Information Security Network Security Manual

Section 1 - Audience

(1) All University staff, affiliates, and students, in all campuses and locations of the University and at all times while engaged in University business or otherwise representing the University.

Section 2 - Purpose

(2) 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.

(3) Securing the network infrastructure is a crucial element in providing a reliable operational environment for the University's academic, research and administrative functions.

(4) The intent of this manual is to establish the minimum standard network security controls to protect University ICT services and systems against downtime due to malicious and unintentional failures, to prevent unauthorised individuals from accessing ICT network resources, and to protect University confidential data.

(5) In recognition of the University’s rapidly evolving lifecycle, network security controls must be adjusting to accommodate new functionality and services. Consequently, network security controls should provide a framework of controls which allows the University to access new and innovative services in a secure and controlled manner.

Section 3 - Scope

(6) The minimum standards defined in this manual apply to all members of the University community including staff, students, vendors and contractors who have any device connected to the University network including, but not limited to, desktop computers, laptops, servers, wireless devices, mobile devices, smartphones and telephone system components.

(7) Where relevant, parts of this manual will apply to any party who has a system outside of the University network that accesses the University network and ICT resources.

Section 4 - Network Security Requirements

(8) The following security configurations are to be followed and implemented across the University ICT network systems and devices.

(9) These standards are also applicable to in-scope systems and devices managed by individuals and teams outside of University IT Services. System Owners should contact the Information Security Team for queries on applicability and implementation.

(10) Exceptions will need to be authorised at an Associate Director level, or assessed by the IT Services Architectural Governance Board (AGB).

Core Principles

(11) University networks must be designed, implemented and managed using security best practices. The following core principles should be followed for network architecture and design:

a. Security by design – address information security requirements throughout a system's lifecycle. This includes security design specifically for the identification, protection, detection, response and recovery capabilities to strengthen the resiliency of a system.
b. Defence in depth – implement multiple layers of security controls, and never allow direct connectivity to trusted University networks from untrusted networks such as the internet.
c. Least Privileged – users must never have administrative privileges by default. Users must elevate privileges when required. Remote administrative access must be protected by multi-factor authentication, unless there is a technical constraint that prevents it from being implemented.
d. Highly available – perimeter infrastructure must be robust, reliable and resilient to failure to ensure external connectivity is maintained as per business needs.
e. Positive security model (default deny) - only required information and services are to be exposed to untrusted networks.
f. Data protection – protect information and services using encryption to prevent session eavesdropping, hijacking, and data loss when sensitive data is being transmitted over untrusted networks.
g. Trust / Zone Model – deploy a security model which is based upon trust, data and service criticality, and security zones. Inherent to this model is the use of enforcement points segregating trust zones.
h. Cloud Environments – consider the risk to information that will be created, stored, transmitted or processed within cloud-based services and to deploy appropriate measures to manage these risks to an acceptable level.
i. IPv4 – network and security design (new and re-design) considerations must be IPv4 by default, and must disable IPv6.

Documentation

(12) Network documentation must be developed that includes:

a. high-level network diagrams showing major connections into the network;
b. logical network diagrams showing all network devices, critical servers and services; and
c. the configuration of all network devices.

(13) Network documentation must be updated as network configuration changes are made, and include a 'current as at [date]' or equivalent statement.

(14) Network documentation provided to a third party, or published in public tender documentation, should only contain details necessary for other parties to undertake contractual services.

Authentication

(15) Any access to internal non-public facing University ICT resources shall only be allowed after valid identification, authentication, and authorisation of the user in accordance with the Information Security Access Control Manual. (This requirement does not apply to "Public Access" services, including "Guest wireless" and "Conference Users").

(16) Where systems allow, before a user gains access to University ICT network services and systems, a general system use notice must be displayed that identifies it as a University owned system and warns against unauthorised

use of the device, and indicates that use of the system implies consent to all relevant University policies.

Firewall

(17) The University's firewall must be managed using a central management console, with changes tracked for auditability.

(18) The University's firewall must be deployed in a highly available configuration for high availability networks.

(19) The University's ICT resources must be protected from the WAN/Internet, by one or more firewalls that incorporate stateful packet inspection to protect the University from untrusted network access.

(20) The University's firewall must filter incoming and outgoing data packets through configurable rules, which inspect every packet and blocks based on policy and protocol violations.

(21) The recommendations of the Internet Engineering Task Force (IETF) Best Current Practices (BCP) 38 should be implemented to help protect the University against Denial of Service (DoS) attacks.

(22) 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.

(23) All access through the University firewalls to restricted or highly-restricted information and systems must obey the “Deny All - Allow Specific”.

(24) For any change to be enabled in the University firewalls, users must raise a firewall change request and the access will be enabled following appropriate approval per the University's change management process.

Remote Access

(25) Access to the University's internal networks via external connections from remote locations shall not be automatically granted.

