INFORMATION SECURITY POLICY

SUMMARY OF PRINCIPAL CHANGES

General changes	
This document has been subject to the annual review process led by the Chief Information Officer and has been re-issued with minor amendments, effective 1 September 2014.	
Section	
1.1	Refer to text
3.2	Refer to text – re-draft for clarification

*(Amendments to version **03.0**, UPR IM03, are shown in italics.)*

Structure

1 INTRODUCTION

1.1 This document sets out the University's Information Security Policy and identifies the key security principles which underpin this policy. It is supplementary to the Information Management Policy (UPR IM02[1]) and should also be read in conjunction with UPR IM08[2], UPR IM01[3], UPR IM19[4], UPR SA12[5], UPR IM13[6], UPR IM11[7], UPR IM16[8] and UPR IM10[9], which contain some elements of information security policy, the staff computing guide and the JANET Acceptable Use Policy.

1.2 This document is informed, but not bound, by the standard code of practice: ISO/IEC 17799:2000; the UCISA/JISC Information Security Toolkit (Edition 3); and the requirements of the *UK Government 'Cyber Essentials Scheme'.*

1.3 This document was originally approved with effect from 11 May 2007[10].

2 PURPOSE

The University's information and the systems that manipulate that information are major corporate assets which must be protected. In determining its Information Security Policy the University has adopted principles, policies and practices which maximise protection against risks so that the security of its information and systems is assured.

3 SCOPE

3.1 All Members of the University, as defined in UPR GV06[11], are required to comply with this policy which also applies to collaborative activities undertaken with Partner Organisations.

3.2 Wholly-owned subsidiary companies which operate with the Financial Regulations (UPR FR06[12]) of the University are automatically subject to the policies and procedures set out in this document (UPR IM03). Wholly-owned subsidiary companies of the Corporation and their wholly-owned subsidiaries (w*here they operate* with separate Financial Regulations), and companies in which the University has an interest (partly-owned companies), will be subject to the policies and procedures set out in this document (UPR IM03) unless, for good reason, an exception is granted by the Chief Information Officer. *Where the Chief Information Officer has given consent,* provision will be made, as necessary, in Financial Regulations, *relevant* Shareholder's Agreements and *relevant* Memoranda of Understanding.

---

1 UPR IM02 'Information Management Policy'
2 UPR IM08 'Data Protection'
3 UPR IM01 'Computer Networks, Security of Information Systems and the Protection of Information Systems from Computer Viruses'
4 UPR IM19 'Internet, online communications and social media'
5 UPR SA12 'Learning Resources'
6 UPR IM13 'Software and On-Line Services'
7 UPR IM11 'Records Management and the Archiving and Retention of Prime Documents'
8 UPR IM16 'Data Management Policy'
9 UPR IM10 ' Privacy Policy'
10 **Academic Board Minute:** 403, 13 June 2007, refers
11 UPR GV06 'Membership of the University'
12 UPR FR06 'Corporate Governance and Financial Regulation'

4 KEY SECURITY PRINCIPLES

4.1 The University has identified the following key security principles as being fundamental to its Information Security Policy. They are the basis for the main policy areas set out in section 5.

4.2 Availability

To enable them to fulfil their defined roles, Members of the University will have access to information and the systems that manipulate that information within the limits of the privileges granted to them.

4.3 Integrity

The information available to Members of the University should be accurate, timely and complete so that the University is able to conduct its academic and business processes effectively.

4.4 Confidentiality

Confidential information should only be available to those who have been authorised to access it. Information that is not confidential should be easily available without restriction.

4.5 Compliance

The information should be held and manipulated in such a way that the University's legal, statutory and contractual obligations are not compromised.

4.6 Responsibilities of Members of the University

All users of University information shall be appropriately authorised. Members of the University should understand fully their responsibilities in relation to information security and comply with the relevant University policies and regulations. Managers will be responsible for defined areas of information security.

4.7 Analysis

Information Security Policy will be based on the systematic identification of appropriate and relevant risks.

5 MAIN POLICY AREAS

5.1 Each of the following policy areas will be used as the basis for Risk Analysis (UPR FR03[13], refers) through which a series of Management Controls will be identified.

5.2 Business Continuity

The University is required to develop and maintain a Business Continuity Plan based on a formal risk analysis. Responsibilities within the Plan should be clearly established and appropriate staff development provided to enable Members of the University to meet those responsibilities. The Plan will be tested and reviewed regularly.

---

[13] UPR FR03 'Risk Assessment and Management'

5.3 Compliance

(This section should be read in conjunction with UPR IM08[2].)

