NETWORK CONNECTION POLICY

Summary

All workstations must implement security measures including up-to-date software and antivirus protection, and should not provide server functionality to other systems on the network. Servers must be properly managed and registered with IT Services. It is not permitted to extend the centrally managed network in any way without permission, and any such requirements must be discussed in advance with IT Services. Anything else to be connected should be discussed with local IT support or IT Services.

Audience

This policy will be relevant to anyone connecting systems or devices to the University network. This includes:

- IT staff, where this is a formal part of their role
- Anyone else connecting workstations, servers or any other devices or systems to the University network

Introduction

The University of Glasgow (UofG) provides a comprehensive data communications infrastructure underpinning the important role IT plays in the University's teaching, research and administration functions. This infrastructure supports a wide range of services via a high bandwidth campus backbone that connects standards-based Local Area Networks (LANs) in all UofG premises. A centralised model for infrastructure management and support has been adopted as this provides a number of benefits with respect to quality, consistency, reliability, conformance, security and on-going development. To maintain the integrity, security and proper operation of the network requires order, standards, procedures and policies governing the following:

- Who can connect
- What can and can't be connected
- How do systems connect
- What address and name space can be used
- What services can be run
- What services can be accessed
- What security measures should be implemented
- What measures will be taken to monitor compliance

Scope

This policy covers the connection of all equipment to the University's centrally managed campus network and building Local Area Networks. It also covers the indirect connection of equipment to the University's campus network via remote access servers.

IT Services (ITS) is responsible for the data communications infrastructure, in terms of:

- Backbone fibre optic cabling
- Building premises distribution schemes (UTP flood wiring)
- Backbone and Building LAN Routers
- Routing services
- Building LANs - Ethernet Switches and hubs
- IP address and name space

and the associated support services, including:

- Network management/maintenance
- Security
- DNS
- E-mail relays

ITS is therefore the logical entity to co-ordinate, manage and support all connections to the campus network and ensure compliance with this policy.

A relatively few Schools, for historical reasons, have authority to manage their own or elements of their own Local Area Network. Schools in this category must adhere to this and all other University IT policies.

It is important to note that **all** equipment physically or indirectly connected to the UofG network must be associated with, and used in support of the University's strategic aims and mission otherwise the University may be in breach of its legal and or contractual obligations.

Who can connect

The UofG data communications infrastructure is designed to support the teaching, research and administrative functions of the University. All Colleges, Schools, Institutes and University Services will therefore have the right to connect to the campus network and gain access to the University's IT resources. In addition other groups may be connected under the following categories:

- Other research groups, e.g MRC
- Honorary Clinical staff
- Affiliated/associated companies engaged in collaborative ventures, teaching and or research/commercialisation activities. NB, if Internet connectivity via JANET is required then an appropriate licence may be needed
- Sponsored/Proxy licensees and Visitor connections provided in accordance with the JANET connection policy

It is a breach of this policy to provide connectivity for any groupings outwith the categories described above.

What can and can't be connected

Technology

The University has implemented the IEEE 802.3 Ethernet standards as the technology of choice for the campus backbone and building Local Area Networks, augmented in certain areas by 802.11 compliant Wireless Local Area Networks. Routing protocol support is provided at 'wire rate' for the IP protocol. Any equipment requiring a connection to the campus network must therefore incorporate a standards-compliant Ethernet network interface and IP protocol stack.

Equipment can only be connected to the campus network if it meets the technology standards and all regulatory standards with respect to electrical, safety and environmental operation. Network connection points have been provided to support the following equipment types:

- User workstations including open access workstations
- Staff/student/visitor provided workstations at selected flexible access locations
- Central/College/School/Research Institute servers
- Networked printers and photocopiers
- Telephony equipment (VoIP)
- Videoconferencing equipment
- Specialised equipment e.g. imaging, scanners, process control systems

Restrictions

This policy forbids Colleges, Schools, Research Institutes, users or other groups from extending centrally-provided network connection points in an ad-hoc manner, or connecting equipment or installing software that could be used to monitor or record network traffic, or still or moving images of the surrounding area without proper authorisation. It is therefore a breach of this policy to connect any of the following equipment or services to a network connection point without authorisation:

- Ethernet Hubs, Switches or Bridges
- Routers
- Firewalls
- Proxy servers
- Access gateways including VPN concentrators and Remote Access Servers
- Wireless LAN access points
- Network cameras, including web cams that do not comply with the University's CCTV policy
- Any equipment configured in promiscuous mode for the purpose of monitoring or recording network traffic not specifically addressed to that equipment e.g traffic with a source or destination MAC address other than the Unicast address of the equipment
- Installing software on workstations or servers that would enable unauthorised monitoring of network traffic

- Staff/Student/Visitor provided workstations to network connection points other than flexible access connection points
- Any equipment, which is not associated with, and used in support of the University's strategic aims and mission

If there is a legitimate requirement to extend or augment the communications infrastructure via any of the above, then this requirement must be discussed and agreed with IT Services.

