1. **Introduction**

This policy explains the necessary steps that must be taken in order to attach a device to the university IT network.

Computing & Library Services reserves the right to disconnect any device from the campus network which does not conform to this procedure until such time as it is compliant.

2. **Network Connections**

To maintain the integrity and protection of university IT facilities, the university requires all equipment connected to the university IT network to comply with a set of minimum standards.

Poorly configured, managed or operated equipment may lead to serious degradation of network operation or a breach in network and systems integrity resulting in:

- Disruption to business as usual processes
- Disclosure of university information
- System or network compromise

For security and network maintenance purposes, authorised individuals within CLS may monitor equipment, systems and network traffic at any time.

3. **Attaching a device to the network**

This section explains what is required in order to attach different types of device to the network.

3.1 **All devices (workstations, servers, etc)**

In order to attach a device of any kind to the university network, the following must be in place as a minimum.

- Permission must be obtained from CLS before any non-standard device is connected to the network. This process is handled through the IT Service Desk
- The device must have the latest supported operating system and applications patches installed (unless an application vendor has specifically stated a version of software that will be supported)
- Appropriate anti-malware software should be installed and configured to automatically update at least daily and perform regular full scans of the device
- The device should be sufficiently hardened so that all unused ports are closed
- CLS will perform a health check before the device is permitted on the network.
- All devices must use DHCP for IP configuration, with the exception of essential IT Infrastructure devices and printers at the discretion of the IT team
- All devices and services connected to the network must have a DNS name. This name must be used for any connections to this device or service. It is not acceptable to reference devices or services by IP address (except printers)
- A device owner must be identified (this would normally be CLS or School/Service technical staff)
- The device owners are responsible for maintaining the security of the device, this includes all patching, hot fixes, operating system and application upgrades. Updates should be applied regularly in line with IT best practise.
University staff, students or researchers may not operate their own IT network facilities, independent of CLS without specific approval from the Head of IT. For example, the connection of hubs or switches; wireless access points; or connections to any other networks are not permitted on the university network. Independent broadband lines are permitted in exceptional circumstance e.g. for links to banks or for secure credit card payments. These types of connections should be discussed with CLS prior to procurement.

3.2 Attaching a new server to the network

3.2.1 Internal facing servers
In addition to the points in 3.1 above, the following must be in place before a server on the internal network can be attached to the network

- A suitable server name is identified
- Check that the service required cannot be hosted on an existing server
- The backup and recovery strategy is agreed
- Predicted growth of any data on the server is calculated
- Specify where will the server be located - building and room no.
- Specify if the server will be supported in the School/Service or by CLS
- Specify whether the server host data or applications
- Specify whether the server will be for staff or student use
- If the server is not within the University data centers, specify the UTP wall point in which the server is to be connected
- Finally, a health check must be performed by CLS before the server is permitted on the network

Regular testing of internal servers

- All internal servers are subject to regular testing via ‘vulnerability’ scanning. This tests whether the criteria above is being adhered to following the connection of a server to the network
- If a server is identified as vulnerable during testing, the server owner will be contacted and be given a grace period to correct any issues. The length of the grace period will depend on the severity of the vulnerability. However, this should be no more than necessary to ensure a resolution is put in place as a priority.
- Failure to mitigate any vulnerabilities during the grace period will result in the server being disconnected from the network

3.2.2 External ‘internet facing’ servers
In addition to the points in 3.1 and 3.2.1 above, the following must be in place before an internet facing server can be attached to the network

- CLS will perform a health check before the server is permitted on the network as an internet facing server
- checks should be conducted to establish whether the applications can be hosted on an existing internet facing server before commissioning a new server
- no databases will be permitted on internet facing servers unless specifically approved by CLS
Regular testing of internet facing servers

- All internet facing servers are subject to regular testing via ‘vulnerability’ scanning. This tests whether the criteria above is being adhered to following the connection of a server to the network
- If a server is identified as vulnerable during testing, the server owner will be contacted and be given a grace period to correct any issues. The length of the grace period will depend on the severity of the vulnerability. However, this should be no more than necessary to ensure a resolution is put in place as a priority.
- Failure to mitigate any vulnerabilities during the grace period will result in the server being disconnected from the network

3.3 Attaching an Internet of Things (IoT) device

In addition to the points in 3.1 above, the following must be in place before an IoT device can be attached to the network

- Discuss the device with CLS before attempting to attach it to the network. These discussions should focus on how best to configure the device for maximum security
- Specify whether the device will operate on the wired or Wi-Fi network.
- If the device is required to run on the Wi-Fi network then it must connect using the existing encryption and authentication methods available on Campus. Guidance on the current levels can be sought from the Networks team in CLS.
- The device should be configured to ‘auto-update’ any patches or bug fixes
- Ideally the device should be registered in AD

3.4.1 Attaching Printers / MFDs to the network

When purchasing a network enabled printer, several checks have to be made to ensure that the printing device isn’t configured by default using different communication protocols over the network. A network printer un-knowingly handing out IPV4 DHCP reservations would cause issues – and the device owner is accountable for the installation and maintenance of the non-network / non-managed printer (including any firmware / security updates required in the future).

Printers leased by our Printing Partner should be managed centrally and therefore shouldn’t need to be modified to avoid any issues. Any changes to our leased printing devices need to be communicated and authorised.

As well as checking the network protocols below to ascertain if they should ne enabled or not, the administrator account username and password will need to be changed from the default factory settings to improve security and maintain the integrity of the device

Default protocol list and approved settings.

- SLP (Service location Protocol) on
- LPD (Line Printer Daemon) on
- I OpenAPI Settings off (embedded on)
- IPV6 off
- DHCP (Server) for IPV4 and IPV6 off
- NetBEUI off
- FTP Server Settings off
- SMB Server Settings off
• Bonjour Settings off
• AppleTALK Settings off
• Airprint Settings off
• Internal Web Server (IWS) off