Information management processes must enable the University to comply with its legal and statutory obligations and any contractual obligations and national agreements it has entered into. Each of the following must have a named individual responsible for compliance issues: Data Protection; Freedom of Information; Copyright; Intellectual Property; Software Protection and Licensing; Equipment Disposal and each area will have a detailed policy governing its management.

5.4 Outsourcing and Third Party Access

(This section should be read in conjunction with UPR IM01[3], UPR IM16[8] and UPR HS05[14].)

5.4.1 External suppliers who are contracted to supply goods and services to the University that will bring them into contact with the University's information resources must agree to abide by the Information Security Policy and related documents. A suitable summary of these policies should be made available.

5.4.2 Any contracts with facilities management or outsourcing companies must include service levels that address information security issues and conform to this policy.

5.5 Personnel

5.5.1 Membership of the University is defined in UPR GV06[11].

5.5.2 Termination of Membership or change of Membership status within the University will result in a modification of information system access privileges as stipulated in UPR IM01[3].

5.5.3 Where a post has a specific Information Security responsibility this will be made clear in the job description. All Members of the University should have a clear understanding of their responsibilities under the Information Security Policy and should receive an appropriate briefing at induction.

5.6 Operations

5.6.1 The security risks to the information assets of all system development projects shall be assessed and access to those assets shall be controlled.

5.6.2 Changes to operational procedures must be controlled to ensure ongoing compliance with the requirements of information security and must have appropriate management approval.

5.6.3 Areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security and access control. Members of the University with authorisation to enter such areas are to be provided with information on the potential security risks and the measures used to control them.

5.6.4 The procedures for the operation and administration of the University's business systems and activities must be documented with those procedures and documents being regularly reviewed and maintained.

5.6.5 Duties and areas of responsibility shall be segregated to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to the University.

---

[14] UPR HS05 'Security and Public Access'

5.6.6 Procedures will be established and widely communicated for the reporting of security incidents and suspected security weaknesses in the University's business operations and information processing systems. Mechanisms shall be in place to monitor and learn from those incidents.

5.6.7 Procedures will be established for the reporting of software malfunctions and faults in the University's business critical information processing systems. Faults and malfunctions shall be logged and monitored and timely corrective action taken.

5.6.8 Development and testing facilities for business critical systems shall be separated from operational facilities and the migration of software from development to operational status shall be subject to formal procedures.

5.6.9 Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place.

5.6.10 Procedures shall be established to control the development or implementation of all business critical operational software. All systems developed for or within the University must follow, as a minimum, the University's Project Management Guidelines.

5.7 **Information handling**

5.7.1 The creation and management of records must conform to the University's record management policy (UPR IM11[7], refers).

5.7.2 An inventory will be maintained of all the University's business critical information assets and the ownership of each asset will be clearly stated. Each asset will be classified according to sensitivity using the University's agreed information security classification scheme.

5.7.3 When permanently disposing of equipment containing storage media, all sensitive data and licensed software will be irretrievably deleted before the equipment is moved off site.

5.7.4 Screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons.

5.7.5 Individuals responsible for business critical systems must ensure that appropriate backup and system recovery procedures are in place.

5.7.6 Backup of the University's information assets and the ability to recover them is an important priority. Management is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the University.

5.7.7 Management must ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of data files, especially where such files may replace files that are more recent.

5.7.8 All hardcopy documents of a sensitive or confidential nature are to be stored securely within lockable cupboards. When no longer required and, in accordance with the University's record management policy (UPR IM11[7], refers), paper records should be shredded or disposed of using a University approved secure disposal service. The document owner must authorise or initiate this destruction.

5.7.9 Prior to sending sensitive information or documents to third parties, the intended recipient must be authorised to receive the information and the procedures and information security measures adopted by the third party must also be seen to continue to assure the confidentiality and integrity of the information.

5.7.10 Sensitive data or information may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured.

5.7.11 All parties/participants are to be notified in advance whenever telephone conversations or videoconference events, such as lectures, are to be recorded.

5.7.12 The identity of recipients or requesters of sensitive or confidential information via the telephone must be verified and they must be authorised to receive the information requested.

5.7.13 No University computer should store credit card or debit card data. The use of credit and debit cards to pay on-line for University services should only be via a University-approved payment agent and with the prior agreement of the Deputy Vice-Chancellor and *Group Finance Director* (or designated deputy).

5.7.14 The University should maintain a list of its on-line journals, e-books and other on-line information sources and services accessible on subscription and ensure that access to these is protected by a suitable authentication mechanism.

