EDINBURGH NAPIER UNIVERSITY ELECTRONIC INFORMATION SECURITY POLICY

Overall Policy

1. Introduction

Edinburgh Napier University's policy is that information it manages shall be protected against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information to authorised users. For information security to be effective it requires the participation and support of all Edinburgh Napier University staff, student and other persons who have access to its information technology.

Information security at the University is governed by its Electronic Information Security Policy which consists of this Overall Policy and a number of subsidiary policies. The subsidiary policies cover specific issues, technologies and types of usage. It is the responsibility of every information technology user to know these policies, and to conduct their activities accordingly.

The Electronic Information Security Policy has been ratified by the Principal's Executive Group (PEG) and forms part of the University's policies and procedures. This policy is managed on behalf of PEG by the Director of Information Services and the University's Information Security Officer working within Information Services (IT).

The policy shall be reviewed and updated regularly to ensure that it remains appropriate in the light of any relevant changes to the law, new threats, organisational policies or contractual obligations. All changes to this policy will be communicated to staff and students.

To determine the appropriate levels of security measures to be applied to information systems a process of risk assessment shall be carried out for each system to identify the probability and impact of security failures.

Edinburgh Napier University will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its Electronic Information Security Policy.

All users must comply with this Electronic Information Security Policy. Failure of a user to comply with this policy will lead to the relevant disciplinary procedures being invoked and in certain circumstances actions may be reported to the police or legal action may be taken (see section 9).

2. Scope

The Electronic Information Security Policy applies to all staff and students of the University and any other persons who are authorised to access the University's information technology facilities.

This policy covers all uses of information technology. Specifically this policy applies to all use of information and information technology on the University's premises even if the University does not own the equipment, to all information technology provided by the University wherever it is used, and to all external access to the University's information technology from wherever this is initiated.

N.B. The above statement includes all home working using University information and information technology.

3. Roles and Responsibilities

The Director of Information Services is responsible for proposing updates to the Electronic Information Security Policy which will be reviewed annually and as required. Revisions to the Electronic Information Security Policy will be approved by the PEG. If necessary proposals will be submitted identifying resources required to improve security measures to support the revised policies.

The University's Information Security Officer is responsible for advising appropriate persons on the compliance with this policy and its associated codes of practice.

The responsibility for ensuring the protection of specific information systems, and ensuring that specific security processes are carried out, lies with the System Sponsor for that system. The System Sponsor is normally the head of the department managing that information system.

Any manager within Information Services (IT) acting as Duty Manager can approve emergency action to be taken when required to enforce this policy. Longer term action requires the written approval of a member of PEG within 2 working weekdays.

4. Business Continuity

All systems will be subject to a formal risk assessment exercise to determine their level of criticality to the organisation and to determine where and at what level business continuity planning is needed.
Where required business continuity plan will be developed. The level of the plan will be commensurate with the criticality of the system to which it relates.

All business continuity plans will be periodically tested. The frequency of testing will be as defined for the level of the plan and will include tests to verify whether management and staff are able to put the plan into operation.

All relevant staff will receive appropriate training to be able to carry out their roles with respect to business continuity plans.

Each business continuity plan will be reviewed, and if necessary updated. The frequency of reviews will be as defined for the level of the plan.

5. Security Breaches

In the first instance users should report any suspicion of a breach of this policy directly to the IT Support Desk. Confidentiality of the information relayed will be ensured although for particularly sensitive matters a user may wish to speak directly to the Information Services (IT) Duty Manager. This information will be relayed to the Information Security Officer who will investigate the security breach.

If a suspected or actual breach of security has occurred the Information Security Officer may request action is taken to remove system access, data or software from the equipment.

The Information Services (IT) managers have the authority to protect the University against breaches of security by whatever means is deemed necessary and reasonable. These actions, if still continuing, will require the written authority of a PEG member within 2 working days.

6. Monitoring and Logging

The University will monitor network activity. Information Services (IT) will proactively consider reports from JANET Computing Emergency Response Team (JANET CERT) and other security sources and take action and/or make recommendations that maintain the security of Edinburgh Napier University's Information Security.

For full details on monitoring please refer to the **Monitoring and Logging** Policy Statement which can be found in the following locations:

Staff: go to the "Information Security Policy" page within the Information Services (IT) section of the Staff Intranet.
Students: go to the "Information Security Policy" page within the "Staying Safe Online" section of the IT myNapier pages.

7. Supporting Policies

The Electronic Information Security Policy's subsidiary policy statements amplify the overall Policy Statement and are available on the University website. Staff, students and other persons authorised to use the information technology of Edinburgh Napier University are required to be familiar with these policies and work accordingly within them. The subsidiary policies are listed below:

- User Policy
- Monitoring and Logging Policy

Links to the User Policy and Monitoring and Logging Policy can be found in the following locations:

Staff: go to the "Information Security Policy" page within the Information Services (IT) section of the Staff Intranet.
Students: go to the "Information Security Policy" page within the "Staying Safe Online" section of the IT myNapier pages.

This policy covers the security of electronic information and it normally does this by controlling the technology without which the information cannot be accessed. The security of non electronic information is covered by the following policy:

- Manual Data Security Policy. Available on the following intranet page: http://staff.napier.ac.uk/services/secretary/governance/DataProtection/Pages/SecurityofPersonalData.aspx

8. Legislation

Information security at the University is subject to various items of legislation including the following:

1. Copyright, Designs and Patents Act (1988)
2. Computer Misuse Act (1990)
3. Criminal Justice and Public Order Act (1994)
4. Data Protection Act (1998)
5. Human Rights Act (1998)
6. Regulation of Investigatory Powers Act (2000)
7. lawful Business Practice Regulations (2000)
8. Regulation of Investigatory Powers (Scotland) Act (2000)
9. Freedom of Information (Scotland) Act (2002)
10. Communications Act (2003)
11. Terrorism Act (2006)
12. Police And Justice Act (2006)
13. Acceptable Use Policy of the Joint Academic Network (JANET), a copy of which can be viewed at URL:

    http://www.ja.net/company/policies/aup.html

Users must comply with any regulations and instructions displayed alongside Information Technology facilities

9. User Compliance and Disciplinary Action

The staff terms and conditions of employment state that employees' must follow the University regulations which include this policy.

Line managers must provide specific guidance on legal compliance to any member of staff whose duties require it.

The student regulations state that students must follow University regulations which include this policy.

All third party users who are given access to the University information technology must agree to abide by the University's Electronic Information Security Policy.

This policy is available electronically in the Information Services (IT) section of the Staff Intranet and the IT section of myNapier. It is also available in hard copy from the IT Support Desk. Updates will be published in the same locations.

Failure of a user to comply with any part of the Electronic Information Security Policy will lead to the relevant disciplinary procedures being invoked and actions may be reported to the police or legal action may be taken.

10. Disclaimers

Edinburgh Napier University accepts no responsibility for the malfunctioning of any equipment or software, failure in security or integrity of any stored program or data or for any loss alleged to have been caused whether by defect in the resources or by act or neglect of Edinburgh Napier University, its employees or agents.