Information Security

Policy

Document Control

Date	Revision/Amendment Details & Reason	Author
July 2010	Initial Document approved by Council	M Beecroft
October 2014	Updated policy	M Beecroft

1. Introduction

1. 1 Background

Computer and information systems underpin all the University's activities and are essential to its research, teaching and administrative functions. Information security is an integral part of information management whether the information is held in electronic or hard copy form. The purpose of security in any information system, computer installation or network is to ensure that:-

- maintain the integrity of information so that it is accurate, up to date and 'fit for purpose'
- information is always available to those who need it and there is no disruption to the business of the University
- confidentiality is not breached so that information is accessed only by those authorised to do so
- University resources are not used by criminals or hostile states to exploit vulnerabilities in security as a route to carrying out their nefarious activities
- The University meets its legal requirements including those applicable to personal data under the Data Protection Act
- The reputation of the University is safeguarded

The level of security required in a particular system will depend upon the risks associated with the system, the data held on the system and the working environment of the system.

This policy has been developed consistent with the Security Policy section of ISO 17799 and the UCISA Toolkit on Information Security.

The ISO standards are periodically reviewed and the most recent version published was in June 2005(ISO/IEC 17799:2005) which has subsequently been adopted as ISO/IEC 27002.

1.2 Need for a security policy

The data stored in **manual and electronic systems** used by the University is a valuable asset. The increasing reliance on Information Technology for the delivery of University services and achievement of strategic objectives makes it essential to ensure that these systems are developed, operated, used and maintained in a safe and secure fashion.

The increasing needs to transmit information across networks of computers render the data more vulnerable to accidental or deliberate unauthorised modification or disclosure.

This information security policy provides management direction and support for information security across the University. Specific, subsidiary policies shall be considered part of this information security policy and shall have equal standing.

This policy has been ratified by the University and forms part of its policies and procedures, including its Regulations for Staff and Student Conduct and Discipline. It is applicable to and will be communicated to staff, students and other relevant parties.

1.3 Who is affected by the policy

The policy applies to anyone using the University's IT facilities. This will include:-

- All staff and students
- Visitors to the University and people accessing the University's On-Line services from off campus
- External partners, contractors and agents based onsite and using the University network or offsite and accessing the University's systems
- Tenants of the University using the computers, servers or network
- Visitors using the University's Wireless service
- Students and staff from other institutions logging on using eduroam

1.4 Where the policy applies

The policy applies to all locations from which the University systems are accessed (including home use or other remote use). Where there are links to enable non University organisations to have access to University information, the University must confirm the security policies they operate meet the security requirements or the risk is understood and mitigated.

The policy applies to all systems and all information whether academic, administrative or any other.

1.5 Security Policy Objectives

- To ensure every user has a proper awareness and concern for computer systems security and an adequate appreciation of their responsibility for information security
- To provide a framework giving guidance for the establishment of standards, procedures and computer facilities for implementing computer systems security
- To specify University responsibilities
- To ensure all staff and students have an awareness of the relevant legislation
- To ensure that all staff are aware of their accountability and that they are aware that failure to comply with the Information Security Policy is a disciplinary offence which may include up to and including summary dismissal. Any action taken will conform to the appropriate University Human Resources policies.

1.6 Governance of the Policy

To manage information security within the University, the IS Steering Committee will include within its Terms of Reference the oversight of this area in order to ensure that there is clear direction and visible management support for security initiatives.

The responsibility for ensuring the protection of information systems and ensuring that specific security processes are carried out shall lie with the relevant head of the department managing that information item or system. Specialist advice on information security shall be made available throughout the University.

The University will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its information security policy.

To determine the appropriate levels of security measures 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.

Within the context of the IS Steering Group and University committees this policy shall be reviewed and updated regularly to ensure that it remains appropriate in the light of any relevant changes to the law, University policies or contractual obligations.

The implementation of the information security policy shall be reviewed independently of those charged with its implementation.

