Information Security Network Security Procedure

Section 1 - Procedure

Audience

(1) All University staff, vendors, students, volunteers, and members of advisory and governing bodies, in all campuses and locations of the University and at all times while engaged in University business or otherwise representing the University.

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 procedure is to establish appropriate 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.

Scope

(5) This procedure applies to:

a. All members of the University community including staff, students, vendor 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. Parts of this document where relevant will also apply to anyone who has systems outside the University network that access the University network and resources.
b. Also applicable UON IT non managed services and systems, respective system owners to reach out to IT Security & Assurance team for queries on applicability and implementation.

Section 2 - Network Security Requirements

(6) The following security configurations are to be followed and implemented across the University ICT network systems and devices. (Applicable also for all systems and devices not managed by UON IT, system owners to reach out to IT Security & Assurance team for queries on applicability and implementation).

(7) Exceptions will need to be authorised at an Associate Director level, or assessed by the Architectural Advisory Group (AAG).

Authentication

(8) Any user access to University's internal non-public facing services shall be allowed only after valid Identification, Authentication, and Authorisation of the users. (This policy does not apply to “Public Access” services, including and not limited to “Guest wireless” & “Conference Users”).

(9) 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

(10) All University's internal network resources must be protected from the WAN/Internet, by one or more firewalls to protect University ICT services and systems from external untrusted network access.

(11) All University ICT services and systems hosting restricted and highly-restricted data must be protected by a network firewall and host-based software firewall (where applicable).

(12) All access through the University firewalls accessing restricted or highly-restricted information must be assessed on a a “Deny All - Allow Specific” principle and ensure that firewall access must be enabled for applications and IP address combinations wherever possible.

(13) Inbound internet traffic shall be limited to only system component and services within the respective security containers protected by intelligent firewalling systems and to other authorised ICT services and systems.

(14) For any change to be enabled in the University firewalls Users must raise a firewall change request and the access will be enabled post approval via the change management process.

Remote Access

(15) All remote access University ICT services and systems must be via a VPN (Refer Cryptography section for acceptable encryption requirements). This will be enabled after approval by the Associate Director responsible for security (or their delegated officer).

(16) Secure remote access must be controlled with encryption and strong passwords or pass-phrases (dependent on the capability of the underlying systems supporting Authentication, Authorisation and Accounting (‘AAA’)). For further information see the Password Requirements section of the University's Access Control Procedure for acceptable password settings.

(17) 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).

(18) University staff performing roles of systems administrators must be required to authenticate using Two-Factor authentication mechanisms where available.

(19) All remote access to any administrative interface for University ICT services and systems other than through the University authorised VPN solution must be blocked. Exceptions need to be approved by the CIO.

(20) 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 mins.

Wireless Access

(21) Wireless access points shall be enabled with minimum IEEE 802.11i settings 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.

Network Design & Segregation

(22) Network-based IPS must be implemented for all critical data centre networks, networks hosting critical research systems & internet hosted applications, to monitor and prevent attacks.

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

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

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

Network Design for Research Systems

(26) System components that store research data should be hosted in a separate security container and where appropriate, segregated from untrusted networks.

(27) Network configurations managing access to research containers shall be configured to restrict all external untrusted inbound traffic to that which is necessary for the research environment and specifically deny all other traffic, i.e. 'Deny All – Allow Specific'.

Network Posture Assessment

(28) User authenticated unmanaged systems and devices connecting to University wireless access 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 network and systems.

(29) University managed systems and devices connecting to University wireless access shall undergo a network posture assessment for availability of current patches, anti-virus software and signatures. With noncompliant devices being denied access, or placed in a quarantined area, or given restricted access to computing resources, thus keeping insecure nodes from infecting the network.

Network Management

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

(31) Before installing a device on the network the default account settings and configurations must be changed and devices must be hardened. (Hardening must include, but no limited: Disabling or blocking of non-essential services; Restrict access to management interfaces (Console / SSH, Web Admin, FTP, SNMP etc) to nominated managed networks or nominated management / monitoring devices / systems; Disable all guest or world read access; Change the name of and/or remove default administrator user accounts).

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

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

(34) Network Device management interfaces should be on a management network.

(35) Any console port used for device management should be secured by a username / password and follow complexity features required as per Password section of the Information Security User Access Management Procedure.

(36) Network management services should be configured with SNMPv3 with encryption enabled (or other option that does not use plaintext community strings).

(37) The following protocols are prohibited for use: FTP, telnet, RDP without NLA, SSHv1, SSLv1, SSLv, SSLv3 and LDAP.

(38) The configuration of all network equipment should be backed up regularly.

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

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

Cryptography

(41) 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

b. **Minimum acceptable encryption algorithms:**

   i. Symmetric: AES, 3DES
   ii. Asymmetric: RSA, DSA

c. Acceptable minimum crypto key length:

   i. Symmetric: 128 bits
   ii. Asymmetric: 1024 bits

Change Management

(42) Any changes required to the Firewall must be requested initiating a request for change request per the change request process along with completing a Change Request form (See associated information). Refer Information Security Operations Management Manual for change management process and guidelines.

(43) Requested changes must be assessed and approved by a senior member of the Networks & Communications Team and by the Networks Team Leader. This assessment will evaluate such areas as the potential impact upon other network devices and network services.

(44) The change application must then be referred to the IT Security Team.

Review and Monitoring

(45) The IT Security team will perform a Quarterly vulnerability assessment on the network devices to check compliance to the configurations listed.

(46) Any intrusion attempts or malicious activity on the network should be monitored on periodic basis. Incidents should be responded to as per the University Information Security Incident Management guidelines.

(47) SIEM solutions shall be implemented to perform log correlation and periodically review and monitor for anomalous events.

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

Exceptions

(49) Exceptions to this procedure may be requested in writing or via email to the relevant IT Associate Director. Exceptions will be assessed based on the business impact, the security risk that the proposed exemption may pose and any compensating controls implemented.

Enforcement

(50) All users performing roles of system or application administrators managing University ICT services and systems should be aware of this procedure, their responsibilities and legal obligations. Non-compliance with the provisions of this procedure may result in action under the University's policies, code of conduct or enterprise agreements, and may also result in referral to a statutory authority and/or agency. Sanctions may include warning, counselling, disciplinary or legal action.

Roles and Responsibilities

(51) The University's IT Operations, System Administration, Database Administrators, ARCS and Network & Communications teams are responsible for ensuring appropriate enforcement of this procedure on all University ICT services and network devices within their areas of responsibility.

(52) The IT Security Team is responsible for routinely performing compliance checks with this procedure.

Status and Details

Status	Historic
Effective Date	31st March 2017
Review Date	1st July 2018
Approval Authority	Chief Information Officer
Approval Date	30th May 2018
Expiry Date	17th June 2019
Responsible Executive	Morven Cameron 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.

"Officer" - Has the meaning given in the Corporations Act 2001 (Cth), or any replacing legislation.

"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.