Physical and Environmental Security Policy and Standard

Section 1 - Executive Summary

(1) The University is obligated to protect the people, information, and physical assets within its facilities. This requires the minimisation of the risk of harm to people; and the risk of information and physical assets being made inoperable or inaccessible, or being accessed, used, or removed without authorisation.

(2) Physical and environment protections must be applied using a risk-based approach and in proportion to the classification and criticality of information and physical assets.

(3) Responsibilities for implementing physical and environmental protections are shared across Infrastructure and Facilities Services (IFS), Digital Technology Solutions, System Owners and Information Owners.

Section 2 - Scope

(4) This document establishes the physical and environmental safeguards for the University's information and physical assets, with a focus on secure areas.

(5) Secure areas are areas where sensitive, classified, or critical information and assets are used, processed, stored, or communicated.

(6) All other areas of the University are protected using controls designed and managed by IFS.

Section 3 - Physical and Environmental Security Requirements

Part A - Secure Areas

Physical Security Perimeter

(7) University data centre facilities and rooms containing server infrastructure must be protected by a physical security perimeter.

(8) System Owner's must ensure appropriate controls are in place to establish secure areas. The selection of controls must be supported by a risk assessment.

(9) Controls that must be applied to secure areas are:

a. the perimeters of buildings containing data centres or server infrastructure must be physically sound (i.e. there must be no gaps in the perimeter or areas where a break-in could easily occur);
b. external walls must be of solid construction and all external doors must be suitably protected against

unauthorised access with control mechanisms, e.g. bars, alarms, locks, etc;

c. doors and windows must be locked when unattended;
d. doors must be fitted with an audible alarm that triggers when the doors have been kept open beyond a pre-determined length of time;
e. external protection must be considered for windows, particularly at ground level;
f. all fire doors on a security perimeter must be alarmed and monitored; and
g. fire doors and external walls must be tested at least annually, to establish the required level of resistance in accordance with suitable regional, national, and international standards.

(10) Where appropriate, data centre entry points must be monitored by a closed-circuit television (CCTV) system on a 24/7 basis. All video surveillance data must be protected from unauthorised disclosure, modification, and erasure, and maintained for at least 30 days. Refer to the University Closed Circuit Television (CCTV) Policy for further information.

Physical Entry Controls

(11) Secure areas must be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

(12) The following controls must be implemented:

a. access to areas where sensitive information is processed or stored must be restricted to authorised personnel only;
b. authentication controls, e.g. access control card system, must be used to authorise and validate access;
c. access logs must be maintained by for facilities and IT systems;
d. visitors must be escorted whilst in buildings by authorised personnel;
e. visitors must only be allowed access for specific and authorised purposes and be escorted whilst in buildings;
f. the date and time of entry and departure of visitors must be recorded;
g. all employees and other authorised personnel must wear visible identification;
h. visitors must be issued badges or tags of a different colour than employees;
i. employees must notify a University Security Officer when they encounter unescorted visitors or anyone not wearing visible identification;
j. contractors and vendors may be granted restricted access only when required and their access must be authorised and monitored; and
k. access rights must be regularly reviewed by the business unit granting access.

Securing Offices, Rooms and Facilities

(13) Controls to ensure security of information and information systems located in University offices, rooms and other facilities must be designed, applied, and documented.

(14) Information Owners and DTS Security Officers must regularly assess the security of areas where sensitive information is processed and/or stored. Controls that should be implemented to manage associated risks are:

a. physical entry controls described in clauses 11 and 12 of this document;
b. ensure sensitive information is stored properly when not in use, in accordance with clauses 54 to 57 of this document; and
c. directories that identify the locations of data centres and other areas where sensitive information is stored must not be made public.

Protecting Against External and Environmental Threats

(15) Physical protection against natural disasters, malicious attacks or accidents must be designed and applied. Information Owners, System Owners planners and architects must incorporate, to the extent possible, physical security controls that protect University information and assets against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of disasters. Consideration must be given to any security threats presented by neighbouring premises or streets. In addition to building code and fire regulations:

a. combustible or hazardous materials must be stored at a safe distance from the secure area;
b. bulk supplies, e.g. stationery, must not be stored in a secure area;
c. backup equipment and media must be located at a safe distance to avoid damage from a disaster affecting the main site; and
d. environmental alarm systems, fire suppression and firefighting systems must be installed and tested.

Working in Secure Areas

(16) Security controls and procedures must be used by personnel when working in secure areas.

(17) Information Owners must identify and document requirements that apply to personnel who have been authorised to work in secure areas. Authorised personnel must be informed that:

a. sensitive information cannot be discussed in a non-secure area;
b. sensitive information cannot be disclosed to personnel who do not have a need-to-know; and
c. visitors must be authorised, logged, and escorted.