5.8 User Management

(This section should be read in conjunction with UPR IM01[3] and UPR SA12[5])

5.8.1 Procedures for the registration and de-registration of Members of the University and for managing access to all information systems shall be established to ensure that all users' access rights match their authorisations. These procedures shall be implemented only by suitably trained and authorised staff.

5.8.2 All users shall have a unique identifier (user ID) for their personal and sole use for access to all the University's information services. The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason (section 5.2, Appendix II, UPR IM01[15], refers).

5.8.3 The selection of passwords, their use and management must adhere to best practice guidelines.

5.8.4 Access control standards must be established for all information systems, at an appropriate level for each system, which minimises information security risks yet allows the University's business processes to be carried out without undue hindrance.

5.8.5 Access to all systems must be authorised by the Data Steward *(as defined in UPR IM16[8])* and/or manager responsible for the information system and a record must be maintained of such authorisations, including the appropriate access privileges and user roles granted.

5.8.6 Procedures shall be established for all information systems to ensure that the access privileges of Members of the University are adjusted appropriately, and in a timely manner, whenever there is a change in business need or role or the Member leaves the University. Members' access privileges will be reviewed at regular intervals.

5.9 Use of computers

(This section should be read in conjunction with, UPR IM01[3], UPR IM19[4], UPR IM16[8] and UPR SA12[5].)

5.9.1 Equipment must be safeguarded appropriately, especially when left unattended.

---

15 Appendix II, UPR IM01 'Security of Management and Administrative Information'

5.9.2 Files downloaded from the internet, including files attached to electronic mail, must be treated with the utmost care to safeguard against both malicious code and inappropriate material. Such files, or any others not known to come from a trusted source, must be scanned for possible malicious code before being opened.

5.9.3 Electronic mail must not be used to communicate unencrypted confidential or sensitive information.

5.9.4 Any essential information stored on a laptop or other mobile device or on the local disk (C: drive) of a personal computer must be backed up regularly. Generally, this should be done by transferring the files to the relevant University system and/or file storage where it will be backed up automatically. It is the responsibility of the user to ensure that this takes place on a sufficiently regular basis.

5.9.5 Sensitive or confidential data should only be accessed from equipment in secure locations and files must never be printed on a networked printer that does not have adequate protection or security.

5.9.6 Utmost care must be used when transporting files on removable media, for example, disks, CDROMs, USB flash drives or similar devices, to ensure both information security and that valid files are not overwritten or incorrect or out of date information is not imported.

5.9.7 The University's Virtual Private Network (VPN) service must be used for off-campus and wireless network access to the University's management and administration systems and services.

5.9.8 Members of the University are not permitted to load any software onto the University's personal computers, laptops, workstations or servers that is not appropriately licensed or is illegal or could potentially threaten the integrity of the network.

5.10 **Systems Planning**

The implementation of new systems or related projects should be informed by the University's Project Management Guidelines.

5.10.1 Prior to acceptance, all new or upgraded systems shall be tested to ensure that they comply with the University's information security policies, access control standards and requirements for on-going information security management.

5.10.2 New information systems or enhancements to existing systems must be authorised jointly by the manager(s) responsible for the information and the Chief Information Officer. The business requirements of all authorised systems must specify requirements for security controls.

5.10.3 The information assets associated with any proposed new or updated systems must be identified, classified and recorded, in accordance with the University's record management policy (UPR IM11[7], refers) and a risk assessment undertaken to identify the probability and impact of security failure.

5.10.4 Equipment supporting critical business systems shall be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment shall be correctly maintained.

5.10.5 Equipment supporting critical business systems shall be given adequate protection from unauthorised access, environmental hazards and electrical power failures.

5.10.6 Access controls for all information and information systems are to be set at appropriate levels in accordance with the value and classification of the information assets being protected.

5.10.7 Access to operating system commands and system administration functions on servers is to be restricted to those persons who are authorised to undertake these operations as part of their job description.

5.11 **Systems management**

(This section should be read in conjunction with UPR IM01[3].)

5.11.1 The University's systems shall be managed by suitably trained and qualified staff to oversee their day-to-day running and to preserve security and integrity in collaboration with individual system owners. All systems management staff shall be given relevant training in information security issues.

5.11.2 Access controls shall be maintained at appropriate levels for all business critical systems and applications by on-going proactive management. Any changes of access permissions must be authorised by the Data Steward and/or manager of the information system or application and a record of the access permissions granted must be maintained.

5.11.3 Access to all information services, other than those to which there is public access, shall use a secure log on process. All access to information services is to be appropriately logged and monitored to identify potential misuse of systems or information.