If the requirement is to install a Network Camera or Web Cam then this must be in accordance with University policy on CCTV Surveillance.

Equipment found to be attached to the campus network in violation of this policy will result in a request to the owners of the equipment to disconnect it. If this is not done in a timely manner then the equipment and any systems operating behind it will be blocked from accessing the campus network.

The unauthorised connection of network monitoring equipment or unauthorised use of network monitoring software will be considered an act of gross misconduct.

Disclaimer

The University takes reasonable steps, however it accepts no responsibility for any loss or damage to hardware, data or software arising directly or indirectly from the use of its computing facilities, and makes no warranty, express or implied, regarding the facilities or their suitability for any particular purpose.

Rights

The University reserves the right to modify, upgrade, withdraw or otherwise alter the facilities it provides.

The University reserves the right to examine all systems, data and software in use on its facilities, and to monitor usage, in order to ensure conformance with all relevant University policies and to ensure the facilities function in a secure, efficient and effective manner.

How do systems connect

Network connection points provide the primary means by which suitable equipment is connected to a Local Area Network and hence the University's campus network. The University has adopted industry standard Premises Distribution Schemes (PDS) as the data communications wiring standard for all University buildings. Approximately 20,000 (PDS) network connection points are available over the entire campus. Each connection point is presented as an RJ45 connector mounted within a suitable faceplate and containment system. The data transmission media used is industry standard unshielded twisted pair (UTP) cable providing four pairs of wires per connection point. The UTP cables run radially from each connection point to specialized termination panels located within secure wiring closets that also house campus network and building LAN active components.

Premises Distribution Schemes are generic systems capable of supporting a wide variety of applications including data communications and telephony services. Indeed, the University's PDS systems are now being used to provide telephone connection points as well as network connection points. This development further emphasises the security status associated with the many building wiring closets. Maintaining the physical integrity of the services running over centrally provided PDS systems dictates that access to building wiring closets be restricted to ITS authorised personnel and their approved sub-contractors. It is therefore a breach of this policy for any other personnel to access any wiring closet for purposes other than dealing with a serious environmental incident e.g. removing power to avoid risk of fire etc.

Network activations i.e. activating an Ethernet service on a centrally provided network connection point must be performed by authorised ITS personnel. Information on obtaining an active Ethernet network connection is available here.

Flexible network access facilities are available that provide authorised users, who wish to use their own systems, access to their work related Information Technology resources. This service is strictly limited to the connection of workstations i.e. it is a breach of this policy to connect any system that provides 'Server' functionality to the flexible access network.

What address and name space can be used

The University owns address and name space, which is used to partition the network into manageable sub-networks and uniquely identify all connected end-systems. The main IPv4 address space is allocated via logical sub-net partitions taken from the globally unique UofG /16 IP network address. The current method of partitioning provides around 254 sub-nets, each with a maximum address space of 254 entries. Further divisions within sub-nets are possible as is the aggregation of sub-nets into larger chunks. What is crucial is that addresses are allocated to sub-nets and end systems in a way that ensures uniqueness, manageability and avoids wasting a precious resource. For these reasons, the following rules apply.

IP addressing

Routable sub-nets are allocated by ITS as required to meet user demand. Although the main address space is limited within the UofG /16 range, current usage indicates that there is sufficient space to handle moderate expansion.

