Information Security Data Classification and Handling Manual

Section 1 - Audience

(1) All University staff, vendors, students, volunteers, 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 2 - Executive Summary

(2) The University of Newcastle routinely gathers, stores, processes, transmits and disposes of information. That information must be protected from unauthorised disclosure, misuse and misrepresentation. At the same time, it must be readily available to those who need it. The classification of information in terms of its business criticality is an essential element in achieving appropriate information security.

(3) This manual outlines the University's standard data classifications, and the standard handling controls required to protect University information.

(4) This manual supports the University's legal obligation to ensure that private information is managed in accordance with the principles outlined in 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. The provisions of these must be taken into account while applying these minimum standards.

Section 3 - Purpose

(5) This manual seeks to ensure the consistent application of controls to the University's information asset and ICT resources by establishing appropriate data classification labels. These classifications are determined by the Information owner, and are based on the sensitivity of the information and the potential impact on the University in the event that the information is disclosed, misused, misrepresented or lost.

Section 4 - Data Classification

Principles

(6) The following are the data classification principles of the University:

a. information is an important asset of the University;
b. the University uses data classifications to define the acceptable use and handling of information;
c. data classifications take into account:
    i. the broader goals of the University, both to share and restrict access to information; and
    ii. the impacts associated with restricting access to, and also the sharing of, information;

d. the Information owner is responsible for determining the value of information within information systems and assigning an appropriate data classification label;
e. data classifications are assigned on the basis of the information's value, legal requirements, sensitivity and criticality to the University;
f. information within information systems is managed throughout its lifecycle:
    i. to ensure the confidentiality, integrity and availability of information; and
    ii. to achieve compliance with the University's legal and regulatory responsibilities;
g. these principles apply to all University information assets stored and processed on all ICT systems and assets, regardless of physical or logical location, storage medium, technology used, or the purpose(s) they serve; and
h. any disputes regarding the appropriate data classification of information will be resolved by the University's Legal & Compliance unit.

Data Classification

(7) Information and assets shall be classified in terms of their value, legal requirements, sensitivity, and criticality to the University. If information is subject to classification, it shall be classified upon its creation by the Information owner according to the below guidelines and shall be re-classified by the Information owner upon any significant change in content.

IMPACT TYPE	**SEVERITY**			
	Lowest	<------>		**Highest**
Impact	**Insignificant to Minor**	**Moderate**	**Major**	**Severe**
Security – What competitive advantage does this information provide.	Little or no advantage.	Might provide some advantage.	Definite advantage.	Significant Advantage.
Likelihood of the competitors looking for this information.	Low or No Possibility.	Low Possibility.	Medium Possibility.	High Possibility.
If this asset or information is disclosed, stolen or lost.				
General / 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).
DATA CLASSIFICATION	Consider for PUBLIC OR UNCLASSIFIED	Consider for X – In Confidence	Consider for Restricted	Consider for HIGHLY Restricted

Alignment with Government Security Classification

(8) The University Data Classifications align to the NSW and Commonwealth security classification as follows:

University	NSW	Commonwealth
Public	Unclassified	Information not requiring additional protection
X-in-Confidence	PROTECTED	PROTECTED
Restricted	CONFIDENTIAL	CONFIDENTIAL
Highly-Restricted	SECRET	SECRET
N/A	TOP SECRET	TOP SECRET

(9) The University does not use dissemination limiting markers (DLMs) nor does it use the classification TOP SECRET when classifying information. DLMs and the Top Secret classification must only be used when required by state or federal obligations.

Section 5 - Data Handling

Data Handling Requirements

(10) Most official information does not need increased security and may be marked 'Public' or left unmarked. This should be the default position for newly created material, unless there is a specific need to protect the confidentiality of the information.

(11) For each data classification, several data handling requirements are defined to appropriately safeguard the information. It is important to understand that overall sensitivity of institutional data encompasses not only its confidentiality but also the need for integrity and availability.

(12) Role based enforcement of data handling controls should be configured wherever possible, to ensure that controls are appropriate for the information available to each role.

(13) The following table lists required safeguards for protecting data based on the data classification. The table lists some of the key information and data handling requirements, and requirements are not limited to this list.

Data Handling					
Control Category	**Description of Controls**	**Public**	**X – In confidence**	**Restricted**	**Highly Restricted**

Data Handling					
Access Control	No restriction on viewing	X			
	Authorisation by Information owner required for modification	X	X	X	X
	Restricted to authorised users only		X	X	X
	Authentication and authorisation required for access		X	X	X
	Information owner grants permission for access			X	X
	Multi-Factor Authentication recommended		X	X	
	Multi-Factor Authentication required				X
	Non-disclosure agreement required to be signed by third parties				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
	Electronic and physical copies must be labeled according to their data classification				X
	Copies must be limited to authorised individuals				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
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
	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

Data Handling					
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 secure environments		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	X	
	Multi-Factor Authentication required for roles with administrative access to data				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
	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
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
Transmission of data	Encryption required (e.g. HTTPS, SCP, SFTP)		X	X	X
	Must not be sent via email unless encrypted			X	X
Backups	Daily backups required	X	X	X	X
	Off-site storage recommended			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		X	X	X
	Wipe, erase or destroy electronic media such as hard drives, USBs, CD and DVDs		X	X	X

Section 6 - Roles and Responsibilities

Information owner

(14) 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.

(15) The Information owner is given the authority to collect, create, retain and maintain information within their assigned area of control, coupled with the responsibility to protect that information on behalf of the University.

(16) The Information owner may delegate some operational responsibilities, but will retain accountability.

(17) The Information owner is required to:

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

Information Custodian

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

(19) 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.

(20) 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.

(21) 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, Information Technology or Records Governance Services (RGS) can offer guidance or provide opportunities for digitisation.

Information User

(22) 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.

(23) 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 and Information Management Policy.

Status and Details

Status	Current
Effective Date	17th June 2019
Review Date	17th June 2021
Approval Authority	Chief Information Officer
Approval Date	17th June 2019
Expiry Date	Not Applicable
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 means the principle of accepting a student's prior learning or previous studies as being, in whole or in part, either identical to or the equivalent of studies contributing to a University of Newcastle award. For all other uses of this term, the generic definition applies.

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

"ICT resources" - All information and communication technology resources and facilities.

"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.

"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.