



## UU Security Policy

### *Electronic Information Security Policy*

<b>Author:</b>	Harry Young
<b>Approved by:</b>	IICTSC
<b>Version:</b>	2.0
<b>Date:</b>	1 June 2006
<b>Status:</b>	Agreed
<b>Classification:</b>	Public
<b>Enquiry point</b>	Harry Young Network Manager University of Ulster Phone: 028 90366488 Email: h.young@ulster.ac.uk
<b>Policy effective from:</b>	1 June 2002
<b>Policy review date:</b>	1 May 2007

## Change History

Version	Changes	Date
1.0	Initial document	1/6/02
2.0	Included BS7799 reference Change department name to CIS	1/6/06

## Contents

UU Security Policy .....	1
Electronic Information Security Policy .....	1
Change History .....	2
Contents .....	2
Electronic Information Security Policy .....	3
Reason for Policy .....	3
Scope .....	3
Responsibilities .....	3
Reporting Procedure .....	4
Sanctions.....	4
Further Information.....	4
BS7799 Reference .....	4

# ***Electronic Information Security Policy***

## **Reason for Policy**

The electronic information security policy of the University of Ulster is designed to,

1. Facilitate best operational practice for ensuring reliable, protected delivery and integrity of data and information necessary for University business.
2. Ensure that the institution complies with relevant legislation in this area.

## **Scope**

- University of Ulster network infrastructure
- Connections between the University infrastructure and external networks
- Host and server systems connected to the infrastructure
- Users of the infrastructure

## **Responsibilities**

- Corporate Information Systems (CIS) are responsible for providing adequate security, in accordance with current and future legislation, the JANET security policy and University regulations. These responsibilities will include,
  - providing the necessary information to enable users to assist with securing University information
  - the charge of granting and controlling access to JANET
  - taking measures to protect against attack
  - assisting in the investigation of a breach of security
- CIS will be solely responsible for the installation and configuration of active components of the network and corporate servers providing core services.
- CIS will provide relevant information to faculty or departmental contacts on securing non-CIS servers.
- CIS reserves the right to monitor use of the network, in accordance with current legislation,
  - in response to information regarding a specific threat or because of reported abuse
  - to diagnose problems
  - to analyse network performance
  - to protect network bandwidth for legitimate University business usage
- Users are responsible for complying with the University's Acceptable Use Policy and any other regulations for use of IT systems to be found in supplementary documents.

- Users must provide support to CIS with investigations into breaches or suspected breaches of security.
- Users are responsible for the security of their machines and locally stored data.

## Reporting Procedure

Security issues or suspected security threats should initially be reported to the Information Services Helpdesk on extension 66777. Calls will be escalated to the appropriate contact within CIS.

## Sanctions

1. In the case of suspected misuse or a compromised machine, it may become necessary to disconnect the user and/or machine from the network until the situation is investigated and rectified.
2. If a user of the University infrastructure misuses a system, they could find themselves in breach of the University disciplinary code and will be subject to disciplinary action.

## Further Information

Policy on Acceptable Use of University Computing and Data  
 Server Connection Policy  
 Network Connection Policy  
 Monitoring Policy  
 Wireless Communications Policy  
 Personal Computer Security Advice Note  
 System Administrator Advice Note  
 Password Policy  
 Janet Acceptable Use Policy  
 Janet 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 6.3.1</b>	<b>Reporting security incidents</b>
<b>A 6.3.2</b>	<b>Reporting security weaknesses</b>
<b>A 9.7.1</b>	<b>Event logging</b>
<b>A 9.7.2</b>	<b>Monitoring system use</b>
<b>A 12.1</b>	<b>Compliance with legal requirements</b>
<b>A 12.2.1</b>	<b>Compliance with security policy</b>