Server Management Policy

Summary

Before deploying a server (or other system providing server functionality), the overheads in terms of security, management, operation and support must be understood. Central IT services should be used where possible. Details, including the purpose, requirements, user base and the personnel responsible for all servers must be identified and registered with IT Services. Firewall rules are maintained such that only registered servers are accessible from the Internet.

Audience

This policy applies to all those involved with operation or support of servers, or other networked services. In particular:

- IT staff, where this is a formal part of their role
- Anyone else involved with the configuration, operation, support or management of servers, or any others systems, including workstations, configured with any server functionality.

Introduction

The purpose of this policy is to ensure that all University IT systems providing network services or applications are configured and operated with appropriate levels of security.

The University's IT infrastructure provides a comprehensive set of centrally managed network services and applications, supported by specialist teams that have responsibility for their day-to-day operation and security requirements. In addition, central support staff liaise with the Information Security Team to help implement additional proactive network service and applications security measures. However, there are significant numbers of decentralised servers operated by Colleges, Schools and Research Institutes where, in some cases, the operational and security standards are unknown. This policy defines operational and security standards that must be applied to all servers, including decentralised as well as centralised servers. In many cases Colleges, Schools and Institutes may find it more appropriate to make use of central service provisions rather than deploying and incurring the significant overheads of operating their own systems. This is particularly true for core services e.g web, email, filestore, DNS and DHCP services.

The proliferation of network servers increases the risk of systems compromise due to the extensive and increasing number of vulnerabilities affecting most popular operating systems, services and applications. Hostile attempts to attack of the University's network are commonplace as are scans designed to probe for vulnerabilities in network systems that can be exploited and lead to compromise. Also, in most modern operating systems, the distinction between server and workstation environments is blurred with many workstations running, or capable of running server software that could pose a security risk.

Therefore, the aims of this Policy are:

- Define the overheads in terms of the management, operation, support and security functions, associated with deploying a network server
- Identify all network servers and establish their purpose, requirements, user base and the personnel responsible for them
- Reduce wherever possible the number of decentralised servers by promoting central services and applications as viable alternatives
- Limit the exposure of all network servers to those services and applications that are critical for their primary function
- Establish access control lists (ACLs) for common Internet applications e.g., web, email and DNS. The ACLs restrict Internet exposure for specific applications to the servers registered to support those applications

Identifying the network systems that could present a security risk and establishing procedures and guidelines to mitigate those risks is critical to the success of the University's information security strategy.

Scope

This policy applies to all networked systems that provide services or applications that support the teaching, research or administration functions of the University. Although the primary focus will be on public servers accessible both from on campus and from the global Internet, the policy applies equally to private internal servers.

Bastion hosts

A Bastion host is a network system that may be exposed to attack from other internal or external systems. Because of this, every effort must be made to ensure that the Bastion host is deployed, configured, operated and managed in a manner that mitigates this exposure. Generally, a bastion host will fulfil a specific role and all unnecessary services, protocols, applications and network ports will either be disabled or removed. Trust relationships with other network systems would be avoided to guard against 'key to the castle' attacks. Bastion hosts require day-to-day management and on-going support, generally from system administrators expert in the operating systems, applications, protocols and potential systems vulnerabilities.

This Policy applies general Bastion host principles to *all* network servers connected to the University's networks.

Central provision

Before deploying a network server and associated services or applications, a College, School or Research Institute should consider using centrally provided solutions. Centrally provided services and applications will offer managed solutions for the majority of requirements, including:

- DNS
- DHCP
- Email
- WWW services
- WWW caches
- File services
- Print services
- Directory services
- Authentication
- Remote access
- Corporate services

If there is a legitimate reason why a College, School or Research Institute should deploy their own solutions then this must be done in a secure and supportable manner. The following sections define the University's general requirements for deploying network servers, services and applications. Any operating system, service or application specific requirements will be advertised and maintained by the Information Security Team.

