Network Security policy

January 2022

UNIVERSITY OF
WINCHESTER

Document Title:	*Network Security Policy*
Document Author:	Fiona Greig
Responsible Person and Department:	Fiona Greig Knowledge & Digital Services
Approving Body:	UMG Senate
Date of Approval:	
Date Effective From:	*1st January 2022*
Review Date:	***31st July 2023***
Indicate whether the document is for public access or internal access only Indicate whether the document applies to collaborative provision? *(Strikethrough text, as appropriate)*	~~**Public Access**~~ **Internal Access Only** ~~**Applies to Collaborative Provision**~~

Summary:

The Network Security Policy sets out the specific responsibilities, conditions and practices to ensure an available, secure and protected Network.

TABLE OF CONTENTS

1. Scope of policy

1.1. This policy sets out the requirements, roles and responsibilities for a secure University network. The Knowledge and Digital Services (KDS) team will:-

a) Ensure, where reasonably practicable, that the network supports the full range of University activity and business; allows our students and academics to achieve their objectives; and provision applications required by the University community and any other authorised user(s)

b) Ensure network availability

c) Protect the Network from unauthorised access

d) Protect the Network from accidental disruption

e) Protect confidentiality

f) Ensure network access can be audited

g) Define what the Network may be used for and what is not acceptable

2. Roles and responsibilities

2.1. Knowledge & Digital Services Leadership Group will:

2.1.1. Support administrators across the University in defining appropriate user groups and roles to support Role-Based Access Control (RBAC).

2.1.2. Audit central user and access lists on a regular basis to ensure that unauthorised attempts are identified and for anomalies in Super User access.

2.1.3. Perform annual policy and procedure reviews

2.2. Architecture Team will:

2.2.1. Create and maintain procedures and document all necessary network and network security configurations.

2.2.2. Monitor and analyse network traffic for optimum performance and security.

2.3. All Network Users will always act responsibly and be aware of the associated risks and penalties for breaches of this policy, including potential disciplinary processes.

3. Physical and environmental security

3.1. All core network switching, management systems and port distribution systems will be housed in a secure location with UPS and access control. These secure areas will:

3.1.1. Allow entry to secure areas with critical or sensitive network equipment only to those who are authorised to do so

3.1.2. Have secure code or card access systems

3.1.3. Only allow visitors or 3rd party access with KDS authorisation. A list of authorised users will be maintained and regularly reviewed.

3.1.4. Will not allow smoking, eating and drinking in these spaces

3.2. Before any visitor or 3rd party is provided access to secure network areas agreement to all relevant University Policies and will be made aware of security requirements.

3.3. All visitors to secure network areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out.

4. Access control to the network

4.1. Access to the network will require a secure log-on procedure (See the IT Acceptable use policy, section 2).

4.2. Registration and de-registration procedure for access to the network will, in the first instance, be driven from the HR System to create employee/staff access and from the Student Records System for student and researcher access. Separate authorisation will be required for remote access to the network.

4.3. Access rights to the network will be allocated on the requirements of the user's job, rather than on a preference or perceived need.

4.4. Similarly, security privileges (i.e. 'Power user' or network administrator rights) to the network will be allocated on the requirements of the user's job. A list of which will be securely maintained and reviewed regularly.

4.5. All users of the network are sent an "ITS Acceptable Use" policy and expected to read and understand their requirements. When logging into University network PCs users are reminded of this before logging in.

4.6. All users to the network will have a unique user identification and password.

4.7. Users are responsible for ensuring their password is kept securely and not shared with others (see the Access Control Policy and User Policy)

4.8. User access rights will, upon notification from the HR or Student Records Systems, be removed or reviewed for those users who have left the University.

5. Firewall standards

5.1. A firewall is defined as any hardware and/or software designed to examine network traffic using policy statements (rule set) to block unauthorised access while permitting authorised communications to or from either a network or electronic equipment.

