# Information Security Physical and Environmental Security Procedure

# Section 1 - Introduction

### Executive Summary

(1) The University of Newcastle is committed to and is responsible for ensuring the confidentiality, integrity, and availability of the data and information stored on its systems.

(2) All users interacting with information assets have a responsibility to ensure the security of those assets.

(3) The University must have controls in place to ensure the smooth operation of the University's ICT resources. Users must be trained, equipped and periodically reminded to use information and associated infrastructure securely.

# Section 2 - Physical and Environmental Security Procedure

## Part A - Secure Areas

### Objective

(4) To prevent unauthorised physical access, damage and interference to the University's information and assets.

#### Physical Security Perimeter

(5) University information processing facilities must be protected by a physical security perimeter.

(6) Information owners must ensure appropriate controls are in place to establish secure areas. Sensitive information and assets must be protected while considering the safety of personnel. Control selection must be supported by an appropriate risk assessment.

(7) Controls that must be applied are:

a. security perimeters must be clearly defined, and the siting and strength of each of the perimeters must depend on the security requirements of the assets within the perimeter and the results of a risk assessment.
b. perimeters of a building or site containing information processing facilities must be physically sound (i.e. there must be no gaps in the perimeter or areas where a break-in could easily occur); the external walls of the site 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; doors and windows must be locked when unattended and external protection must be considered for windows, particularly at ground level;
c. a manned reception area or other means to control physical access to the site or building must be in place; access to sites and buildings must be restricted to authorised personnel only;
d. physical barriers must, where applicable, be built to prevent unauthorised physical access and environmental

contamination;

e. all fire doors on a security perimeter must be alarmed, monitored and tested in conjunction with the walls to establish the required level of resistance in accordance to suitable regional, national, and international standards.
f. suitable intruder detection systems must be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas must be alarmed at all times; cover must also be provided for other areas, e.g. computer room or communications rooms.

(8) A secure area may be a lockable office, or several rooms surrounded by a continuous physical security barrier. Additional barriers and perimeters to control physical access may be needed between areas with different security requirements inside the security perimeter.

(9) Special consideration must be given towards physical access security when the facility houses multiple organisations or business units.

**Physical Entry Controls**

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

(11) 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 such access;
c. an audit trail of all access must be maintained;
d. visitors must be escorted by authorised personnel;
e. visitors must only be allowed access for specific and authorised purposes;
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 security personnel when they encounter unescorted visitors or anyone not wearing visible identification;
j. third-party support personnel may be granted restricted access only when required; their access must be authorised and monitored; and
k. access rights must be regularly reviewed.

**Securing Offices, Rooms and Facilities**

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

(13) Information owners and IT Security Officers must regularly assess the security of areas where sensitive information is processed and/or stored. Controls that may be implemented to reduce associated risks are:

a. Physical entry controls described in clauses 10 and 11 of this procedure.
b. Ensure sensitive information is stored properly when not in used in accordance with clauses 58 to 61 of this procedure.
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**

(14) Physical protection against natural disasters, malicious attack or accidents must be designed and applied.

(15) Information owners, Data Center Managers, IT Security Staff, planners and architects must incorporate – to the extent possible – physical security controls that protect against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural and man-made disaster. 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. stationary, must not be stored in a secure area;
c. backup equipment and backup 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.

**Working in Secure Areas**

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

(17) Information owners and University IT Security Officers 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;
c. no type of photographic, smartphone, video, audio or other recording equipment can be brought into a secure area unless specifically authorised;
d. maintenance staff, cleaners and others who require periodic access to the secure area must be screened and their names added to an access list; and
e. visitors must be authorised, logged and escorted.

**Delivery and Loading Areas**

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

(19) Information owners, University IT Security Officers, planners and architects must ensure that:

a. access to a delivery and loading area from outside of the building must be restricted to identified and authorised personnel;
b. the delivery and loading area must be designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building;
c. the external doors of a delivery and loading area must be secured when the internal doors are opened;
d. loading docs and delivery areas must be regularly inspected and actively monitored;
e. incoming material must be inspected for potential threats before this material is moved from the delivery and loading area to the point of use;
f. incoming material must be registered in accordance with asset management procedures on entry to the site; and
g. incoming and outgoing shipments must be physically segregated where possible.

# Part B - Equipment

## Objective

(20) To prevent loss, damage, theft or compromise of assets and interruption to the University's operations.

### Equipment Siting and Protection

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

(22) Information owners, University IT Security Officers, planners and architects must ensure that University facilities are designed in a way that safeguards sensitive information and assets.

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

(24) Workstations, laptops, digital media and storage devices should be located and used in an area that is not accessible to the public.

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

(26) Shared printers, scanners, copiers and fax machines should not be located in an area that is accessible to the public.

(27) Kiosks and other devices that are intended for public use must be clearly labelled and placed in a publicly accessible area.

### Supporting Utilities

(28) Equipment must be protected from power supply interruption and other disruptions caused by failures in supporting utilities.

(29) The following controls must be implemented to help ensure availability of critical services.

(30) All supporting utilities such as electricity, water supply, sewage, heating/ventilation and air conditioning must be adequate for the systems they are supporting. Support utilities must be regularly inspected and as appropriate tested to ensure their proper functioning and to reduce any risk from their malfunction or failure. A suitable electrical supply must be provided that conforms to the equipment manufacturer’s specifications.