Delivery and Loading Areas

(18) Access points such as reception, delivery and loading areas must be controlled and, if possible, isolated from secure areas or offices to avoid unauthorised access.

(19) Information Owners, System Owners, planners and architects must ensure that:

a. loading docks and delivery areas must be regularly inspected and actively monitored;
b. incoming material must be inspected for potential threats before this material is moved from the delivery and loading area to the point of use;
c. incoming material must be registered on entry to the site; and
d. incoming and outgoing shipments must be physically segregated where possible.

Public Areas

(20) Public areas are areas that are freely accessible to the public, students, and visitors to the University.

(21) The value of IT assets situated in public areas should either be low (e.g. desktop PCs in general access areas) or the assets should be physically large to avoid theft (e.g. printing facilities or print credit kiosks).

(22) All equipment not intended for public use should be situated to minimise the risks of unauthorised access, and the compromise of information.

(23) Systems located in public areas that may be used to access confidential information must be situated in such a way as to prevent unauthorised individuals from viewing the displayed data.

(24) All publicly accessible IT assets should be appropriately defended against vandalism, modification, and theft.

Part B - Equipment

Equipment Protection

(25) Equipment must be protected to reduce the risks of unauthorised access, environmental threats, and hazards.

(26) System Owners, planners and architects must ensure that University facilities are designed in a way that will safeguard sensitive information and assets.

(27) Servers, routers, switches, and other centralised computing equipment must be located in a room with access restricted to only those personnel who require it.

(28) Equipment should be located, and monitors angled, in such a way that unauthorised persons cannot observe the display.

(29) Staff printers and scanners should not be located in an area that is accessible to the public.

Supporting Utilities

(30) ICT infrastructure must be protected from power supply interruption and other disruptions caused by failures in supporting utilities.

(31) The following controls must be implemented to help ensure availability of critical services:

a. all supporting utilities such as electricity, water supply, sewage, heating/ventilation and air conditioning must be adequate for the systems they are supporting. Supporting utilities must be regularly inspected and, as appropriate, tested to ensure their proper functioning and to reduce any risk of malfunction or failure;
b. an uninterruptible power supply (UPS) to support orderly close down or continuous running is recommended for equipment supporting critical business operations. Power contingency plans must cover the action to be taken on failure of the UPS. A back-up generator must be considered if processing is required to continue in the event of a prolonged power failure. An adequate supply of fuel must be available to ensure that the generator can perform for a prolonged period. UPS equipment and generators must be checked regularly to ensure they have adequate capacity and are tested in accordance with the manufacturer's recommendations;
c. emergency power off switches must be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting must be provided in case of main power failure;
d. the water supply must be stable and adequate to supply air conditioning, humidification equipment, and fire suppression systems (where used). An alarm system to detect malfunctions in the supporting utilities must be installed to limit any damage that a fault may cause to equipment;
e. telecommunications equipment must be connected to the utility provider by at least two diverse routes to prevent failure in one connection path impacting voice or data services; and
f. voice services must be adequate to meet local legal requirements for emergency communications.

Cabling Security

(32) Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage.

(33) Power and telecommunications lines into information processing facilities must be underground or subject to adequate alternative protection.

(34) Network equipment must be protected from unauthorised physical access or damage by placing it within a secured data centre, or a locked cabinet or room.

(35) Power cables should be segregated from communications cables to prevent interference.

(36) Cables and equipment must be clearly marked to minimise handling errors such as accidental patching of incorrect network cables. A documented patch cabling standard should be used to reduce the possibility of errors.

Equipment Maintenance

(37) Equipment must be correctly maintained to help ensure availability and integrity of sensitive information and assets.

(38) When equipment is serviced, System Owners must consider the sensitivity of the information it holds, and the value of the assets. System Owners must ensure the following controls are applied:

a. equipment must be maintained in accordance with the supplier's recommended schedule and specifications;
b. only formally contracted maintenance personnel undertake repairs and service equipment;
c. records of all suspected faults and maintenance activity are maintained by IFS;
d. maintenance activity is scheduled at a time of day that limits interference with services or operations; and
e. users are notified before equipment is taken off-line for maintenance.

(39) If off-site maintenance is required, appropriate controls must be implemented; confidential information should be cleared from the equipment, maintenance personnel should be sufficiently cleared, and appropriate supplier relationship agreements should exist to ensure the appropriate protection of information.

Removal of Assets

(40) University-owned equipment, information and software must not be removed from University premises without appropriate authorisation by a senior staff member (or their nominee).

