Information Services

The University of Kent
Information Technology Security Policy

1. General

The University IT Security Policy (*the Policy*) shall be approved by the Information Services Committee (ISC) taking the following into account:

1.1.1. The prevailing legislation;

1.1.2. The University's mission statement and objectives;

1.1.3. The views of interested parties including both information providers and users.

1.1.4. The terms and conditions of the JANET academic network operated by JANET (UK).

1.1.5. The terms and conditions of the Kentish MAN network operated by Kent MAN Ltd.

The Policy will seek to:

1.2.1. Protect the University from legal liability;

1.2.2. Protect the good name of the University;

1.2.3. Ensure effective operation of the processes of the University.

The *Regulations for the Use of IT Facilities* contain elements designed to ensure the security of University IT systems.

Regulations for the Use of Computers & Mobile Devices Not Owned and/or managed by the University and Connected to the University of Kent Network contains sections relating to computerised equipment not owned or managed by the University but connected to the University data network.

The *Security Procedures for Systems Administrators* define:

1.5.1. Who is authorised to undertake monitoring activities;

1.5.2. What types of monitoring are permitted;

1.5.3. How data collected during monitoring may be used.

The IT and the Library *Misuse/Abuse Procedures* define how suspected cases of misuse/abuse are handled.

The Policy defines a number of key roles in relation to IT system security.

2. Definitions of roles

The Network Controller has been identified by the University as the person designated as having the authority to perform interceptions on the University data network in accordance with the Regulation of Investigatory Powers (RIP) Act 2000 – (Communications Data) (Additional Functions and Amendment) Order 2006.

The Compliance Officer is the person with responsibility to ensure that the University data network is operated within UK law: principally the RIP Act 2000 and the Computer Misuse Act 1990 but also other relevant legislation.

The Systems Administrator is the person with responsibility for and privilege to perform the technical management of a computerised system. Specified Systems Administrators will be explicitly authorised by the Network Controller to perform particular types of monitoring within the scope of these procedures. These Systems Administrators may be from Professional Services or Academic Schools.

The Investigating Officer will assess cases of suspected misuse/abuse and initiate such investigations and actions as are appropriate under the terms of these procedures.

The IT and Library Implementation Officer may review such evidence as is collected by the Investigating Officer and assist in investigations, informal or formal proceedings according to the nature of the incident.

The University’s IT Security Team is headed by the Network Controller and has responsibility for the security of the University data network and attached systems. The Team will report suspected misuse to the Investigating Officer and liaise with Systems Administrators.

3. The Role of the Network Controller

The Network Controller has the primary authority to intercept data under the terms of the RIP Act 2000 and will authorise other members of staff to perform monitoring and/or investigative procedures as a result of misuse/abuse and will monitor the use of these procedures.

4. Kent IT Account Authentication

Information Services creates and maintains electronic user identities for members of the University and other authorised users of the University’s IT systems.

4.1 These identities are used to authenticate access to Professional Services or Academic School IT facilities.

4.2 Security access logs should be used on IT systems where appropriate to ensure that systems administrators are able to check for unauthorised access attempts.

4.3 Temporary withdrawal of user accounts may be necessary for operational and/or misuse/abuse reasons.

5 Connection of IT Systems to the University Network

5.1. The *Regulations for the Provision of Network Services on the University of Kent Network* defines the conditions under which the Network Controller will permit the connection of University owned computerised (and mobile) equipment and devices to the University data network.

5.2. Before allowing a connection the Network Controller may require a risk assessment taking the following into account:

5.2.1. The benefits of a service measured against the University's mission statement and objectives.

5.2.2. The hazards associated with the provision of the service. Issues include hardware reliability and maintenance; software reliability and maintenance (including updates); potential cost of loss of data or service; disaster recovery plans; interaction with other University systems.

5.2.3. The availability of qualified and sustainable systems administration staff.

5.3. It is a condition of connection to the University data network that the Network Controller be authorised to investigate suspected cases of misuse/abuse involving the connected system.