(31) 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 case 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 regularly checked to ensure it has adequate capacity and is tested in accordance with the manufacturer’s recommendations. In addition, consideration could be given to using multiple power sources or, if the site is large, a separate power substation.

(32) 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.

(33) The water supply must be stable and adequate to supply air conditioning, humidification equipment and fire suppression systems (where used). Malfunctions in the water supply system may damage equipment or prevent fire suppression from acting effectively. An alarm system to detect malfunctions in the supporting utilities must be

evaluated and installed if required.

(34) Telecommunications equipment must be connected to the utility provider by at least two diverse routes to prevent failure in one connection path removing voice services. Voice services must be adequate to meet local legal requirements for emergency communications.

**Cabling Security**

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

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

(37) When identified in a Risk assessment, network cabling must be protected from unauthorised interception or damage by using a conduit and by avoiding routes through public areas.

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

(39) Cables and equipment must be clearly marked to minimise handling errors such as accidental patching of wrong network cables. A documented patch list must be used to reduce the possibility of errors.

(40) When a Risk assessment finds a need for more safeguards, consider:

a. installation of rigid conduit and locked rooms or boxes at inspection and termination points;
b. use of alternative routings and/or transmission media providing appropriate security;
c. use of fibre optic cabling;
d. use of electromagnetic shielding to protect the cables;
e. initiation of technical sweeps and physical inspections for unauthorised devices being attached to the cables; and
f. controlled access to patch panels and cable rooms.

**Equipment Maintenance**

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

(42) When equipment is serviced Information owners must consider the sensitivity of the information it holds and the value of the assets. The following controls must be applied:

a. equipment must be maintained in accordance with the supplier’s recommended schedule and specifications;
b. only authorised maintenance personnel may carry out repairs and service equipment;
c. records must be kept of all suspected faults and all preventive and corrective maintenance
d. maintenance must be scheduled at a time of day that limits interference with services or operations;
e. users must be notified before equipment is taken off-line for maintenance.

(43) If off-site maintenance is required then the asset must be cleared of all sensitive information. If it’s not possible to de-sensitise assets before sending for maintenance then the University CIO and Information owner must consider destruction of the asset.

**Removal of Assets**

(44) University owned equipment, information and software must not be removed from University premises without

prior authorisation.

(45) Information owners must establish a formal authorisation process for the removal of assets for re-location, loan, maintenance, disposal or any other purpose. Authorisation must include:

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

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

(47) Personnel must be informed of and accept responsibility for protection of the asset.

**Security of Equipment and Assets Off-Premises**

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

(49) Information owners must ensure that equipment used or stored off-site is safeguarded in accordance with the sensitivity of the information and the value of the assets. Controls to apply include:

a. encrypt sensitive data;
b. use a logical or physical access control mechanism (BIOS password, USB key, smart card) to protect against unauthorised access;
c. use a physical locking or similar mechanism to restrain the equipment;
d. ensure personnel are instructed on the proper use of the chosen controls.

(50) Personnel in possession of University equipment:

a. must not leave it unattended in a public place;
b. must ensure the equipment is under his/her direct control at all times when travelling;
c. must take measure to prevent viewing of sensitive information by unauthorised personnel;
d. must not allow other persons to use the equipment;
e. must report loss or stolen equipment immediately.

**Secure Disposal or Re-Use of Equipment**

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

(52) Information 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.

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

a. the integrity of the University records must be maintained by adhering to the Records Management policy;
b. information and software must be backed up by the original Information owners; and
c. the storage media must be wiped in accordance with the Asset Management Procedure (Disposal of Media).

(54) Storage media that will no longer be used in the University must be wiped by a method approved by the IT Security team, in compliance with the Asset Management Procedure. Asset inventories must be updated to record

details of the data wiping including:

a. asset identifier
b. date of erasure
c. names of personnel conducting the erasure.

(55) 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**

(56) Users must ensure unattended equipment has appropriate protection.

(57) User must safeguard unattended equipment by:

a. terminating the active session when finished;
b. lock the session with a password protected screen saver or other approved mechanism;
c. logoff computers, servers, terminals and other devices when session is finished;
d. enabling password protection on mobile devices, printers, kiosks and portable storage devices; and
e. secure devices with a cable lock when enhanced physical security is justified.

**Clear Desk and Clear Screen Policy**

(58) Users must safeguard sensitive information from unauthorised access, loss or damage.

(59) Users must secure their work space when it cannot be monitored by authorised personnel. Secure work spaces 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. safeguarding incoming and outgoing mail
f. retrieving documents from printers and fax machines; and
g. ensuring that sensitive hard copy documents no longer needed are placed in shredding bins, not recycle bins.

(60) When visitors, cleaning staff or other personnel without a “need to know” are in the area, safeguard sensitive information by:

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

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

## Status and Details

| | |
|---|---|
| **Status** | Historic |
| **Effective Date** | 31st March 2017 |
| **Review Date** | 1st July 2018 |
| **Approval Authority** | Chief Information Officer |
| **Approval Date** | 31st March 2017 |
| **Expiry Date** | 17th June 2019 |
| **Responsible Executive** | David Toll<br>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.

**"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.

**"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.

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

**"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.