(41) An inventory of IT assets must be maintained, which notes equipment that has been removed from the University. The inventory must include:

a. item description and serial number;
b. where the asset is (or will be) located;
c. the name of the individual responsible for the asset;
d. the removal date and return date; and
e. the reason for removal.

(42) The description and serial numbers must be verified when the asset is returned.

(43) Personnel involved in the removal must be informed of and accept responsibility for protection of the asset.

Security of Equipment and Assets Off-Premises

(44) Assets must be safeguarded using documented security controls when off-site from University premises.

(45) System Owners must ensure that equipment used or stored off-site is safeguarded in accordance with the value of the asset and the sensitivity of information stored on it. Controls to apply include:

a. encrypting sensitive data;
b. using a logical or physical access control mechanism (such as a password) to protect against unauthorised access;
c. using a physical locking or similar mechanism to restrain the equipment; and

d. ensuring personnel are instructed on the proper use of the chosen controls.

(46) Personnel in possession of University equipment must:

a. not leave it unattended in a public place;
b. ensure the equipment is under their direct control at all times when travelling;
c. take measures to prevent viewing of sensitive information by unauthorised personnel;
d. not allow unauthorised individuals to use the equipment; and
e. report loss or stolen equipment immediately.

(47) Due care must be taken by University staff when travelling with a laptop or other equipment holding sensitive information. Specific security mechanisms, such as strong authentication and encryption, must be considered for the devices according to the classification of the data stored on each device.

Secure Disposal or Re-Use of Equipment

(48) All data and software must be erased from equipment prior to disposal or redeployment.

(49) System Owners must consider the sensitivity of information and the value of the assets when determining whether or not hardware or media will be re-used or destroyed.

(50) Prior to re-use within the University:

a. the integrity of the University records must be maintained by adhering to the Records Governance Policy;
b. information and software must be backed up by the original System Owner in case information recovery is required; and
c. the storage media must be wiped.

(51) Storage media that will no longer be used in the University must be wiped by a method approved by the Information Security Team. Asset inventories must be updated to record details of the data wiping including:

a. asset identifier;
b. date of erasure; and
c. names of personnel performing the erasure.

(52) When a supplier conducts the data wiping there must be contractual and audit procedures to ensure complete destruction of the information. The University must receive certification that the destruction has occurred.

Unattended User Equipment

(53) Unattended equipment must be safeguarded by:

a. terminating the active session when finished;
b. locking the session with a password protected screen saver or other approved mechanism;
c. logging off computers, servers, terminals, and other devices when session is finished;
d. switching off devices when not required;
e. enabling password protection on mobile devices, printers, kiosks, and portable storage devices; and
f. securing devices with a cable lock when enhanced physical security is justified.

Clear Desk and Clear Screen Policy

(54) Sensitive information must be safeguarded from unauthorised access, loss, or damage.

(55) Workspaces must be secured when they cannot be monitored by staff. Workspaces can be secured by:

a. clearing desktops and work areas;
b. locking hard copy sensitive information in an appropriate cabinet;
c. locking portable storage devices with sensitive information in an appropriate cabinet;
d. activating a password-protected screen saver;
e. retrieving documents from printers; and
f. ensuring that sensitive hard copy documents that are no longer needed are placed in shredding bins, not recycle bins.

(56) When visitors, cleaning contractors, or other staff without a “need-to-know” are in the area, sensitive information must be safeguarded by:

a. covering up and maintaining control of hard-copy files;
b. minimising windows, blanking computer screens or activating the password-protected screen saver.

(57) Sensitive information must not be discussed in public or other areas where there is a risk of being overheard by unauthorised personnel.

Part C - Defence Industry Security Program (DISP)

(58) Prior to agreeing to store, process, or communicate information or assets under DISP, approval from the Information Security Team must be obtained.

(59) The Information Security Team must ensure that physical security controls required by the Defence Security Policy Framework (DSPF) are implemented when approving activity under the DISP.

Status and Details

Status	Current
Effective Date	8th December 2022
Review Date	8th December 2025
Approval Authority	Chief Information Officer
Approval Date	5th December 2022
Expiry Date	Not Applicable
Responsible Executive	David Toll Chief Operating Officer
Enquiries Contact	Infrastructure and Facilities Services

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.

"Risk assessment" - The overall process of risk identification, risk analysis, and risk evaluation.

"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.

"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.

"Personnel" - In relation to a party, any employee, officer, agent, contractor, sub-contractor, student or volunteer of that party.

"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.

"System Owner" - An authorised individual who has been allocated responsibility by the University and is held accountable for an ICT resource.