ITSS_12 IT Security Standard – Physical Security

Version	Approved by	Approval date	Effective date	Next review date
1.0	Vice-President, Finance and Operations	7 June 2016	7 June 2016	7 June 2017

Standard Statement			
Purpose	Robust physical and environmental controls must exist to protect information assets and systems from unauthorised access, and safeguard against environmental threats. This Standard sets out the rules for the protection of information systems from physical and environmental threats to ensure the confidentiality, integrity, and availability of the data contained within the physical environment.		
Scope	This standard applies to all users of UNSW Information and Communication Technology resources – including (but not limited to) staff (including casuals), students, consultants and contractors, third parties, agency staff, alumni, associates and honoraries, conjoint appointments and visitors to UNSW.		
Are Local Documents on this subject permitted?	☐ Yes	☐ Yes, subject to any areas specifically restricted within this Document	☐ No
Standard			

1. Controls

Facility design and equipment security

1.1 Cabling Security

1.1.1 In line with industry electrical / cabling standards precautions must be taken to mitigate the risk of unauthorised / malicious data interception and accidental / malicious damage to ICT installations.

1.1.2 Electric cabling is physically separated from data cabling to prevent interference and reduce risk of injury and damage to equipment.

1.1.3 All power and telecommunications lines into information processing facilities are underground, or subject to adequate alternative protection.

1.1.4 All cabling and networking equipment is clearly labelled using a documented convention to minimise handling errors.

1.1.5 Any communications or networking equipment (routers, switches, hubs, and patch panels) is protected against unauthorised physical access by either placing it within a secured data centre or a locked cabinet or room.

General workplace security

1.2 Removal of equipment and security of off-site equipment

1.2.1 Employees and contractors must not remove property (except mobile devices) from UNSW premises without prior authorisation.

1.2.2 An inventory of all IT assets must be maintained, which lists equipment that has been removed from UNSW premises.

1.2.3 UNSW employees that travel with a laptop or other equipment with “Sensitive” information, including portable hard drives, must be cautious and keep the items secure. Specific security mechanisms (strong authentication and encryption) should be considered for the devices according to the classification of the data stored on each device (Data Classification Standard).

1.2.4 All storage media taken off site by service providers (such as faulty disk drives and tapes) requires specific physical management and destruction procedures, as described in the Data Classification Standard.

1.3 Controlling access to buildings

1.3.1 All employees, contractors, vendors, and visitors must be authorised by the equivalent UNSW Manager or an appropriate approval authority, for physical entry into secure UNSW facilities.

1.3.2 Badges must be carried by employees, internal contractors and displayed by third party contractors or visitors. Badges must be designed to clearly distinguish visitors and employees. Temporary badges must expire after a pre-determined period of time.

1.3.3 All employees, contractors, vendors and visitors must report any lost identification badges immediately to Facilities and inform UNSW IT Service Desk.

1.3.4 Employees must notify UNSW Security of any suspicious personnel within UNSW secure areas.

1.3.5 Physical access rights must be removed or disabled as soon as possible when an employee, contractor or visitor no longer needs access due to changing roles or leaving UNSW.

1.3.6 Physical access rights must be regularly reviewed by the UNSW Manager or delegate who initially approved access to UNSW premises. This review must be conducted annually.

1.4 Controlling incoming and outgoing objects

1.4.1 When receiving incoming objects, caution should be taken, anything suspicious should be reported to management for direction before handing the object further.

1.4.2 Equipment, except for portable devices, must not be removed from UNSW premises unless authorisation has been obtained in writing (email) from a UNSW Manager or delegate.

Data Centre Security

The controls in this section of the Standard apply to all UNSW Data Centres including decentralised computer rooms located in Divisions and Faculties.

1.5 Data Centre environmental control

1.5.1 All data centre facilities are protected against fire, water damage, vandalism, and other threats known or likely to occur at their geographical locations.

1.5.2 Walls surrounding data centres are non-combustible and resistant to fire. All openings to these walls (e.g., doors, ventilation ducts, etc.) must be self-closing and resistant to fire.

1.5.3 All IT equipment in UNSW data centres operate in a climate-controlled environment at all times. Temperature and humidity sensors are installed to detect any environmental change and trigger an alarm.

1.5.4 All necessary measures must be in place to ensure that if a fire breaks out, it can be quickly controlled and suppressed. Specific measures must be in place such as smoke detectors, automated fire suppression systems as well as fire-extinguishers.

1.5.5 All data centre personnel are trained in the use of portable fire extinguishers.

1.5.6 Data centres must be equipped with environmental controls to manage the environment such as water, power or temperature.

