Physical and Environmental Security Policy

Section 1 - Executive Summary and Purpose

(1) The University of Newcastle (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 minimisation of the risk of information and physical assets being made inoperable or inaccessible, or being accessed, used, or removed without authorisation.

(2) This Policy establishes the physical and environment protections to the University's information and physical assets that must be applied and establishes the responsibilities for implementing physical and environmental protections.

(3) This Policy should be read in conjunction with:

a. Digital Security Policy;
b. Information Classification and Protection Policy; and
c. Information Security Access Control Policy.

Section 2 - Scope

(4) This document applies to the University and it’s onshore controlled entity's information and physical assets, including secure areas.

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

Section 3 - Physical and Environmental Security Requirements

Part A - Secure Areas

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

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) The following controls must be applied to secure areas:

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. all doors on a security perimeter must secured; and
f. fire doors must be tested at least annually to comply with the Building Code of Australia (Building Code).

(10) Where appropriate, data centre entry points must be monitored by a closed-circuit television (CCTV) system on a 24/7 basis. Refer to the University Closed Circuit Television (CCTV) and Security Recordings Operational 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) Access to secure facilities must be authorised by an Information Owner, System Owner, or a Senior Leader.

(13) 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:
    i. only be allowed access for specific and authorised purposes;
    ii. be escorted by authorised personnel whilst in secure areas;;
    iii. be issued badges or tags of a different colour than staff;
    iv. have their date and time of entry and departure recorded;
e. all employees and other authorised personnel must wear visible identification;
f. staff must notify a University Security Officer when they encounter unescorted visitors or anyone not wearing visible identification;
g. visitors engaged under a supply contract may be granted restricted access only when required and their access must be authorised and monitored; and
h. access rights must be regularly reviewed by the business unit granting access.

Securing Offices, Rooms and Facilities

(14) Information Owners 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 this document; and
b. appropriate storage of sensitive information when not in use, in accordance with this document.

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 the Building Code and AS1851-2012 Routine Service of Fire Protection Systems and Equipment:

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. environmental alarm systems, fire suppression and firefighting systems must be installed, tested and maintained.

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) Receiving staff members and employees of onshore controlled entities must ensure that:

a. loading docks and delivery areas are regularly inspected and actively monitored;
b. incoming material are inspected for potential threats before this material is moved from the delivery and loading area to the point of use;
c. incoming material is registered on entry to the site.

Part B - 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) IT assets 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 C - 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) Critical ICT infrastructure, including network components and servers, 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 for equipment supporting critical business operations must be installed. Power contingency plans must cover the action to be taken on failure of the UPS.
c. 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.
d. UPS equipment and generators must be checked regularly to ensure they have adequate capacity and are tested in accordance with the manufacturer’s recommendations;
e. 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;
f. 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;
g. 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
h. 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 who have been subject to the University's procurement processes may undertake repairs and service equipment;
c. records of all suspected faults and maintenance activity must be maintained by IFS; and
d. maintenance activity must be scheduled at a time of day that limits interference with services or operations; and

(39) Users should be notified before equipment is taken off-line for maintenance wherever possible.

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

Removal of Assets

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

Security of Equipment and Assets Off-Premises

(42) IT assets must be safeguarded in accordance with University policy when off-site from University premises.

(43) 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.

(44) 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.

(45) 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

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

Unattended User Equipment

(47) 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

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

(49) 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.

(50) 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.

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

Part D - Defence Industry Security Program (DISP)

(52) Prior to agreeing to store, process, or communicate information or assets under DISP, approval from the Cyber Security team must be obtained.

(53) The Cyber 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	24th June 2026
Review Date	24th June 2029
Approval Authority	Chief Operating Officer
Approval Date	22nd June 2026
Expiry Date	Not Applicable
Responsible Executive	Morven Cameron Chief Operating Officer
Enquiries Contact	Digital Technology Solutions

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.

"Controlled entity" - Has the same meaning as in section 16A of the University of Newcastle Act 1989.

"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.