(26) Remote access to the University network shall be available only after an explicit request is made by the user which is endorsed by the appropriate line manager, and approved by the Associate Director responsible for security (or their delegated officer).

(27) Remote access shall only be provided through a University-managed secure tunnel such as a Secure Sockets Layer (SSL) or Internet Protocol Security (IPSec) Virtual Private Network (VPN).

(28) Remote access must be controlled with encryption and strong passwords. For further information on acceptable password parameters see the Password Requirements section of the University's Information Security Access Control Manual.

(29) The VPN shall be configured in such a way that the users would not be able to access any other network simultaneously while connected to University network (split tunnel).

(30) University staff performing roles of systems administrators must be required to authenticate using Multi-Factor Authentication (MFA) mechanisms where available.

(31) All remote access to administrative interfaces must be blocked unless access is established via the University's authorised VPN solution, or MFA is enforced by the administrative interface. Exceptions must be approved by the CIO.

(32) All systems providing VPN termination must be configured with an idle time-out. The time-out shall be configured to end all sessions after an idle period of 30 minutes.

Wireless Access

(33) Wireless access points shall be enabled with minimum IEEE 802.11i settings (WPA2-Enterprise with EAP-TLS) to implement strong encryption for authentication and transmission. The use of WEP as a security standard to access University confidential / internal resources must be avoided.

(34) All wireless access points should be Wi-Fi Alliance certified.

(35) Wireless networks provided for the general public to access, e.g. guest and conference users, must be segregated from all other networks.

(36) The administrative interface on wireless access points should be disabled for wireless network connections.

(37) The Pairwise Master Key (PMK) caching period should not be set to greater than 1440 minutes (24 hours).

Network Design & Segregation

(38) Networks must be divided into multiple functional network zones according to the sensitivity and criticality of information and services.

(39) Database servers and web servers should be functionally separated, physically or virtually.

(40) A network Intrusion Prevention System (IPS) must be implemented between trusted and untrusted networks to monitor and protect critical data centre networks, network hosting critical research systems, and internet hosted application against attack.

(41) Management traffic should be separated from user traffic.

(42) VLAN’s shall be set up to restrict network traffic between production environment and non-production environment inside the Data Centre infrastructure.

(43) Network devices implementing VLANs must be managed from the most trusted network.

(44) Security containers / network segmentation shall be created to host all internet facing applications and services in a segregated network from the internal network.

Using Internet Protocol version 6 (IPv6)

(45) Internet Protocol version 6 (IPv6) functionality can introduce additional security risks to the University network. As such, to minimise the attack surface of the network and ensure that any IPv6 functionality that is not intended to be used cannot be exploited, IPv6 functionality must be disabled until it is approved for use.

(46) To aid in the transition from Internet Protocol version 4 (IPv4) to IPv6, numerous tunnelling protocols have been developed that are designed to allow interoperability between the protocols. IPv6 tunnelling protocols must be disabled on network devices and ICT resources that do not explicitly require such functionality, to prevent the bypassing of traditional network defences by encapsulating IPv6 data inside IPv4 packets.

(47) Stateless Address Autoconfiguration (SLAAC) is a method of stateless Internet Protocol (IP) address configuration available in IPv6 networks. SLAAC reduces the ability of the University to maintain effective logs of IP address assignment on the University network. For this reason, stateless IP addressing should be avoided.

(48) Unless explicitly required, IPv6 tunnelling must be disabled on all network devices and ICT equipment.

(49) IPv6 tunnelling must be blocked by network security devices at externally connected network boundaries.

BYOD Network Segmentation

(50) User-authenticated BYOD systems and devices connecting to the University network shall be quarantined to a segregated network which permits identical access to that of a user accessing the University from the internet; with only restricted access to University internal networks and systems.

Network Management

(51) All network device passwords should be created and managed in accordance with the Privileged Account Password Requirements section of the Information Security Access Control Manual.

(52) Before installing a device on the network the default account settings and configurations must be changed and devices must be hardened. Hardening must include:

a. disabling or blocking of non-essential services;
b. restricting access to management interfaces (Console / SSH, Web Admin, FTP, SNMP etc) to nominated managed networks or nominated management / monitoring devices / systems;
c. disabling all guest or world read access; and
d. changing the name of and/or removing default administrator user accounts.

(53) Patches and updates must be applied to network devices as per Information Security Patch Management Manual.

(54) Plain-text protocols should not be used in network management.

(55) Network device management interfaces should be on a separate management network.

(56) All management interfaces must be secured by credentials that meets the requirements of the Privileged Account Password Requirements section of the Information Security Access Control Manual.

(57) Network management services should be configured with SNMPv3 with encryption enabled (or other option that does not use plaintext community strings). The use of SNMPv2 should be avoided as far as possible.

(58) All default SNMP community strings on network devices must be changed and must have write access disabled.