5.2. All network (physical) firewalls installed and implemented, must be implemented by the Architecture Team.

5.3. All firewall modification requests must be logged in the ServiceDesk call logging system (TopDesk)

5.4. All changes to firewall rule sets will be documented and recorded.

5.5. All related documentation is to be retained by the Network & Systems Team and is subject to regular review.

5.6. All firewall implementations must adopt the position of "least privilege" and deny all inbound traffic by default (the initial rule set will be set to "logging or learning mode" to prevent service interruptions). The rule set will only be opened incrementally to only allow permissible traffic.

5.7. Firewalls must be installed within production environments where "Legally/Contractually Restricted Information" is captured, processed or stored, to help achieve functional separation between web-servers, application servers and database servers.

5.8. Firewall rule sets and configurations require annual review to ensure they afford the required levels of protection.

5.9. Architecture Team must review and agree all network firewall rule sets and configurations during the initial implementation process.

5.9.1. Firewalls protecting enterprise systems must be reviewed twice a year.

5.9.2. Firewalls not protecting enterprise systems must be reviewed annually by a responsible firewall administrator.

5.9.3. Firewall administrators must retain the results of firewall reviews and supporting documentation; all results and documentation are subject to regular review.

5.9.4. Firewall rule sets and configurations must be backed up frequently to alternative storage (not on the same device). Multiple generations must be captured and retained in order to preserve the integrity of the data, should restoration be required. Access to rule sets and configurations and backup media must be restricted to those responsible for administration and review.

5.9.5. Network firewall administration logs (showing administrative activities) and event logs (showing traffic activity) are to be written to alternative storage (not on the same device) and reviewed regularly.

5.9.6. Network & Systems Team will execute approved changes to the firewall rule sets on behalf of the University.

6. Wired network

6.1. Only university owned equipment may be connected to the wired University Network. This includes network services supplied to all campuses and University buildings.

6.2. Personal laptops are not eligible for wired network connections (this does not extend to ResNet). The University does provide wireless networks, which are for mobile computing connectivity including; laptops, mobile phones and smart devices. Where Laptops or mobile devices require physical network connection this must be formally requested and then logged and supported by Knowledge & Digital Services.

6.3. Use of network addresses other than those provided by Knowledge and Digital Services are prohibited.

6.4. Access to networking equipment in data centres and communications rooms is limited to Knowledge & Digital Services staff and authorised personnel only.

6.5. Only one device may be connected to any physical wired network port. No hubs, switches, wireless access points or routing devices may be connected, directly or indirectly, without prior agreement from Knowledge & Digital Services.

6.6. Architecture Team has the right to limit network capacity or disable network connections that are affecting available network bandwidth to the detriment of the University. Where possible, and depending on the severity of the incident, this will be done in negotiation with the impacted units of the University.

6.7. No individual may connect a device to the campus wired network that provides unauthorised users access to the network or provides unauthorised IP addresses for users.

6.8. Non-Knowledge & Digital Services supported servers configured to provide services for campus users are allowed in exceptional circumstances subject to the following conditions:

6.8.1. A server registration form that has been completed and approved by the Architecture Team.

6.8.2. The service is established in support of authorised business and / or commercial activity.

6.8.3. The service is established only for legitimate and authorised support of teaching, research or student services.

6.8.4. The established service must follow the policies and procedures required by the University.

6.8.5. The service will be subject to internal and external auditing.

6.8.6. A responsible owner and their line manager must sign off as Data

6.8.7 Controllers will comply with all relevant legislation for all data stored. The responsible owner and authorising managers must be aware of their personal and corporate liabilities should their service result in the loss of data

6.8.8. The server owner is responsible for the backups, restoring and patching of the server and applications.

6.8.9. The service will be managed effectively to ensure no excessive loading adversely affects the University's wired network bandwidth.

6.8.10. The service will be subject to periodic network security evaluation which will include penetration testing by Network & Systems Team.

6.8.11. The server authorisation will be reviewed on an annual basis.

6.9. Students living in University accommodation using the ResNet wired network are able to connect their personal devices to the network. Instructions of how to do this, and to register smart devices are provided at point of moving into accommodation.