Role

The role of each network server should be clearly established with respect to:

- Purpose - services and applications provided
- User community - who will use it
- Type of data stored or flowing through it, and associated risk level
- Security considerations
- Public vs. private access
- Legal and regulatory requirements
- Availability requirements - importance of services offered

Location

A network server must be dedicated to the specific tasks associated with its role and located in a lockable, restricted-access room with environmental and network provisions commensurate with the importance of the services and applications it provides. Network server locations should address the following requirements:

- Physical security and access restrictions
- Air conditioning
- Emergency power source e.g Uninterruptible Power Supply (UPS)
- Fire prevention
- Dedicated network ports

These requirements preclude the deployment of a network server or dual role server/workstation in staff offices or other areas with little physical security and/or environmental provision.

Management, support and operation

The management, support and operational requirements for each network server must be established. The personnel responsible for each role must be identified, i.e:

- Systems administrator(s)
- Systems operator(s) - where appropriate
- Service or applications support specialists - where appropriate
- Maintenance contractors, including hardware and software maintenance

The designation and number of individuals involved will depend on the importance of the network server and the resources available. However even a relatively small server, delivering modest network services or applications will require at least 2 individuals to be identified with at least one being the systems administrator.

Operational and security procedures must be established, documented and maintained by systems managers or administrators. These procedures will include:

- Asset register detailing all hardware and software components, including licensed software
- System change procedures including reversion procedures
- System configuration details including security measures and details of admin/root accounts
- Hardware and software contractors call out procedures where appropriate
- System recovery procedures including location of system backup/restore media, network, operating system, service and applications installation media and licence keys where required
- Physical security and access procedures - who is responsible for physical access security and who has physical access privileges.

Initial server builds or recovery procedures must be exercised with extreme caution; servers may be at their most vulnerable during the system build process since security patches, hot fixes and ACLs tend to be applied late in the process or indeed after it completes.

System administration

System administrators will be responsible for most aspects of the day-to-day operation and support of their network servers. They should have experience with the operating systems, services, applications and network protocols running on the servers they manage and understand the threats their systems may be exposed to. Because of their privileged position and the likelihood that they will come into contact with personal, sensitive or confidential information, they must adhere to the University's *Guidelines for System and Network Administrators*. Systems administrators will implement, configure, support and monitor the operational and security procedures associated with the network servers they manage, as detailed in the guidelines.

There may be occasions where network server deployments cannot be adequately secured by local system, service or application tools. In such cases alternative provisions should be discussed with IT Services. It is possible that deployment of a suitably configured network firewall may be recommended to protect such servers.

If a network server subsequently causes disruption to other systems, either locally or remotely, then the system administrator(s) must take action to rectify the situation. Disruption may be caused by software malfunction, users' actions or system compromise. Disruptions caused by system security-related incidents must be reported to the Information Security Team who will be responsible for ensuring that the incident is handled appropriately. If prompt action cannot be taken to rectify any disruption then the network server may need to be disconnected from the network until the problems can be properly addressed.

Network server registration

In order to ensure that the roles, management, operation and security requirements associated with network server deployments are fully understood and adequately addressed, all network servers must be registered with IT Services via the IT Apps portal. Failure to register a network server will be considered a breach of this policy and may result in loss of service or severe operational difficulties due to access restrictions and future network developments, which will only address registered server requirements.

Internet access restrictions

This policy introduces access restrictions for common Internet applications, implemented on the University's boundary routers and firewalls via access control lists (ACLs). The access restrictions ensure that common Internet applications are only available on public servers that have been configured and registered to support them. This reduces the risk of attack twofold:

- Servers are exposed to external attack *only* on ports they’re intended to serve
- All other systems on the network, including workstations, and other devices, are by default protected from direct external attacks.

It is therefore necessary to ensure all ports requiring Internet exposure are registered as part of the server details entered into the IT Apps portal. Otherwise, the campus firewalls will not have updated ACLs, effectively blocking access from the Internet to unregistered servers or unregistered ports.

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:	Server Management Policy (was Bastion Host Policy)
Version:	2.1
Status:	Approved by IGG
Last update:	2017-05-05
Last review:	-