ITSS_15 IT Security Standard – Network 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	The UNSW network provides baseline connectivity between all end user, compute and storage devices. It also provides access between UNSW and external networks, including both partner networks and the Internet. The information security controls which are deployed to the network are critical to the overall security posture of UNSW, and failure of these controls may expose the confidential and sensitive information that UNSW manages. Network technology and topologies are evolving rapidly. This is observed in the rapid shift to virtualisation technology at the network layer as well as next generation network devices which can be solely responsible for multiple functions such as switching, routing, packet filtering, load balancing and traffic inspection. Specific care must be taken with such devices as a simple configuration error may have a detrimental effect on the security of the overall device, and therefore the networks that it services. In alignment with this rapidly evolving lifecycle, network security controls must be adjusting to accommodate this new functionality and services. Consequently Network Security controls must not constrain the ability of UNSW to innovate, but should give a framework of controls which allows UNSW to access new and innovative services in a secure controlled manner. This standard aims to ensure that UNSW networks are designed, implemented and managed according to good practice security standards in order to protect the UNSW data and IT services, whilst allowing UNSW to utilise innovative and evolving technologies.		
Scope	This security standard applies to all UNSW network environments.		
Are Local Documents on this subject permitted?	☐ Yes	☐ Yes, subject to any areas specifically restricted within this Document	☐ No

Standard

1. Controls

1.1 Security Principles

UNSW networks must be designed, implemented and managed using security best practices. The following are the best practice principles by which the UNSW network architecture and design must align to:

- Security by design – Deploy infrastructure and services which can be secured appropriately and accessed by authorised parties only. All infrastructure and devices must be secured in line with vendor best practices.
- Defence in depth – Implement multiple layers of security enforcement points / controls and never allow direct connectivity to internal (trusted) UNSW networks from untrusted networks (e.g. Internet).
- Least Privileged – Users must never have administrative privileges by default, they must be escalated to the administrator by an appropriate method. Remote administrator access must require two factor authentication to access the administrative account. For remote access details see the ITSS_05 User Access Management Standard.
- Highly available – Perimeter infrastructure must be robust, reliable and resilient to failure to ensure external connectivity is maintained for business services. Consider using Distributed Denial of Service (DDoS) infrastructure and/or services.
- Positive security model (default deny) - Only required information and services are exposed to untrusted networks, explicit permit must be granted on a case by case basis. See firewall section for details.
- Data protection – Protect information and services using encryption or other secure channels to prevent session eavesdropping/hijacking and data loss when sensitive data is being sent via untrusted/public networks (refer to the UNSW Data Classification Standard).
- Trust / Zone Model – deploy a security model which is based upon trust, data / service criticality and security zones. Inherent to this model is the idea of enforcement points segregating trust zones, and highly critical data contained within highly secure / trusted zones.
- IPv6 – Network and security design (new and re-design) considerations must take into account IPv6 requirements (e.g. new devices must be IPv6 capable).
- Cloud Environments – For both internal and external cloud security controls, see the ITSS_07 Cloud Security Standard.

1.2 Network Diagrams

1.2.1 Logical network diagrams must be created and maintained for UNSW networks. The format of these diagrams can be stored as hard copy (e.g. paper), soft copy (e.g. MS Visio diagram) or logical (e.g. dynamically created via network management applications). The information captured in these diagrams should consider the following environments and be able to aid support, design and implementation. System owners are at liberty to decide how best to achieve this requirement.

- Gateway and core network connectivity.
- Data Centre connectivity.
- Management network connectivity.
- Wireless network connectivity.
- WAN connectivity from the local distribution layer to the UNSW core.
- Campus connectivity from the distribution layer to the UNSW core.
- Faculty, Divisional access layer connectivity.
- Trust / Security zone boundaries and traffic flow.

1.2.2 For multiple sites or multiple devices with the same or similar design, a site/device template should be documented and referenced for each site or group of systems.

1.2.3 Network topology diagrams must be kept protected and access limited to authorised IT personnel only; as network topology diagrams typically contain private IP addressing and other sensitive information.

