Version	Approved by	Approval date	Effective date	Next review date

Standard Statement

Purpose	Appropriate management of IT assets is a fundamental requirement of any Information Security Management System (ISMS). UNSW must employ robust IT asset management processes to ensure IT assets are identified, inventoried and maintained. In the context of this standard, an IT asset is any UNSW owned or managed data link, physical device, o/s firmware, application, database, middleware (collectively known as a service) that connects to the UNSW enterprise. This document does not address information assets such as data or process documentation which should be inventoried within the appropriate management system (i.e. SharePoint, EDW), classified and handled in line with the Data Classification Standard and Handling Guidelines. The System Owner is the individual (manager) and entity (organisation e.g. UNSW IT communication unit, HR, Finance) that has approved management responsibility (business owner) for the support of the asset. The Business Owner is the individual (i.e. CTO / Chief Digital Officer / Dean / HoS / Directors) and entity (organisation e.g. UNSW IT, HR, Finance) that has property rights (financial) of the asset. **Asset Examples:** • Data Link: ADSL, MPLS. • Device: PABX, Switch, Router, Firewall, Server (physical & virtual), appliance, notebook, desktop, smart phone or tablet, printers. • O/S: LINUX, Microsoft. • Application: Oracle PeopleSoft Financials, Salesforce. • Database Oracle. • Middleware: SAS, SQL, Oracle Fusion. Project Management, Design, Implementation, Support and ISMS processes rely upon an accurate, asset inventory in order to operate effectively. These processes include, but are not limited to, the following: • Change management. • Security risk assessment. • System currency (supported version, maintenance, licence agreements). • Configuration management. • Vulnerability and patch management. This Standard defines and sets out how IT assets must be managed, addressing the controls that account for and maintain an accurate asset inventory.
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

1.1 IT Asset Management

1.1.1 System Owners must identifyand maintain accurate details of assets in a central asset Inventory (Configuration Management Data Base). The asset inventory must include, if applicable:

a) The System Owner.

b) Business Owner.

c) Unique asset identifier (e.g. barcode) and location i.e. Secure Data Centre.

d) Description of the business and technical purpose of the asset, e.g. faculty access switch.

e) Information such as vendor name, model number, serial number, code / firmware version, hostname / application (i.e. FQDN), IP address, circuit reference, license number.

f) Security Zone, as per the ITSS_15 Network Security standard i.e. Trusted.

g) Risk Classification i.e. high as calculated by the classification questionnaire.

1.1.2 The IT asset inventory must be updated when:

a) An asset is commissioned e.g. brought into production.

b) A break-fix or upgrade situation involving the replacement of an asset i.e. infrastructure module replacement where the hardware and therefore serial number has changed.

c) Code or version change owing to upgrade or patch.

d) An asset is decommissioned i.e. removed from production.

1.1.3 The IT asset inventory must be reconciled at least annually.

1.1.4 Access to the IT asset inventory is limited to authorised staff who have a valid business need.

1.2 IT Asset Business and System Owner Responsibilities

1.2.1 Business and System owners must be assigned for all assets under management.

1.2.2 Business owners are ultimately accountable for all assets and must nominate, define and document responsibilities of the appointed System Owner.

1.2.3 System Owners must ensure in scope controls detailed within the ISMS standards are addressed, specifically:

a) Document and manage the asset as per the 2.1 IT Asset Management section ofthis document.

b) Identify, deploy, monitor and report the effectiveness of information security control's associated with the assets across in scope information security standards.

c) Identify, assess, treat and review risks for their assets.

d) Report security incidents and perceived risks affecting assets via the UNSW IT Service desk.

e) Ensure asset resident data is destroyed (wiping) before asset disposal or repurposed in line with Data Handling Guidelines (Destruction of Data).

f) Post decommissioning return asset to the Business Owner or as instructed by the Business Owner.

1.2.4 System Owners must protect IT assets according to the requirements specified by Business Owners.

1.3 Data Classification and Handling

1.3.1 Data owners (opposed to Business or System Owners) must classify the data being processed, stored or transmitted in line with the Data Classification Standard.

1.3.2 Based on Data Classification the System Owner must implement appropriate ISMS and Data Handling controls to maintain Confidentiality, Integrity and Availability of UNSW Data.

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_08 IT Asset Management Standard with the security domains of ISO27001:2013 Security Standard and the Principles of Australian Government Information Security Manual.

ISO27001:2013	Information Security Manual
8 Asset management	TBA

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	
ITC - Information Technology Committee	
CDO – Chief Digital Officer	

Accountabilities	
Responsible Officer	Chief Digital Officer
Contact Officer	
Supporting Information	
Parent Document (Policy)	IT Security Policy
Supporting Documents	Nil

Related Documents	Data Classification Standard Data Handling Guidelines ISMS Base Document ITSS_15 Network Security Standard
Superseded Documents	Nil
UNSW Statute and / or Regulation	Nil
Relevant State / Federal Legislation	Nil
File Number	2016/16925 [ITSS_08]

Definitions and Acronyms

No terms have been defined

Revision History

Version	Approved by	Approval date	Effective date	Sections modified