5.4. There will be lightweight or fast track procedures for simple cases such as managed desktop systems.

5.5. There will be specific procedures for the connection of non University owned computers to the Network [see *Regulations for the Use of Computers & Mobile Devices Not Owned and/or Managed by the University and Connected to the University of Kent Network*]

6. Suspected Misuse

6.1. The Systems Administrator is authorised by the Network Controller to take all reasonable actions to assure the provision and operation of the service.

6.2. Suspected misuse must be reported to the Investigating Officer as soon as possible. The Investigating Officer will authorise appropriate investigations to be carried out.

6.3. Where an IT system has been involved in a security incident steps must be taken to contain the damage; where appropriate:

6.3.1. The system must be disconnected from the network to ensure that:

6.3.1.1. Unauthorised access to or modification of data is prevented;

6.3.1.2. The system does not present a risk to other IT systems;

6.3.1.3. Evidence is not compromised or liable to loss.

6.3.2. The system must be rebuilt taking note of best security practice.

7. Minimising Risks

7.1. Systems Administrators should adopt procedures for the following:

7.1.1. Regular reviews of security and audit information;

7.1.2. Applying manufacturer's security updates in a timely fashion;

7.1.3. Backup of stored data;

7.1.4. The use of properly maintained anti-virus software is recommended;

7.1.5. A local firewall product may be necessary.

8. Access to and from the Internet

8.1. Information Services will operate and maintain security firewalls at the boundary between the campus networks and the Internet.

8.1.1. It is noted that the Internet poses a significant extra hazard to IT systems and heightened security awareness is required to minimise the associated risk.

8.1.2. It is noted that there is a risk of (possibly private) data from campus based systems being sent to the Internet for example as a result of infection of IT systems (malware[1], Jailbreaking[2] etc).

8.2 Restrictions will be placed on the types of data traffic permitted to enter or leave the University and the IT systems allowed to send or receive this traffic.

8.2.1. The types of traffic allowed or denied will be reviewed periodically (or in response to specific security threats) by ISC.

9. Access within the University

9.1 Security controls will be put in place within the University network to protect high-risk facilities from potential attack.

9.2 Networks will be categorised for security purposes:

[1] Software designed to infiltrate a computer system without the owner's informed consent

[2] Unlocking mobile devices (like Apple iPad, iPhone, iPod Touch, Android mobile phones and tablets) with the user choosing to run software code on the device other than that authorised by the manufacturer

9.2.1. Public server networks will house facilities which are accessible from most parts of the campus network and, where appropriate, from off campus.

9.2.2. Networks to which public access IT facilities are connected may be restricted as to those parts of the campus network they can access.

9.2.3. Private networks are likely to provide services to academic or administrative staff. Access to private networks from other parts of campus may be restricted to provide a more secure working environment.

9.2.4. Restrictions may be placed between the student study bedroom network and the rest of the campus network.

9.2.5. Restrictions may be placed between the wireless network and the rest of the campus network.

9.3. Analysis of the required usage pattern for a service will be used to design suitable security controls.

10. Connecting to University Services from off campus

10.1. The personal computer/laptop/netbook/mobile device can be the weakest link in the security model, therefore:

10.1.1. A virtual private networking (VPN) system will be provided by Information Services to enable encrypted secure sessions between authorised users from off-site and the University facilities;

10.1.2. Users of personal computers/laptops/netbook/mobile devices should where appropriate ensure that their computer/device runs an effective anti-virus software package;

10.1.3. Users of personal computers/laptops/netbook/mobile devices are encouraged to consider running a properly configured personal firewall package where appropriate to protect their computer/device from attack while connected to the Internet.

11. Reviews

11.1. An annual audit of security incidents will be reported to ISC.

11.2. This Policy will be reviewed from time to time with recommendations submitted to ISC by the Director of Information Services.

11.3. Connection risk assessments will be reviewed annually or as a result of security incidents.