Information Security Data Classification Procedure

Section 1 - Procedure

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.

Executive Summary

(2) The University of Newcastle routinely gathers, stores, processes, transmits and disposes of records containing 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. Classification of information in terms of its business criticality is an essential element in achieving appropriate information security.

(3) This procedure 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 and the State Records Act 1998, and the Universities Privacy Management Plan. The provisions of these Acts must be taken into account while applying this procedure.

Purpose

(4) This procedure seeks to apply effective security controls to the University's information systems by establishing appropriate information classification labels. These classifications are identified by the Information owner. These classifications 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.

(5) This procedure endorses the University's Information Security Policy requirements.

Procedure Principles

(6) The following are the principles of this procedure:

a. Information is an important asset of the University.
b. The University uses information security classification levels to define the acceptable use of information.
c. Information security classifications take into account:
    i. the broader goals of the University, both to share and restrict access to information, and
    ii. the impact associated with such needs.
d. The Information owner is responsible for determining the value of information within information systems and assigning an appropriate Security Classification label.
e. Information security classifications are assigned on the basis of the sensitivity level of the data.
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. This procedure applies to all information assets including all ICT systems and assets regardless of physical or logical location, storage medium, technology used, or the purpose(s) it serves.
h. A mechanism will exist to ensure that the classification level assigned to a particular subset of information is appropriate. This mechanism will take into account the need to reclassify information throughout its life cycle.
i. Any disputes regarding the appropriate classification of information will be resolved by the University's Legal Office.

Information Classification

(7) Information and assets shall be classified in terms of its value, legal requirements, sensitivity, and critically to the University. If information is subject to classification, it shall be classified upon its creation by the Information owner according to below guidelines and shall be re-classified by the Information owner upon any significant change in content. Information owners and respective IT Asset owners shall observe the following information classifications:

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&E	No impact to employees / WHS&E	Continuity of employment concerns across the University. WHS&E incident requiring significant medical attention. WHS & E event reported and investigated.	Significant (up to 15%) loss of staff contained to one faculty / division. Widespread damage to staff morale. WHS&E even 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&E 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 Faculty. 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 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	Faculty 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).
SECURITY CLASSIFICATION	Consider for PUBLIC OR UNCLASSIFIED	Consider for X – In Confidence	Consider for Restricted	Consider for HIGHLY Restricted

Data Handling Requirements

(8) For each 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.

(9) The following table lists required safeguards for protecting data based on their 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**
Access Control	No restriction on viewing	X			
	Restricted to University related individuals		X	X	X
	Information owner grants permission for access		X	X	X
	Authentication and authorisation required for access		X	X	X
	Viewing and modification restricted to authorized individuals as needed for business-related roles			X	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
	Copies must be limited to individuals with a need to know				X
Network Security	May reside on public network	X			
	Protection with firewall and Intrusion Prevent System (IPS) required		X	X	X
	Servers hosting the data should not be visible to the Internet			X	X
	Servers hosting the data should not be visible to unprotected internal networks such as Students				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
	Laptop hard drives must be encrypted				X
Physical Security	Must be locked or logged out when unattended	X	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

Data Handling					
Remote Access to systems hosting data	No restrictions unless for system administrative purposes.	X			
	Requires user authentication		X	X	X
	Access restricted to campus network or VPN			X	X
	Remote access by third party for technical support limited to authenticated VPN			X	X
	Two-Factor authentication recommended			X	X
	Unsupervised remote access by third party for technical support not allowed				X
Audit logs	Log login and logoff events	X	X	X	X
	Log fail and delete events			X	X
	Forward logs to a remote log server			X	X
	Log read and write events				X
Transmission of data	Encryption required (via TLS or secure file transfer protocols)		X	X	X
	Must not be sent via email unless encrypted				X
Backups	Daily backups required		X	X	X
	Off-site storage recommended			X	X
	Off-site storage in a secure location required.			X	X

Section 2 - Roles and Responsibilities

Asset / Data / Information Owner

(10) Information processed by an information system will have an information owner. This responsibility will be formally assigned and documented.

(11) Information owners will be senior business or faculty unit managers who have been given the authority to collect, create, retain and maintain information and information systems within their assigned area of control.

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

(13) The Information owner will be required to:

a. determine the value of the information within the information system.
b. determine the statutory requirements regarding privacy and retention;
c. assign an appropriate security classification label in consultation with the Records Governance Services and staff in the Governance Advisory Services Unit.
d. assign custody of the information;
e. authorise access to the Information;
f. specify controls to ensure confidentiality, integrity and availability;
g. communicate the control requirements to the custodian and users of the information;
h. develop a disaster recovery or business continuity plan for the information which identifies:
    i. any potential risks, and

ii. vital information, and

i. communicate this to the Information Custodian.

Information Custodian

(14) Information Custodians are those individuals who control information systems regardless of physical or logical location, storage medium, technology used, or the purpose(s) they serve.

(15) The Information Custodian will be responsible for the administration of controls as specified by the owner. This will include:

a. evaluating the cost-effectiveness of controls based on the classification attributed by the owner;
b. implementing physical and/or technical controls;
c. administering access to information;
d. ensuring the availability of information by implementing appropriate recovery options based on the business criticality of the information in their possession, as per the disaster recovery or business continuity plan produced by the Information owner.

Information User

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

(17) An Information User will be responsible for:

a. using the information only for the purpose intended by the owner;
b. complying with all controls established by the owner and custodian;
c. ensuring that classified or sensitive information is not disclosed to anyone without the permission of the owner;
d. only destroying information in accordance with the requirements of the Records and Information Management Policy.

Status and Details

Status	Historic
Effective Date	30th May 2018
Review Date	30th May 2019
Approval Authority	Chief Information Officer
Approval Date	30th May 2018
Expiry Date	16th June 2019
Responsible Executive	Anthony Molinia Chief Digital & Information Officer +61 49138713
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.

"Campus" - means any place or premises owned or controlled by the University, but may also specifically refer to a designated operating location such as the Callaghan Campus.

"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.

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

"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.

"Term" - When referring to an academic period, term means a period of time aligned to an academic year for the delivery of a course in which students enrol and for which they are usually charged fees for example semesters, trimesters, summer, winter or full-year term. The academic year for a term is determined by the academic year in which the course commences, not concludes. For all other uses of this term, the generic definition applies.

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