1.3 Logical Network Security Zone Model

In line with the new Security Architecture model, UNSW networks should be viewed as security zones, each zone (reference new security architecture) is defined as having criteria which describes the type of services that can be deployed for processing or storage and therefore the strength of security control afforded.

To understand which zone is appropriate for service within the new model the appropriate security questionnaire must be completed which takes into consideration data classification, threats and vulnerabilities.

1.4 Security Zones Characteristics

Security Zone	Zone Characteristics
Internet	External (Internet) networks or other networks without a trust relationship.
External Trusted	External Cloud or Managed Service provider.
Secure DMZ Semi-Trusted	Devices such as security appliances (Firewalls, IDS/IPS, SIEM, Content Filters), RAS and Web Servers.
Old Architecture Semi Trusted	Legacy network architecture hosting systems outside the new security architecture.
New Security Architecture (low, medium) trusted	An internal zone which can host highly sensitive information for systems of a low or medium risk nature.
New Security Architecture (high) highly trusted	An internal zone which can host highly sensitive information for systems of a high risk nature.

1.5 Traffic Flows between Security Zones

1.5.1 Information flow between different security zones must be via an appropriate enforcement point. The following security technologies can provide this functionality (NB: one or more of the following technologies can be used as an enforcement point):

- Firewalls to enforce the flow of information between zones based on port, protocol and/or application (next generation firewalls).
- Intrusion Detection/Prevention Systems to inspect traffic for malicious and anomalous activity.
- Proxy technology e.g. content filtering to monitor and control the use of specific services, for example email (SMTP) and web browsing (HTTP/S) traffic.
- Web Application Firewalls (WAF) to protect internet facing web applications.

1.6 Virtualisation

Modern network and infrastructure equipment supports virtualisation techniques making it possible for a single hardware platform to run a number of virtual instances hence reducing cost of ownership and improving implementation timeframes dramatically. Virtualisation is permitted when:

1.6.1 Security Zone and Traffic Flow requirements are adhered to.

1.6.2 All applicable ISMS key controls are implemented at Hypervisor and VM level just as they would for a physical deployment as outlined in the ISMS base document:

- Establishment of Services.
- Inventory Management.
- ID Management.
- Access Control.
- Key Management.
- Syslog Management.
- Backup Management.
- Patch Management.
- Vulnerability Scanning.
- Malware (AV) Management.
- IDS / IPS Management.
- Configuration Integrity Management.
- Unauthorised Change Management.
- Security Incident Management.
- Documentation Management (Policy, Process, Procedure).
- Risk Management.

- Disestablishment of Services.

1.7 Firewalls

1.7.1 Firewalls must be:

- Managed using a central management console with change control tracking capability.
- Deployed in a high availability / fail-over configuration for high availability networks.

1.7.2 Firewalls must perform the following functions:

- All incoming and outgoing data packets are filtered through stateful inspection.
- Filter incoming and outgoing data packets through configurable rules.
- Inspect every packet and blocks on both policy and protocol violations.

1.7.3 Use due diligence and rule validation when creating or modifying firewall rules to ensure changes do not negatively impact the security posture of the environment.

1.7.4 Firewall rules must:

- Specify the permitted service, service port number/protocol, source and destination address relevant to the business, security or management need of the traffic flow.
- Each firewall rule set (management, security & operational) that permits traffic must have a specific business requirement and associated owner documented to avoid miss configuration and aid revalidation.
- Be formally reviewed at a frequency decided and justified by the owner. The review must be conducted to validate the rule base for appropriateness and accuracy.
- Be reviewed to highlight used and unused rules.
- Revalidate management, security and operational rules bases with owners to confirm continued need and appropriateness of rule.

1.7.5 Any discrepancies identified must be recorded and resolved accordingly via the Change Management Process.

1.8 Intrusion Prevention

1.8.1 Intrusion prevention system capability must be deployed to detect and block malicious and suspicious traffic. If intrusion prevention is not available then intrusion detection must be used and integrated into the incident response process. Note: Care should be taken to arrive at a reasonable baseline and not act on false positive events that may cause an unnecessary outage.