5.11.4 Where feasible, inactive connections to the University's business systems shall shut down after a defined period of inactivity to prevent access by unauthorised persons.

5.11.5 Password management procedures shall be put into place to ensure the implementation of the requirements of information security policies and to assist users in complying with best practice guidelines.

5.11.6 The implementation of new or upgraded software must be planned and managed carefully. Formal change control procedures, with audit trails, shall be used for all changes to business critical systems. All changes must be properly tested and authorised before moving to the live environment.

5.11.7 The implementation of new or upgraded software and/or data loads by external suppliers and third party organisations is subject to prior planning and agreement with the University through the relevant trained and qualified systems management staff.

5.11.8 Capacity demands of systems supporting business processes shall be monitored and projections of future capacity requirements made to enable adequate processing power, storage and network capacity to be available.

5.11.9 Security event logs, operational audit logs and error logs must be properly reviewed and managed by qualified staff.

5.11.10 System clocks must be regularly synchronised between the University's various processing platforms.

5.12 **Network management**

(This section should be read in conjunction with UPR IM01[3].)

5.12.1 The University's network shall be managed by suitably authorised and qualified staff to oversee its day-to-day running and to preserve its security and integrity. All network management staff shall be given relevant training in information security issues.

5.12.2 The network must be designed and configured to deliver high performance and reliability to meet the University's needs, whilst providing a high degree of access control and a range of privilege restrictions.

5.12.3 The network must be segregated into separate logical domains with routing and access controls operating between the domains. Appropriately configured firewalls shall be used to protect the networks supporting the University's critical business systems.

5.12.4 The network must be monitored for malicious intrusion and proactively scanned for vulnerabilities.

5.12.5 Access to the resources on the network must be strictly controlled to prevent unauthorised access. Access control procedures must provide adequate safeguards through robust identification and authentication techniques. Access to all computing and information systems and peripherals shall be restricted, unless explicitly authorised.

5.12.6 Remote access to the network will be subject to robust authentication and VPN connections to the network are only permitted for authorised users ensuring that use is authenticated and data is encrypted during transit across the network.

5.12.7 The implementation of new or upgraded software or firmware must be planned and managed carefully. Formal change control procedures, with audit trails, shall be used for all changes to critical systems or network components. All changes must be properly tested and authorised before moving to the live environment.

5.12.8 Moves, changes and other reconfigurations of users' network access points will only be carried out by staff authorised by the Chief Information Officer (or nominee) *in accordance with procedures determined by the Chief Information Officer from time-to-time.*

5.12.9 Networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised intrusion.

5.13 Business Critical Software Management

(This section should be read in conjunction with UPR IM13[6].)

5.13.1 The University's critical business applications are to be managed by suitably trained and qualified staff to oversee their day-to-day running and to preserve security and integrity in collaboration with the key stakeholders. All critical business application staff shall be given relevant training in information security issues.

5.13.2 The procurement or implementation of new, or upgraded, software must be carefully planned and managed and any development for or by the University must always follow a formalised development process. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls.

5.13.3 Business requirements for new software or enhancement of existing software shall specify the requirements for information security controls.

5.13.4 Formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to business software. All changes must be properly authorised and all software, including that which interacts with the amended software, must be tested before changes are moved to the live environment.

5.13.5 Modifications to vendor supplied software shall be discouraged. Only strictly controlled, essential changes shall be permitted and the development of interfacing software shall only be undertaken in a planned and controlled manner.

5.13.6 The implementation, use or modification of all software on the University's business critical systems shall be controlled. All software shall be checked before implementation to protect against malicious code.

5.14 **Mobile computing**

5.14.1 Members of the University accessing information systems remotely to support business activities must be authorised to do so by an appropriate authority within the University. A risk assessment, based on the criticality of the information asset being used, must be carried out. Where technically feasible, all access should be through the VPN.

5.14.2 The University will publish guidelines for users of mobile computing equipment advising them on how these should be used to conform to the University's information security policy and other good practices.

6 MONITORING AND REPORTING

6.1 *Overall responsibility for the implementation of the Information Security Policy resides with the Chief Information Officer.*

6.2 The Chief Information Officer must be informed of all breaches of information security through regular reporting channels and for major breaches on an ad hoc emergency basis. The Chief Information Officer should bring major breaches to the notice of the Office of the Vice-Chancellor, as appropriate.

6.3 This policy will be reviewed every three (**3**) years or, exceptionally, more frequently if risk analysis or audit suggests there are new security threats that require it to be revised.

Mrs S C Grant
Secretary and Registrar
Signed: **1 September 2014**