



## UU Security Policy

### *Monitoring Policy*

<b>Author:</b>	Janine A. Asquith
<b>Approved by:</b>	IICTSC
<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 Server and Hosts Systems Manager 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> June 2002
<b>Policy review date:</b>	1 <sup>st</sup> May 2007

## Change History

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

## Contents

UU Security Policy .....	1
Monitoring Policy .....	1
Change History .....	2
Contents .....	2
Monitoring Policy .....	3
Definition .....	3
Reason for Policy .....	3
POLICY .....	3
Enforcement of Policy .....	3
Relevant Legislation: .....	4
BS7799 Reference .....	4

## ***Monitoring Policy***

### **Definition**

Monitoring : is the interception of communications, checking of systems, the logging, recording, inspecting and auditing of data.

### **Reason for Policy**

There are legal requirements & conditions upon University of Ulster for connection to JANET.

There is a business requirement for monitoring because the University is liable under legislation for what employees and students do in the course of their work or study. It is one method of preventing, detecting or investigating abuse of the University's computer systems or resources.

### **POLICY**

Corporate Information Systems (CIS) may monitor and record communications

- To establish existence of facts to ascertain compliance with regulatory practices
- In interest of national security
- To prevent or detect crime
- To investigate or detect unauthorised use of networked systems
- To secure effective system operation

### **Enforcement of Policy**

Monitoring will be conducted in accordance with the requirements of the Data Protection Act 1998.

It will be necessary and proportionate to achieving the business purpose of the University yet respect the privacy of individuals.

Interception will only be by persons authorised by the University – typically CIS staff in accordance with their main areas of responsibility. Note that scanning without authority may well be a criminal offence, so such activities

must be agreed with the Compliance Officer (Director of Information Services) of the University.

Anyone found to have abused the facilities provided by the University in their course of study or during the performance of their duties will find themselves subject to the disciplinary ordinances of the University as set out in the Charter, Statutes, Ordinances and Regulations.

**Relevant Legislation:**

Data Protection Act (DPA '98) - fair processing of data - previously agreed with user or on application form.

Regulation in Investigatory Powers (RIP) Act 2000

Computer Misuse Act 1990.

Human Rights Act

Obscene Publications Act.

JISC Policies - Acceptable use policy, connections policy and security policy.

**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 12.1</b>	<b>Compliance with legal requirements</b>
<b>A 9.7.1</b>	<b>Event Logging</b>
<b>A 9.7.2</b>	<b>Monitoring system use</b>
<b>A 8.3</b>	<b>Protection against malicious software</b>