7. Wireless network

7.1. The University has established an ubiquitous wireless network across the campus, quadrants and locations which is for the use of staff and students and authorised representatives only, to connect University owned IT and user owned devices communications devices and equipment.

7.2. The wireless network security standards are as follows:

7.2.1. Access Layer: users will connect to the WLAN via access points, which will provide the 802.11g/n connection standard for the client devices.

7.2.2. Service Set Identifier (SSID2): The SSID for the main wireless network for the University is Eduroam.

7.2.3. The Network & Systems team provision guest SSIDs for Open Days, Conferences and Guest Accommodation these are broadcast so as to make it easily available to authorised visitors.

7.2.4. The Eduroam network will utilise AES (Advanced Encryption Standard) level of encryption. This encryption standard is mandatory to enable the 802.11n network to be supported.

7.2.5. The Eduroam service supports only WPA2 (Wi-Fi Protected Access) which is the preferred security standard.

7.2.6. Unauthorised devices connected to the wireless network will be blocked without warning.

7.2.7. Staff or students are prohibited from connecting additional wireless network hotspots to the University network.

8. Third party access control to the network

8.1. Third party access to the network will be based on appropriate authorisation and compliance with all relevant policies.

8.2. Knowledge & Digital Services are responsible for ensuring all third party access to the network is recorded in our Service Desk solution (TopDesk).

8.3. Access to the internet may be provided for University staff, students or University employed contractors via the Knowledge & Digital Services support desk. Connection to the University Wi-Fi infrastructure may be approved where the appropriate request is made in writing to establish a named account or the appropriate self-registration process is undertaken.

9. External network connections

9.1. Knowledge & Digital Services is responsible for implementing all connections to external networks that connect to the primary University and JANET supported Network, ensuring systems conform to the necessary legislative and JANET compliance.

9.2. Knowledge & Digital Services is responsible for ensuring all connections to external networks and systems are documented and approved by the IT Governance before they commence operation.

10. External network connections

10.1 Knowledge & Digital Services will ensure that maintenance contracts are maintained and regularly reviewed for all essential network equipment.

10.2 We use the Service Desk system for ensuring that a log of all faults on the network is maintained.

10.3 Architecture will ensure a log of current network and switch configurations. Changes will be maintained and stored securely and backups of switch configurations taken regularly. The Architecture Team will:

10.3.1 Document procedures for the backup process and ensure that it is communicated to all relevant staff.

10.3.2 Document procedures for the storage of backup tapes or media will be produced and communicated to all relevant staff.

10.3.3 Ensure all backup media will be stored securely and a copy will be stored offsite.

10.3.4 Document procedures for the safe and secure disposal of backup media will be produced and communicated to all relevant staff.

10.4 Users are responsible for ensuring that they backup their own data to the network server using mapped drives, OneDrive or SharePoint.

10.5 Network patches and any fixes will only be applied by the Architecture Team following a suitable change control procedure.

11. Protection and malicious attacks

11.1 The Cyber Security Team will ensure that;

11.1.1.1 Measures are in place to detect and protect the network from viruses and other malicious software.

11.1.1.2 They have suitable monitoring of network traffic, network access and intrusion detection in place.

11.1.1.3 The network will be monitored for potential security breaches. All monitoring will comply with current legislation.

11.2 Knowledge & Digital Services reserves the right to access, modify or delete all data stored on or transmitted across the University's network. This includes data stored in personal network folders, mailboxes etc. Data of a personal nature should be stored in a folder marked or called 'Personal'. This does not preclude access or removal of such a folder on the authority of the IT Governance Group, the Chief Operating Officer or other member of the University Senior Management Team where the Group are not available for approval.

11.3 Knowledge & Digital Services reserves the right to disconnect or block any device connected either by physical or wireless means to the network

12. Enforcement

12.1 Any employee, student or user, found to have violated this policy may be subject to disciplinary or legal action. Deviation from this policy is permitted only if a valid business case has been provided and subsequently reviewed and approved prior to the activity is undertaken.