1.5.7 Uninterruptible Power Supplies (UPS) are used to provide short-term power when the power fails and to protect information systems from voltage spikes and reductions.

1.5.8 Where appropriate (risk based approach), redundant electrical power supply (e.g., backup power generator) must be in place to support information systems in the event of a prolonged power outage.

1.6 Controlling access to Data Centres

1.6.1 Physical access to data centres is controlled through physical access card control system. In case where a physical access control system cannot be installed to decentralised computer rooms, other authentication methods must be in place such as combination locks.

1.6.2 Physical access to Data centre access is limited to employees with a valid business reason. Access must be revoked immediately once it's no longer needed. Additional access should be revalidated as a secondary control.

1.6.3 Access logs produced by physical access card control systems are retained for one (1) year. Access to the system storing the logs is strictly controlled and limited to authorised individuals.

1.6.4 All visitors must sign in when entering data centres. The name, organisation being represented, date, time of entry and departure, and person being visited must be logged. Visitor log information must be retained for a minimum of two (2) years.

1.6.5 Where appropriate (risk based approach), data centres entry points are monitored via a Closed-Circuit Television (CCTV) system on a 24/7 basis. All video surveillance data must be protected from unauthorised disclosure and modification and maintained for at least ninety (90) days.

1.6.6 Data centres are equipped with doors that automatically close immediately after they have been opened, and that set off an audible alarm when they have been kept open beyond a pre-determined period of time.

1.6.7 Decentralised computer rooms containing network, wiring or communications equipment (e.g., wiring closets, etc.) are locked at all times with access restricted to authorised personnel only. Signs are not to be posted on wiring closets, telephone rooms, data centre facilities or other equipment components that would attract the attention of unauthorised individuals.

1.6.8 UNSW IT employees hosting visitors (e.g., IT vendors) must ensure that their visitors are escorted at all times when in data centres.

1.7 Equipment Maintenance

1.7.1 All equipment utilities (e.g. UPS, generator, fire suppression system) are monitored in accordance with manufacturer specification and correctly maintained. Procedures exist for UNSW Facilities Management to test equipment at least once every six (6) months. The test results must be documented and communicated to the Security Operations Manager.

1.7.2 All regular maintenance activities are documented in the operational documentation of the Facilities Management Division. The documentation includes the frequency and details of routine maintenance that needs to be performed.

1.7.3 Facilities Management must make available to the Data Centre Manager the following:

- The maintenance schedule of equipment depicting the activities to be conducted and the contact details of the individuals (including third parties) who will be performing the maintenance work.
- The maintenance reports describing the activities completed, any problems identified and the respective problem resolution activities.

1.7.4 Details of maintenance agreements such as start-date, end-date and vendor contact details must be kept in operational documentation maintained by Facilities Management.

1.7.5 Only authorised maintenance personnel are allowed to perform repairs. Data Centre Managers must grant access to the maintenance personnel outlined in the maintenance schedule.

2. Control Exceptions

All exemption requests must be reviewed assessed, and approved by the relevant business stakeholder. Please refer to the ISMS Base Document for more detail.

3. ISMS Mapping with Industry Standards

The table below maps the ITSS_12 Physical Security Standard with the security domains of ISO27001:2013 Security Standard and the Principles of Australian Government Information Security Manual.

ISO27001:2013	Information Security Manual
11– Physical and Environmental Security	Physical Security for Systems

4. Document Review, Approval & History

This section details the initial review, approval and ongoing revision history of the standard. Post initial review the standard will be presented to the ISSG recommending the formal UNSW policy consultation and approval process commence.

A review of this standard will be managed by the Chief Digital Officer on an annual basis.

4.1 Quality Assurance

This document was designed and created by external and internal consultants in consultation with internal key technical subject matter experts, business and academic stakeholders.

4.2 Sign Off

Endorsement	Date
ISSG - Information Security Steering Group	30th July 2015
ITC - Information Technology Committee	27th August 2015
CDO – Chief Digital Officer	7th June 2016

Accountabilities	
Responsible Officer	Chief Digital Officer
Contact Officer	ITpolicy@unsw.edu.au
Supporting Information	
Parent Document (Policy)	IT Security Policy
Supporting Documents	Nil

Related Documents	Data Classification Standard Data Handling Guidelines ISMS Base Document
Superseded Documents	Nil
UNSW Statute and / or Regulation	Nil
Relevant State / Federal Legislation	Nil
File Number	2016/16925 [ITSS_12]

Definitions and Acronyms

No terms have been defined

Revision History

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Vice-President, Finance and Operations	7 June 2016	7 June 2016	This is a new document