



UU Security Policy

Server Connection Policy

Author:	Janine A. Asquith
Approved by:	IICTSC
Version:	2.0
Date:	1 st June, 2006
Status:	Agreed
Classification:	Public
Enquiry point	Janine A. Asquith Server and Host Systems Manager University of Ulster Phone: 028 90368116 Email: ja.asquith@ulster.ac.uk
Policy effective from:	1 st June, 2002
Policy review date:	1 st May, 2007

Change History

Version	Changes	Date
1.0	Initial document	01/06/02
2.0	Included BS7799 Reference Changed department name to CIS	01/06/06

Contents

UU Security Policy	1
Server Connection Policy	1
Change History	2
Contents	2
Server Connection Policy	3
Definitions	3
Reason for Policy	3
System Administration.....	3
System Configuration.....	3
Corporate Information Systems (CIS) Support.....	4
Access Policy	4
Physical Security.....	4
Enforcement.....	4
Further Information:.....	5
BS7799 Reference.....	5

Server Connection Policy

Definitions

- A “server” for any service is any system which responds to requests on the port(s) associated with that service.
- A “workstation” is any system which makes requests for any service to any server.
- “Local” means any other system on the same network segment.
- “Remote” means any system located on any other network segment.

Reason for Policy

- To help ensure that services visible to the public operate correctly.
- To provide reasonable protection for services from attack using established exploits.
- To secure services from being subverted for use by unauthorised parties, possibly for use in attacks on other servers at other sites.

System Administration

- Every system providing any service must have an identified “system administrator” whose responsibilities include the maintenance of the computer system(s) concerned.
- Systems providing services to remote workstations must also have at least one identified deputy responsible officer with system knowledge and administration access, so that a contact is available at all times during the normal working week.
- It is the system administrator's duty to ensure that servers are operated in a secure manner. See System Administrator Advice Note.

System Configuration

- Servers must be appropriately configured. This entails ensuring that unnecessary services are turned off (or preferably not installed) and that access to the server is logged appropriately.
- System administrators must provide relevant logfile extracts to Corporate Information Systems (CIS) staff when this is required in order to investigate incidents involving suspected misuse of the system.
- System administrators are responsible for keeping server software up to date by the application of update patches.

Corporate Information Systems (CIS) Support

CIS will provide support for system administrators as follows:

- Advice on the selection of appropriate software and its configuration in order that a reasonably secure service may be provided.
- Advice on the procurement and installation of any update patches which may be required from time to time in order to keep the server operating securely. This may include the provision of a local repository of patches for common software products.
- Security auditing of individual servers at the request of the system administrator.
- Assistance on the investigation of any compromise of the server, and advice on the restoration of the service following a compromise.

Access Policy

- Services must be audited before remote access to the server will be granted.
- Remote access to any server will be immediately withdrawn if it proves impossible to contact the system administrator or any nominated deputy when this is required for any reason during normal working hours.
- Remote access to any server may be withdrawn if routine security auditing of the service reveals it to be insufficiently secure due to the installation of software with known vulnerabilities or configured in a way which permits the service to be compromised.

Physical Security

- Servers must not be located in public areas. Access to physical consoles must be restricted to prevent interference with server configuration or software.
- Remote access to servers for the purposes of system administration must use only approved secure protocols.
- Servers providing public access services should be located in the campus computer room, which provides a safeguarded mains power supply as well as a reasonably secure physical environment.

Enforcement

- In the event that the operation of any server causes disruption to other services for any reason including software malfunction or compromise of the system, the system administrator (or deputy officer) must take any action necessary to rectify the situation. If prompt action is not taken, CIS will take any action necessary up to and including physical disconnection

of the system. [Reversing the effect of any such action taken without the consent of CIS is to be regarded as a serious breach of the University's Acceptable Use Policy.]

- CIS staff who disconnect or restrict access to any server must promptly report the action together with the reason to the system administrator concerned and to their Head of Section.

Further Information:

Policy on Acceptable Use of University Computing and Data

Password Policy

System Administrator Advice Note

BS7799 Reference

A 3.1.2	Review and evaluation
A 4.1.3	Allocation of information security responsibilities
A 7.1.2	Physical entry controls
A 7.1.3	Securing offices, rooms and facilities
A 8.1.3	Incident management procedures
A 8.3	Protection against malicious software
A 7.2.1	Equipment siting and protection
A 9.7.1	Event Logging
A 9.7.2	Monitoring system use
A 12.2.1	Compliance with Security Policy
A 8.4.2	Operator Logs