1.8.2 Intrusion prevention systems should be deployed in monitoring / learning mode for a predefined period, or when UNSW is confident it can manage the level of detected false positives. Once learning mode has been completed the intrusion prevention systems must be modified to operate in blocking mode in order to enforce traffic (both ingress and egress) passing between internal and external facing security zones.

1.8.3 Intrusion prevention system policy must be configured to:

- Use specific signature sets appropriate for the networks it is protecting.
- Detect traffic anomalies.
- Utilise emerging intrusion prevention technologies as defined as best practice by the Intrusion Prevention manufacturer.

1.8.4 Intrusion prevention system policy must be formally reviewed at least annually.

1.8.5 Intrusion prevention system signatures must be set to update automatically.

1.8.6 Intrusion prevention systems must be:

- Managed using a centralised management console with change tracking capability.
- Deployed in a high availability configuration.

1.8.7 Make use of malware analysis / sandbox features if available.

1.9 Gateway and WAN Edge Connectivity

1.9.1 Gateway and WAN edge routers/firewalls must be configured with the following controls:

- Apply access control lists (ACLs) to filter traffic required traffic.
- Out of band management port with ACLs.
- Disable unused services.

- Highly available.

1.9.2 Gateway and WAN edge routing services are critical for maintaining connectivity between UNSW and external networks. Any change to edge routing configuration or devices involved in edge routing, must be part of the formal Change Management Process and have the appropriate authorisation before the change is implemented.

1.9.3 Where appropriate manufacturer best practice must be applied to the configuration of all WAN edge routing services, for example, Cisco guidance on control plane protection and securing Border Gateway Protocol (BGP).

1.10 Connections to un-trusted and third-party networks

1.10.1 Any connection between UNSW networks and any third-party network may increase the risk to UNSW systems and information. All connections to third party networks must connect through one or more security enforcement points and be approved through the UNSW Change Management Process.

Security of core network services

1.11 Domain Name Services

Domain Name Services (DNS) available on the Internet are high-risk. Steps must be taken to configure Internet DNS services to restrict common DNS-based attacks, for example:

- Zone transfer attacks that will provide attackers with useful information on network configuration and topology.
- Zone changes that could allow domain hi-jacking that could have a high impact on external access to UNSW systems.

1.11.1 Internal and external DNS servers must be used and hosted on segregated infrastructure.

1.11.2 The configuration of DNS servers must be regularly checked for configuration changes, vulnerabilities and treated as high priority if anything out of the ordinary is discovered.

1.11.3 DNS services must be both IPv4 and IPv6 compliant.

1.12 Network Time Protocol

Network Time Protocol (NTP) provides a common time source to all UNSW IT services so that all device and system clocks can be synchronised. The NTP source must be accurate and reliable for use by cryptographic services, to allow UNSW to record events in a time-consistent way and to allow correlation of events both internally and externally during incidents and investigations.

1.12.1 The network must provide a reference clock source based on the NTP that is available to all UNSW IT services.

1.12.2 The NTP service must be based on at least NTP version 4 and synchronised to a ‘known-good/reputable’ external time reference source (e.g., stratum 1, 2 or 3)

1.12.3 As incident response relies on accurate timestamps from devices, loss of the NTP service must be progressed via the incident management process.

1.12.4 Internal NTP services must:

- Not be accessible from the Internet.
- Be deployed in a high availability configuration.

1.13 Secure network management

1.13.1 Dedicated management stations (jump box) must be configured to access the devices for management activities only. These stations must be hardened and locked down.

1.13.2 Access control lists must be applied to only allow management traffic between the network management stations and the intended end devices. These access control lists apply to both network devices and network servers. For example, TCP wrappers configured on Unix servers or Cisco ACLs on Cisco network devices.

1.14 Access to network management facilities

1.14.1 Network devices are required to support centralised authentication for access control to the device. Acceptable but not limited protocols are:

- LDAP over SSL (LDAPS).
- RADIUS.
- TACACS(+).
- TLS/SSL.

1.14.2 Network device failure due to misconfiguration or user error may have a critical impact on UNSW's ability to do business. Administrative access to network devices must be restricted to an approved list of personnel with appropriate skills and qualifications.

