellectual property. ITC system design and configuration information. Departmental intranet.	Student and Staff HR Data. Organisational financial data. Current exam material. Research Data (containing personal data).	Data subject to regulatory control. Employee relations and complaints information. Medical, Children & Young person's information. Credit card information. Research data (containing personal medical data).
Recommended information classification	Public	X–in-Confidence	Restricted	Highly-Restricted

Alignment with Government Security Classification

(18) The University's Information Classification Scheme broadly aligns with the NSW and Commonwealth information classification schemes as per Table 2.

Table 2 – Alignment of University Information Classification Scheme with Government Security Classification

University	NSW	Commonwealth
Public	UNOFFICIAL and OFFICIAL	UNOFFICIAL and OFFICIAL
X-in-Confidence	OFFICIAL: Sensitive	OFFICIAL: Sensitive
Restricted	PROTECTED	PROTECTED
Highly-Restricted	SECRET	SECRET
N/A	TOP SECRET	TOP SECRET

(19) The NSW and Commonwealth classifications and associated protections must be applied when dealing with state and federal government information. In these scenarios, guidance on implementing data protections must be sought from the Information Owner and from the University's Information Security Team.

Section 6 - Data Protections

Data Protection Requirements

(20) Data protections are defined for each classification level and must be applied throughout the information lifecycle. The protections address data confidentiality, integrity, and availability requirements.

(21) Data protection requirements are described in Table 3.

Table 3 – Data Protection Requirements

Data Protections					
Control Category	**Description of Controls**	**Public**	**X – In confidence**	**Restricted**	**Highly Restricted**
Access Control	No restriction on viewing	X			
	Role-based access to ICT resources and data		X	X	X
	Access to authorised users only		X	X	X
	Authentication and authorisation required for access		X	X	X
	Information Owner must grant permission for access			X	X
	Authorisation by Information owner required for modification	X	X	X	X
	Multi-Factor Authentication recommended		X	X	
	Multi-Factor Authentication required				X
	Non-disclosure agreement required to be signed by third parties		X	X	X
Copying / Printing (paper and electronic forms)	No restrictions	X			
	Should not be left unattended on a printer		X	X	X
	Data should only be printed when there is a legitimate need		X	X	X
	Electronic and physical copies must be labeled according to their data classification		X	X	X
	Copies must be limited to authorised individuals		X	X	X
Network Security	Protection with firewall and Intrusion Prevent System (IPS) required	X	X	X	X
	Access to user interfaces must be via a virtual server or reverse proxy. No direct access to servers permitted for end users	X	X	X	X
	Servers hosting the data should not be visible to the Internet. Presentation layer services should reside in a DMZ network		X	X	X
	Servers hosting the data should not be visible to unprotected internal networks such as Students, Guest & Quarantine				X

Data Protections					
System Security	Systems should be hardened as per vendor hardening guidelines	X	X	X	X
	Apply security patches within defined SLA	X	X	X	X
	Anti-virus software must be installed on all applicable systems, and must be automatically updated with the latest signatures	X	X	X	X
	Host-based firewall enabled in default deny mode, and permit minimum necessary services			X	X
	PC hard drives and removable media must be encrypted		X	X	X
	Data should not be stored or processed on PCs, portable devices, and removable media. Data should remain secured within the University Data Centre environment and encrypted-at-rest.				X
Physical Security	Facility that provides access to data must be locked or logged out when unattended or unused		X	X	X
	Documents and information assets to be stored in approved and supported environments. Approved storage for documents includes locked cupboards and cabinets.		X	X	X
	Must be hosted in a Secure Data Centre			X	X
	Physical access must be monitored, logged, and limited to authorised individuals				X
Remote Access to systems hosting data for administrative purposes	Requires user authentication	X	X	X	X
	Multi-Factor Authentication recommended for roles with administrative access to data		X		
	Multi-Factor Authentication required for roles with administrative access to data			X	X
	Access to administrative interfaces restricted to IT Management networks, or via a Jump Server, or protected with Multi-Factor Authentication			X	X
	Remote access by third party for technical support limited to authenticated VPN, or via supervised session utilising Zoom, WebEx or similar		X	X	X
	Unsupervised remote access by third party, such as an application vendor, for technical support is not allowed, unless covered by an appropriate formal agreement stipulating data handling requirements equivalent to or stronger than those in this document		X	X	X
Audit logs	Log login and logoff events, and login failures		X	X	X
	Log delete events			X	X
	Forward logs to a remote log management server (SIEM)			X	X
	Log read and write events			X	X
Transmission of data	Encryption required (e.g. HTTPS, SCP, SFTP)		X	X	X
	Must not be sent via email unless encrypted		X	X	X

Data Protections					
Backups	Daily backups required	X	X	X	X
	Geographically dispersed storage required			X	X
Disposal	All disposals of data (electronic and hard copy) must be made in accordance with the appropriate General Disposal Authority (GDA) – University Record Retention and Disposal	X	X	X	X
	Paper-based information shredded and placed in managed confidential bins		X	X	X
	Wipe, erase or destroy electronic media such as hard drives, USBs, CD and DVDs		X	X	X

Section 7 - Roles and Responsibilities

Information owner

(22) The Information Owner is the person responsible for the business use of the information asset. The Information Owner is the authoritative head of the respective College, School, Division or Unit within the University.