The procedure for obtaining a unique IP address for use on the campus network is as follows:

- Requests should be submitted via local IT support.
- Local IT support should determine if a previous allocation is available for use
- Local IT support should email hostmaster@gla.ac.uk with a request for a new allocation or an indication that a previous allocation has been re-used.
- The following information should be included in the request:
    - Ethernet MAC address
    - System designation - Server or workstation

    - System specification, including operating system and applications software
    - Meaningful domain name to be associated with the new or re-used allocation
- If a block of addresses are required then a detailed case must be submitted
- Requests for address blocks for ‘future use’ will not be granted. To avoid hoarding and wasting a valuable resource, only addresses that are required immediately will be granted
- ITS reserves the right to reclaim IP addresses that have not been used for six months or more

In environments where IP addresses are allocated to systems via approved DHCP servers, procedures for recording each MAC address (or user), IP address and date/time stamp associations must be implemented. The recommended way to implement this requirement for DHCP clients that remain at fixed locations is to maintain a static binding between each MAC address and IP address association wherever possible.

It will be a breach of this policy for an IP address to be acquired and used by any other means. In particular, users and IT support staff must not:

- borrow or appropriate addresses from colleagues or other sources
- guess or scan for free addresses based on a knowledge of the sub-net in use
- use reserved address space i.e. the sub-net broadcast addresses, default gateway addresses or those reserved for managed network equipment (normally addresses <= 20)
- Users must not change their unique address assignment unless instructed to do so by their local IT support or IT Services.

Name Space

The University primary Domain Name space is registered via JISC:

- gla.ac.uk
- glasgow.ac.uk

In addition, a variety of domains have been registered in under other ‘top-level’ domains to accommodate a variety of PR, business and collaborative ventures. The UofG top-level domains and the majority of sub-domains are managed entirely via the University's central Domain Name Servers (DNS). For historical reasons a very small number of sub-domains have been delegated to Schools and local DNS servers manage these.

The UofG Domain Name System (DNS) is crucial for most service delivery tasks, including access to and from the global Internet. This policy requires all IP systems to be registered with the DNS server(s) authoritative for the appropriate domain. Details of which domains would be appropriate for specific users, IP addresses or sub-nets may be obtained from IT Services, or local IT support.

Local IT support and end users are asked to ensure that up-to-date and meaningful associations are maintained between allocated IP addresses and domain names.

Colleges, Schools or other groupings wishing to register and use a domain outwith existing UofG top-level domains must discuss their requirements with IT Services. Any such domains that indicate a commercial or non-academic activity may require a suitable license to operate on JANET. Please note JISC will only grant a license if the activity satisfies their acceptable use and connection policies.

What services can be run

The services that can be run on systems connected to the University's network will be dependant on the following:

- Systems classification - workstation or server
- Importance of service to the users of that service
- Bespoke, specialised systems

Workstations

A workstation is defined as a personal system, or open access cluster system that is designed to support a single user at any point in time. This includes laptop computers and other mobile devices.

Workstations are intended to support the client software necessary to provide users with access to their work-related IT resources. Workstations should not be configured with software that provides server functionality to users on or off the campus network, or any tools that may compromise the workstation, other networked systems or the credentials of any users. In particular the following services **must not** be configured:

- Routing or NAT services
- Proxy arp services
- DHCP services
- SMTP server
- Network scanning/sniffing tools
- Session monitoring, spying or keyboard logging tools

It is recognised that there may be a legitimate reason for configuring certain services such as:

- Remote login services
- Remote desktop services
- File / print sharing services
- Peer-to-peer services, including P2P filesharing

In such circumstances users should first discuss their requirements with local IT support staff or IT Services to assess and address the security implications. As a minimum, users must:

- Limit the scope of service provision
- Protect access to resources via usernames and strong passwords

Servers

Servers are defined as systems that are configured, operated and supported to provide groups of users with access to specific IT resources. Because servers typically support many users it is important to ensure maximum service availability and integrity. Special consideration should therefore be given to the following:

- Environmental conditions - including air conditioning, emergency power source (UPS)
- Physical security
- Systems security
- Systems administration - operating system and application service, support and maintenance
- Performance - bandwidth requirements and affect on other sub-net users

Servers must be configured to provide only those services necessary for their primary purpose. In particular servers should not be configured to provide any of the following:

- Routing or NAT services
- Routing advertisements, e.g RIP, OSPF
- Proxy ARP services
- DHCP services unless approved by ITS
- Remote access services unless approved by ITS
- Dual role server/workstation

Remote Access Services

Remote Access Services provide methods of accessing University IT resources that may bypass normal boundary security measures. It is therefore essential that remote access services are established, administered and supported in a way that does not compromise the integrity of the University's security environment.

