



Information Systems Security Policy

Document Status Details

Title	Information Systems Security Policy
Status	Approved
Version History	1
Date	October 2008

Information Systems Security Policy

1 Introduction

1.1 Information Systems play a major role in supporting the day-to-day activities of the Company. The availability, confidentiality and the data integrity of the Company's information systems are essential to the success of its academic and administrative activities. Effective security is achieved by working with a proper discipline, in compliance with legislation and Company policies.

1.2 The various System Security Policies set out the responsibilities for ensuring the security of Information Systems within the Company and the procedures to be followed to safeguard the resources provided and the confidentiality and integrity of the information held thereon; the maintenance of the Company's good name and the avoidance of civil or criminal proceedings.

1.3 The policies apply to all staff of the Company and all other users authorised by the Company. They relate to their use of Company-owned/leased/rented and on-loan facilities, to all private systems, owned/leased/rented/on-loan, when connected to the Company network directly or indirectly, to all Company-owned/licensed data/programs, be they on Company or on private systems, and to all data/programs provided to Company by sponsors or external agencies.

1.4 The objectives of this policy are to:

- Ensure that all of the Company's computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse;
- Ensure that all users are aware of and fully comply with this Policy Statement and all associated policies;
- Ensure that all users are aware of and fully comply with the relevant UK and European Community legislation;
- Create across the Company an awareness that appropriate security measures must be implemented as part of the effective operation and support of Information Security (IS);
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.

1.5 Definitions of the terms used in this Policy Statement, the IS Security Policies and the supporting documentation may be found at Annex 1.

1.6 This Policy Statement has been approved by the Company, which has delegated the implementation of it to the Directors.

2 Responsibilities for Information Systems Security

2.1 Table of Responsibilities

Position / Officer	Role / responsibilities
Managing Director	<ul style="list-style-type: none"> • Chair of the Risk Management Group • Accounting Officer • Chief Executive Officer
Company Secretary	<ul style="list-style-type: none"> • Chief Administrative Officer • Convener of the Risk Management Group
Directors	<ul style="list-style-type: none"> • Ensuring physical security procedures for Company premises are in place and being followed • Ensuring safety procedures are in place and being followed • Liaison with emergency services • Provision of resources for the implementation of the information security policy and for recovery procedures • Overall control of disaster recovery procedures • Management of teams or working groups to ensure the development and maintenance of policies and procedures
Data Protection Officer	<ul style="list-style-type: none"> • Maintenance of Data Protection Policy • Maintenance of data protection registration(s) • Provision of support documents • Provision of advice on data protection issues • Monitoring of compliance
Webmaster	<ul style="list-style-type: none"> • Development of standards for the creation and maintenance of web pages • Operation of the web site to provide a consistent web presence with minimum downtime
Members of staff	<ul style="list-style-type: none"> • Acting in accordance with Company policies • Taking personal backups on a regular basis • Acquainting themselves with support documents and other relevant materials when provided

2.2 Special Information Security Groups

Risk Management Group

Managing Director
Company Secretary
Directors

3 Compliance with Legislation

3.1 The Company has an obligation to abide by all UK legislation and relevant legislation of the European Community. Of particular importance in this respect is the Computer Misuse Act 1990 and the Data Protection Act 1998; these policies satisfy the Data Protection Act's requirement for a formal statement of the Company's security arrangements for personal data. The requirement for compliance devolves to all users defined in (1.3) above, who may be held personally responsible for any breach of the legislation.

3.2 Summaries of the legislation most relevant to the Company's IS policies may be found on the Company's Web Site

4. Risk Assessments and Security Review

4.1 The Risk Management Group must periodically carry out a risk assessment of the business value of the information users are handling and the IS security controls currently in place, in order to take into account changes to operating systems, changing business requirements and priorities and any changes in the relevant legislation and revise their security arrangements accordingly.

5. Breaches of Security

5.1 The Administrative Unit will monitor network activity, reports from the Computer Emergency Response Team (CERT) and other security agencies and take action/make recommendations consistent with maintaining the security of Company IS.

5.2 Any member of staff suspecting that there has been, or is likely to be, a breach of IS security should inform the Managing Director immediately who will advise on what action should be taken.