(23) The Information Owner is responsible for collecting, creating, retaining and maintaining information within their assigned area of control, coupled with the responsibility to protect that information on behalf of the University.

(24) The Information Owner may delegate some operational responsibilities but will retain overall responsibility.

(25) The Information Owner is required to:

a. determine the statutory requirements regarding privacy and retention and any risks associated with the data;
b. assign an appropriate classification;
c. define the method for applying classification labels;
d. authorise access to the information;
e. specify any additional handling controls needed to ensure the confidentiality, integrity, and availability of the information;
f. communicate the control requirements to the information custodian and to users of the information;
g. develop a disaster recovery or business continuity plan for the information to the Information Custodian, which identifies:
    i. any potential risks; and
    ii. vital information.

Information Custodian

(26) Information Custodians are those individuals who control information assets and information systems regardless of physical or logical location, storage medium, technology used, format, or the purpose(s) they serve. In most cases, Digital Technology Solutions will act as the Information Custodian.

(27) The Information Custodian defines information systems architecture and provides technical consulting assistance to Information Owners so that information systems can be built and operated to best meet business objectives.

(28) Information Custodians are responsible for safeguarding the information assets in their possession, including implementing access control systems to prevent inappropriate disclosure, as well as developing, documenting, and

testing disaster recovery or business continuity plans as defined by Information Owners.

(29) In cases in which the information being stored is paper-based, and not electronic, the Information Custodian responsibilities will logically fall to the department gathering the information. For such systems, Digital Technology Solutions or Records Governance Services (RGS) can offer guidance or provide opportunities for digitisation.

Information User

(30) Information Users are individuals who have been granted explicit authorisation by the relevant Information Owner to access, use, alter, or destroy information within an information system.

(31) An Information User will be responsible for:

a. using the information only for the purpose intended and authorised by the Information Owner;
b. complying with all controls established by the Information Owner and Information Custodian;
c. ensuring that restricted and highly-restricted information is not disclosed to anyone without the permission of the Information Owner;
d. only destroying information in accordance with the requirements of the Records Governance Policy.

(32) When dealing with state or federal government classified data, advice must be sought from the Information Security Team to ensure appropriate data protections are applied.

Status and Details

Status	Current
Effective Date	24th January 2024
Review Date	8th December 2025
Approval Authority	Chief Digital & Information Officer
Approval Date	24th January 2024
Expiry Date	Not Applicable
Responsible Executive	David Toll Chief Operating Officer
Enquiries Contact	Information Security Team

Glossary Terms and Definitions

"University" - The University of Newcastle, a body corporate established under sections 4 and 5 of the University of Newcastle Act 1989.

"Risk" - Effect of uncertainty on objectives. Note: An effect is a deviation from the expected, whether it is positive and/or negative.

"Asset" - Any tangible or intangible item (or group of items) that the University owns or has a legal or other right to control and exploit to obtain financial or other economic benefits.

"Course" - When referring to a course offered by the University, a course is a set of learning activities or learning opportunities with defined, assessed and recorded learning outcomes. A course will be identified by an alphanumeric course code and course title. Course types include core courses, compulsory courses, directed courses, capstone courses and electives. For all other uses of this term, the generic definition applies.

"Credit" - When referring to course credit, credit is the recognition of equivalence in content and learning outcomes between different types of learning and/or qualifications. Credit can reduce the amount of learning required to achieve a qualification. For all other uses of this term, the generic definition applies.

"Personal information" - Has the same meaning as in the Privacy and Personal Information Protection Act 1998 (NSW).

"Student" - A person formally enrolled in a course or active in a program offered by the University or affiliated entity.

"Information asset" - A body of information, knowledge or data that is organised as a single entity and has value to the University.

"Information Owner" - A senior business, college or unit manager whom the University has authorised to collect, create, retain and maintain information within their assigned area of control.

"Intellectual property" - Intellectual property (IP), as defined by the World Intellectual Property Organisation, refers to creations of the mind: inventions; literary and artistic works; and symbols, names and images used in commerce. Intellectual property is divided into two categories: Industrial property includes patents for inventions, trademarks, industrial designs and geographical indications; and Copyright covers literary works (such as novels, poems and plays), films, music, artistic works (e.g. drawings, paintings, photographs and sculptures) and architectural design. Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings, and broadcasters in their radio and television programs.

"Research" - As defined in the Australian Code for the Responsible Conduct of Research, or any replacing Code or document.

"School" - An organisational unit forming part of a College or Division, responsible for offering a particular course.

"Senior staff" - Deputy Vice-Chancellor, Pro Vice-Chancellor, Global Innovation Chair, Global Innovation Professorial Fellow, Head of School, Director or equivalent.

"Staff" - Means a person who was at the relevant time employed by the University and includes professional and academic staff of the University, by contract or ongoing, as well as conjoint staff but does not include visitors to the University.

"Third party" - A person or group other than the University or any of the University's partner institutions.

"College" - An organisational unit established within the University by the Council.