Secure remote access services are provided via the centrally managed Virtual Private Network (VPN) service and Remote Desktop terminal servers. In exceptional circumstances Colleges, Schools or Research Institutes may have a legitimate need to provide and operate their own private remote access service. All requirements relating to private remote access services must be discussed and agreed with ITS, who will stipulate the security, support and administration overheads associated with such a service (ref: *Bastion Host Policy*). In addition, all remote access services must be registered with IT Services and the following information provided:

- Type of service - VPN, Remote Desktop etc
- Hardware, software and location
- Services provided - full LAN access, restricted LAN access etc
- IP address space used
- System administrators - contact details
- Number of simultaneous users
- User registration procedure
- User authentication procedure
- Security policy

Bespoke, specialised systems

Care must be exercised when connecting bespoke systems, “appliances” or other devices to the campus network, as in many cases they will be based on common operating systems running services that may pose a risk to the integrity of the system and other systems on the network. If risks and solutions have not been identified at the outset then advice from ITS should be sought before requesting connections. As a minimum, it will be necessary to keep software on the device up to date.

What services can be accessed

Workstation users may only access services for which they have a legitimate need, are authorised to access, and have the proper authentication credentials. Knowingly accessing or attempting to access a service without authorisation is a breach of this policy. The services available to users of the flexible access network will be restricted to those currently available to authorised remote access users. All users of the UofG IT Infrastructure must comply with this and all relevant University policies.

What security measures should be implemented

Workstations

Workstations must not be configured with software that provides server functionality to users on or off the campus network or any tools that may compromise the workstation, other networked systems or the credentials of any users.

The integrity of the workstation operating system and applications must be maintained by ensuring that it remains free from viruses/malware. Therefore all workstations:

- must be kept up to date with latest operating system and application versions and patch levels
- must run an up to date version of University-recommended antivirus software configured with the latest virus definition files

Disabling antivirus software will be considered a breach of this policy.

All workstations must be configured to enforce acceptable levels of security. The UofG University's Standard Staff Desktop (SSD) and Common Student Computing Environments (CSCE) implement this requirement by design. Other workstation environments must as a minimum implement the following:

- User sessions must be authenticated before access to other resources is permitted
- User accounts must have strong passwords
- Local Admin/Root accounts must be restricted to system administrator use
- All “guest” accounts must be removed or their use restricted
- File system and data integrity must be maintained by implementing network file storage or local system backup and restore procedures

Open access workstations must be configured such that they revert to a consistent and useable state on system reset or user logout. They must preserve the confidentiality of any previous user sessions and require a successful user authentication dialog before access to other resources is permitted. (CSCE workstations meet these requirements).

Particular attention must be given to laptop computers that are used as workstations on the main campus network e.g where staff or other users are allowed to connect their University-provided or personal laptop to a network connection point other than a flexible access connection point. Since there is a high risk that a device used in this way may have been connected to *other* external networks then procedures must be adopted to ensure that the system is free from viruses/malware before it is connected to the University network. The following measures must be implemented:

- IT support staff must make users aware of the risks involved in connecting their portable computer to the Internet via different providers (ISPs), either from home, other institutions or commercial facilities (hotels etc).
- Proactive security measures must be implemented as for other workstations (see above)
- All copyright software installed must be properly licensed
- Authorised personnel must be able to audit a portable computer to ensure compliance with this policy

Servers

Servers must be configured to provide **only** those services necessary for their primary purpose.

Servers must comply with this policy and the requirements on server configuration, operation and support as specified in the University's *Bastion Host Policy*, and *Guidelines for Guidelines for System and Network Administrators*.

What measures will be taken to monitor compliance

IT Services will adopt a range of measures to monitor compliance with this policy, including:

- System inspection. As a condition of connection to the University's network, system owners must agree that ITS Security Team or other authorised personnel may inspect their systems on request and at any reasonable times
- Network management systems - tracking network connection point, MAC address and IP address bindings
- Network management systems - tracking active Ethernet switch ports for number of MAC address associations
- Active scanning for security vulnerabilities
- Audit system logs on the central servers, routers and IDS systems
- Liaise with national CSIRT teams

Further info

For further information and advice, please contact your local IT Team, or IT Services:

IT Services
ithelpdesk@glasgow.ac.uk
Ext. 4800

Title:	Network Connection Policy
Version:	2.2
Status:	Approved by IGG
Last update:	2017-05-05
Last review:	-