1.14.3 Administration access must use cryptographically secure protocols such as SSH or HTTPS (ITSS_02 Data Security Standard / Secure Algorithm List).

1.14.4 Login access for all accounts must be locked as per the ITSS_05 User access management standard.

1.14.5 All administrative access to network devices must be logged and monitored according to the ITSS_06 Logging and Monitoring Standard.

1.14.6 Administrative passwords and other authentication tokens for accessing network equipment must be treated as sensitive information.

1.14.7 Unused services and interfaces must be disabled, for example HTTP management services

1.14.8 Port-locking must be configured on critical network and security infrastructure to prevent attacks based on physical access. Management interfaces are exempt.

1.14.9 Local fall back/safe accounts must be stored in a secure location in the event of all users being locked out of devices. This location must be monitored and reported on.

1.14.10 All devices must be monitored by a management station such as an SNMP manager. Consider using secure management protocols such as SNMPv3 with authentication and encryption.

1.15 Network configuration management and integrity checking

1.15.1 Network devices are key security controls. All network infrastructure devices must be under a formal configuration and change management regime.

1.15.2 It must be possible to verify the integrity of network device configurations, for example by the use of automated integrity checking solutions or by comparison to a baseline configuration. The integrity of network devices must be checked on a regular basis.

1.15.3 If a network device is discovered to be incorrectly configured, this must be treated as a Security Incident and investigated and resolved according to the ITSS_03 Security Incident Management Standard.

1.15.4 All network devices must be backed up according to ITSS_01 Data Backup Standard

1.16 Security of wireless networks

1.16.1 Wireless endpoints must be configured to only permit authenticated and encrypted data:

- WPA-2 must be used to encrypt traffic on wireless links (WEP and MAC filtering are not satisfactory controls).
- End points must be authenticated.
- The use of 802.1x technology with certificate-based authentication to the access point is considered appropriate.

1.16.2 The emanation range of wireless networks must be both considered and tested when designing and implementing wireless networks that connect to UNSW networks.

1.17 Security of Voice over IP (VoIP) networks

1.17.1 VoIP terminals must only be configurable and display configuration information after end user authentication on the terminal (e.g., username/password)

1.17.2 VoIP servers must be hardened and patched. Servers must be configured to:

- Disable “auto registration” of VoIP terminals and allow only registered VoIP phones.
- Enforce a password complexity of 4 or more.
- Disable all service and testing codes.

1.17.3 Harden and limit software loading on VoIP terminals.

1.17.4 Access to web based interfaces (e.g. client web management, voicemail web interface etc) must be restricted.

1.17.5 VoIP networks must be segregated from UNSW data networks (VLAN separation is acceptable).

1.17.6 Insecure VoIP protocols must not be allowed on data networks.

1.17.7 VoIP rules/signatures must be established on next generation firewalls to inspect the traffic.

1.17.8 If call recording is required the *Privacy Act 1988* should be consulted. The general rule is that the call may not be recorded. There are exceptions in limited circumstances, including where a warrant applies. If a call is to be recorded or monitored, an organisation must advise you at the beginning of the conversation so that you have the chance to either end the call, or ask to be transferred to another line where monitoring or recording does not take place.

1.17.9 To combat the misuse of the VoIP environment resulting in financial loss (Toll fraud), all VoIP activities must be logged. In particular this includes:

- Device registration events.
- Call metadata.

1.17.10 Where appropriate, sensitive VoIP traffic must be encrypted (note that encryption may negatively affect performance).

1.17.11 All VoIP equipment must be configured in line with vendor best practices as described in the overarching security principle security by design.

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_15 Network 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
13 - Communications security	Network Security

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 ITSS_01 Data Backup Standard ITSS_02 Data Security Standard ITSS_03 Security Incident Management Standard ITSS_05 User Access Management Standard ITSS_06 Logging and Monitoring Standard ITSS_07 Cloud Security Standard
Superseded Documents	Nil
UNSW Statute and / or Regulation	Nil
Relevant State / Federal Legislation	Nil
File Number	2016/16925 [ITSS_15]
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