5.3 In the event of a suspected or actual breach of security, the Directors may, after consultation with the relevant line manager, make inaccessible/remove any unsafe user/login names, data and/or programs on the system from the network.

5.4 Any breach of security of an Information System could lead to loss of security of personal information. This would be an infringement of the Data Protection Act 1998 and could lead to civil or criminal proceedings. It is vital, therefore, that users of the Company's Information Systems comply, not only with this policy, but also with the Company's Data Protection Policy and associated policies, details of which may be found on the Company website.

5.5 The Managing Director and Directors has the authority to take whatever action is deemed necessary to protect the Company against breaches of security.

6. Policy Awareness and Disciplinary Procedures

A copy of this Policy Statement will be given to all new members of staff by the Personnel & Training Officer. Existing staff and students of the Company, authorised third parties and contractors given access to the Company network will be advised of the existence of this policy statement and the availability of the associated policies and guidelines which are published on the Company website. Failure of member of staff to comply with this policy may lead to the instigation of the relevant disciplinary procedures and, in certain circumstances, legal action may be taken. Failure of a contractor to comply could lead to the cancellation of a contract.

7. Supporting Policies and Guidance Notes

7.1 Supporting Policies amplifying this Policy Statement and guidelines associated with these policies are published with it and are available on the Company Web.

7.2 Staff and any third parties authorised to access the Company Network to use the systems and facilities identified in para (1.3) of this policy, are required to familiarise themselves with these and to work in accordance with them.

7.4 Further Guidance Notes will also be published to facilitate this.

8. Status of the Information Systems Security Policies

These policies do not form part of a formal contract of employment with the Company, but it is a condition of employment that employees will abide by the Regulations and policies made by the Company from time to time.

Other bodies receiving services from the Company have Service Level Definitions with these policies embedded in them.

ANNEX 1

DEFINITION OF TERMS USED IN THE POLICIES AND GUIDANCE NOTES

Company Network: A system of physical computer network apparatus and logical network connections that are identifiable with the Company by an Internet network domain-identifier, such as .net or by some other means. This definition shall also apply where, by agreement of the Company, third-party network service providers provide facilities that are identifiable with the Company Network, for example 'virtual local area network' (VLAN) and 'virtual wide area network' (VWAN) type connections.

Local Area Network (LAN): that combination of networks and computing and network equipment serving an Office of the Company.

System Administrator: a person or persons responsible for the day-to-day operation and management of an Information Server.

Data Controller: a member of Company staff who, in the terms of the Data Protection Act 1998, either alone or jointly, determines the purposes for which and the manner in which any personal data are, or are to be processed on Company equipment or manually in paper files. It is the duty of the Data Controller to comply with the data protection principles in respect of all personal data under his/her control and, where necessary, impose extra security measures in respect of this data, subject to the approval of the Data Protection Officer.

Data Owner: a person who authorises the use of a Company information system to originate, store, edit and/or publish material on that system, subject to the security procedures laid down by the Directors.

Data User: a person authorised by a data owner to access a Company information system to originate, store, edit and/or publish material on that system, subject to the security procedures laid down by the Directors, although the data owner may impose additional security on that data with the approval of the Managing Director.

Information System: a single computer, group of computers, server or group of servers which stores and processes information for a discrete purpose to facilitate teaching, research and administrative activities, and which may be accessed by staff or third parties authorised to do so.

Information Server: any computer system which may be used to store, publish, distribute, advertise or in some other way make available information such as text, images, video and sound to people and automated aspects on the Internet. Examples include but are not limited to: E-mail servers, mailing-list servers, Web servers, Usenet News Servers (NNTP servers), FTP servers, Gopher Servers, Index Servers, Multimedia servers, Mirror archives, Internet Relay Chat servers.

Data Protection Officer: a person appointed by the Company to manage the registration of the Company's use of personal data under the Data Protection Acts 1994 and 1998, to advise the Secretary General on the appropriateness of the Company's Data Protection Policy, monitor the Company's compliance with that policy and to be the Company's point of contact with the Government's Information Commissioner appointed under the 1998 Act.