(59) The following protocols are prohibited for use:

a. File Transfer Protocol (FTP) – Use Secure File Transfer Protocol (SFTP), File Transfer Protocol Secure (FTPS) or Secure Copy Protocol (SCP) instead.
b. Telnet – use Secure Shell (SSH) v2 instead.
c. Remote Desktop Protocol (RDP) without Network Level Authentication (NLA) – use RDP with NLA instead.
d. Simple Network Management Protocol (SNMP) v1 – use SNMP v2 or v3 instead.
e. Secure Shell (SSH) v1 – use SSH v2 instead.
f. Secure Sockets Layer (SSL) v1, v2, & v3 – use TLS v1.0 or greater instead (note Clause 60).
g. Lightweight Directory Access Protocol (LDAP) – use Lightweight Directory Access Protocol Over Secure Socket Links (LDAPS) instead.
h. Post Office Protocol (POP) – use Exchange ActiveSync, Messaging Application Programming Interface (MAPI) or Exchange Web Services (EWS) instead.
i. Internet Message Access Protocol (IMAP) – use Exchange ActiveSync, Messaging Application Programming Interface (MAPI) or Exchange Web Services (EWS) instead.

(60) The following protocols should not be used, and will become prohibited for use from 1 March 2020:

a. TLS v1.0
b. TLS v1.1

(61) The configuration of all network equipment should be backed up regularly, and immediately following any configuration change.

(62) The configurations should be subject to managed revision control.

(63) Logs generated from the security devices should be stored and backed up. Refer to Information Security Operations Management Manual for log retention guidelines.

Cryptography

(64) Where technically feasible all communication devices and systems shall be enabled with encryption solutions and must comply with applicable laws and meet the following requirements:

a. minimum acceptable hash algorithm: SHA 256 (i.e. SHA-224, SHA-256, SHA-384 and SHA-512);
b. minimum acceptable encryption algorithms:
    i. Symmetric: AES, 3DES (with 3 distinct keys);
    ii. Asymmetric: RSA, DSA, DH, ECDH, ECDSA;
c. acceptable minimum crypto key length:
    i. Symmetric: 128 bits;
    ii. Asymmetric: 2048 bits.

Network Time Protocol (NTP)

(65) The NTP source must be accurate and reliable for use by cryptographic services.

(66) 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).

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

(68) Internal NTP services must:

a. not be accessible from the internet.
b. be deployed in a high availability configuration.

Change Management

(69) Any changes required to the Firewall must be according to the change request process, and by completing a Change Request form (See associated information). Refer Information Security Operations Management Manual for change management process and guidelines.

(70) Requested firewall changes must be assessed and approved by a senior member of the IT Capability Line responsible for firewall administration. This assessment will evaluate such areas as the potential impact upon other network devices and network services.

(71) The change application must then be referred to the Information Security Team for review and endorsement before implementation.

Review and Monitoring

(72) The Information Security Team will perform an annual assessment of network devices to check compliance with these standards.

(73) Security Information and Event Management (SIEM) solutions shall be implemented to perform log correlation and periodically review and monitor for anomalous events.

(74) Firewalls protecting enterprise systems must be reviewed annually and the documentation supporting the firewall rule sets are to be retained.

Exceptions

(75) Exceptions to the standards defined in this manual may be requested in writing to the Chief Information Officer (CIO). Exceptions will be assessed based on the business impact, the security risk that the proposed exemption may pose and any compensating controls implemented.

Enforcement

(76) All users performing roles of system or application administrators managing University ICT services and systems should be aware of the minimum standards defined in this Manual, their responsibilities and legal obligations. Non-compliance with the provisions of this Manual may result in action under the University's Policies, Code of Conduct or enterprise agreement, and may also result in referral to a statutory authority and/or agency.

Roles and Responsibilities

(77) The University's Delivery and DevOps teams are responsible for ensuring appropriate application of these minimum standards on all University ICT services and network devices within their areas of responsibility.

(78) All other University staff, affiliates, vendors, students, in all campuses and locations of the University are responsible for ensuring appropriate application of these minimum standards on network devices that they may own, use and/or manage on the University network.

(79) The Information Security Team is responsible for routinely performing compliance checks with these standards.

Status and Details

Status	Historic
Effective Date	18th June 2019
Review Date	18th June 2021
Approval Authority	Chief Information Officer
Approval Date	17th June 2019
Expiry Date	19th January 2023
Responsible Executive	David Toll 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.

"Law" - All applicable statutes, regulations, by-laws, ordinances or subordinate legislation in force from time to time anywhere in Australia, whether made by the Commonwealth, a State, a Territory or a local government and, where the context permits, includes the common law and equity.

"Student" - A person formally enrolled in a course or active in a program offered by the University or affiliated entity.

"Exemption" - When referring to a student’s learning pathway, exemption means being excused from undertaking preparatory subjects, units, modules or competencies in a course or program, while still being required to undertake the same number of subjects, units, modules or competencies as would be completed if an exemption had not been granted. For all other uses of this term, the generic definition applies.

"ICT resources" - All information and communication technology resources and facilities.

"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.