



## UU Security Policy

### *System Administrator Advice Note*

<b>Author:</b>	Janine A. Asquith
<b>Approved by:</b>	CIS
<b>Version:</b>	2.0
<b>Date:</b>	1 <sup>st</sup> June, 2006
<b>Status:</b>	Agreed
<b>Classification:</b>	Public
<b>Enquiry point</b>	Janine A. Asquith University of Ulster Phone: 028 90368116 Email: <a href="mailto:ja.asquith@ulster.ac.uk">ja.asquith@ulster.ac.uk</a>
<b>Policy effective from:</b>	1 <sup>st</sup> Sept. 2002
<b>Policy review date:</b>	1 <sup>st</sup> May 2007

## Change History

Version	Changes	Date
1.0	Initial document	01/09/04
2.0	Included BS7799 Reference Change of department name to CIS	01/06/06

## Contents

UU Security Policy .....	1
System Administrator Advice Note .....	1
Change History .....	2
Contents .....	2
System Administrator Advice Note .....	3
Authorisation and Authority .....	3
Responsibilities .....	3
Recommendations for Administrators .....	3
Further Information.....	6
BS7799 Reference .....	6

## ***System Administrator Advice Note***

### **Authorisation and Authority**

- Delegated authority to administrator to control system by owner of equipment.

There should be at least one administrator and a deputy with system knowledge and administrator access available at all times during the University's business hours to be called upon by the owner department or Corporate Information Systems (CIS) for security reasons or emergencies.

### **Responsibilities**

1. Support of system and services for the accessibility of the server to registered users.
2. Protection of system and data integrity of server contents.
3. Adhere to, support and enforce legislation regarding security, Janet guidelines and UU electronic Information Security Policies, in particular the Server Connection Policy.

### **Recommendations for Administrators**

1. Support of Services and Accounts

- System Checks

System checks must be carried out daily to ensure the system remains operational and services are usable and accessible from the network. Activity must be logged and checked for evidence of misuse. These logs should be retained for inspection for a period of two years.

- Installations

Server systems install with more software and services than is necessary and also with user accounts with administrative rights created as default. Each of these must be examined to determine if they are part of the intended function of the server and those services and accounts which are not subsequently required should be disabled, de-installed or deleted and passwords set for accounts. Note that it is imperative that such configurations be set for the reboot sequence.

The CIS recommendation is to never perform a default installation of any operating system or application but to do a custom install so that the administrator appreciates what is being installed, where its associated files are being written and which accounts are being created as a consequence.

CIS strongly advise:

Disable all unused services, especially for the reboot sequence.  
Disable or password all accounts created using the Password Policy recommendations.

## 2. Protection of Systems & Data Integrity

### ➤ Restricted Account Passwords

The system console should always be password protected; either with a screen saver password or the Administrator account logged out. These two important passwords should be stored in a sealed envelope with the HFA's or Head of Department's office for access in the case of an emergency.

### ➤ User Accounts

There should be a policy of registering one account per named individual to adhere to the Network Connection Policy. This account should be given an initial password, set with a change upon login, to the individual concerned. This is to protect the users' privacy. Users should be encouraged to logout of the system once work is finished to safeguard filestore. User privileges should be set to match their required level of access.

### ➤ Intrusion Detection System Software

Where possible, some form of software should be installed to protect against unauthorised or malicious attack and monitor the traffic trying to access the server from the network. A campus firewall is installed to control access to services on the server but for additional protection a personal firewall can also be installed.

### ➤ Server Backups

System files should be backed up on a regular basis and those of the users on a daily basis to ensure that information lost inadvertently can be restored. The importance of backups cannot be overstated as this is the only secure way of recovering a corrupted file or data. The backup data should be regularly tested to ensure that it can be relied upon for restore when needed. These backup copies should be cycled and stored securely away from the server.

If there is access to a 'ghosted' version of the system via an emergency disc, this version should be updated after any system or application upgrade or patch revision.

➤ System and Application Upgrades

System software and applications should be upgraded and patched to the latest recommended versions on a regular or as required basis.

➤ Anti-Virus Software

Software should be installed to protect the system and updated regularly with new engines and data definition files as they become available to quarantine new viruses which may appear on the internet. CIS support McAfee's Netshield to detect viruses on incoming mail messages and Groupshield for viruses found within the user filestore.

### 3. Legislation and Policies

There should be at least two administrators of the system and at least one available at all times during the University's business hours, to be called upon by the owner department or CIS for security reasons or emergencies.

➤ Associated Operational Activities Required

1. Monitor and record connections to server

If running a web server or a peer to peer network, the owner could find himself classified as a service provider. The owner is required by law to retain logs and allow access to them upon demand by the police and intelligence services, without interception warrant. Please see below for a "best practice" document.

2. Examine any relevant files

3. Rename any files or change access permissions

4. Create relevant new files

5. Upon change of user filestore, affected user must be informed of change and reason for change as soon as possible.

➤ Policy Activities

If a file is deliberately protected by its owner, the administrator must not make any attempt to make content readable without authorisation from management or the owner of file.

➤ Disclosure of Information

Respect privacy of files and correspondence.

Information is treated as confidential, not to be disclosed to another person unless as part of a specific investigation. Such information may be passed to managers involved in investigation.

## Further Information

Electronic Information Security Policy  
Server Connection Policy  
Password Policy  
Network Connection Policy  
Personal Computer Security Advice Note

## BS7799 Reference

<b>A 3.1.2</b>	<b>Review and evaluation</b>
<b>A 4.1.3</b>	<b>Allocation of information security responsibilities</b>
<b>A 8.1.3</b>	<b>Incident management procedures</b>
<b>A 8.4</b>	<b>Housekeeping</b>
<b>A 9.7.1</b>	<b>Event logging</b>
<b>A 9.7.2</b>	<b>Monitoring system use</b>
<b>A 9.5.4</b>	<b>Password management system</b>
<b>A 12.2.1</b>	<b>Compliance with security policy</b>
<b>A 8.3</b>	<b>Protection against malicious software</b>
<b>A 8.1.2</b>	<b>Operational change controls</b>
<b>A 12.1.4</b>	<b>Data Protection and privacy of personal information</b>
<b>A10.5.4</b>	<b>Covert channels and Trojan code</b>