2. Security Policy

Use of Computers

- 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.
- The selection of passwords, their use and management must adhere to best practice guidelines
- Equipment must be safeguarded appropriately – especially when left unattended
- Files downloaded from the internet, including mobile code and 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
- Electronic mail must not be used to communicate confidential or sensitive information unless appropriate measures have been taken to ensure authenticity and confidentiality, that is correctly addressed and that the recipients are authorised to receive it
- Any essential information stored on a laptop or on a PC's local disk must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis.
- 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.
- Utmost care must be used when transporting files on removable media (e.g. disks, CDROMs and USB flash drives) to ensure that valid files are not overwritten or incorrect or out of date information is not imported
- Employees are not permitted to load unapproved software onto the University's PCs, laptops and workstations

Teleworking

- Persons who will be doing part or all of their work using dedicated equipment in a fixed location outside the University (teleworking) must be authorised to do so by an

appropriate authority within the relevant University manager. A risk assessment based on the criticality of the information assets being used and the appropriateness of the proposed telework location should be carried out.

- Teleworkers will be provided with appropriate computing and communications equipment and must use only this equipment for teleworking. The equipment provided may only be modified or replaced if this has been authorised. All equipment must be returned at the end of the teleworking arrangement, or when the teleworker leaves the University.
- All teleworking agreements must include appropriate measures, based on a risk assessment, to protect the security of information assets. Teleworkers must follow the agreed security procedures at all times.
- All teleworking agreements must include rules on the use of equipment provided for teleworking. Teleworkers must abide by these rules at all times unless specifically authorised.

Mobile Computing

- Persons 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.
- 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.

Outsourcing and Third Party Access

- All third parties who are given access to the University's information systems, whether suppliers, customers or otherwise, must agree to follow the University's information security policies. A summary of the information security policies and the third party's role in ensuring compliance will be provided to any such third party, prior to their being granted access.
- The University will assess the risk to its information and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, the University will require external suppliers of services to sign a confidentiality agreement to protect its information assets.
- Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the content and spirit of the University's information security policies.
- All contracts with external suppliers for the supply of services to the University must be monitored and reviewed to ensure that information security requirements are being satisfied. Contracts must include appropriated provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.
- Any facilities management, outsourcing or similar company with which the University may do business must be able to demonstrate compliance with the University's information security policies and enter into binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance..

Operations

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

- 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.
- Duties and areas of responsibility shall be segregated, where practicable, to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to the University
- 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.
- Procedures will be established for the reporting of software malfunctions and faults in the University's information processing systems. Faults and malfunctions will be recorded and timely corrective action taken
- Changes to operational procedures must be controlled to ensure on-going compliance with the requirements of information security and must have management approval.
- Development and testing facilities for business critical systems will be separated from operational facilities and the migration of software from development to operational status shall be subject to formal change control procedures
- 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
- Procedures shall be established to control the development or implementation of all operational software. All systems developed for or within the University must follow a formalised development process
- The security risks to the information assets of all system development projects shall be assessed and access to those assets shall be controlled.
- Equipment supporting business systems shall be given adequate protection from unauthorized access, environmental hazards and failures of electrical power or other utilities.

System Planning

- New information systems, or enhancements to existing systems, must be authorised jointly by the manager(s) responsible for the information and the Director of I.T. Services. The business requirements of all authorized systems must specify requirements for security controls.
- The implementation of new or upgraded software must be carefully planned and managed, to ensure that the information security risks associated with such changes are mitigated using a combination of procedural and technical controls. Formal change control procedures, with audit trails, shall be used for all changes to critical systems or network components.
- The information assets associated with any proposed new or updated systems must be identified, classified and recorded, in accordance with the Information Handling Policy, and a risk assessment undertaken to identify the probability and impact of security failure.
- Equipment supporting 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
- 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
- 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 ongoing information security management.

System Management

- 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.
- Access controls shall be maintained at appropriate levels for all systems by on-going proactive management and any changes of access permissions must be authorised by the manager of the system or application. A record of access permissions granted must be maintained
- Access to all information services shall use a secure log on process and access to the University's business systems shall also be limited by time of day or by the location of the initiating terminal or both. All access to information services is to be logged and monitored to identify potential misuse of systems or information
- Inactive connections to the University's business systems shall shut down after a defined period of inactivity to prevent access by unauthorised persons
- Access to operating system commands is to be restricted to those persons who are authorised to perform systems administration or management functions. Use of such commands should be logged and monitored
- 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 made available
- Security event logs, operational audit logs and error logs must be properly reviewed and managed by qualified staff
- System clocks must be regularly synchronised between the University's various processing platforms

Network Management

- The University network will be managed by suitably authorised and qualified staff to oversee its day to day running and preserve its security and integrity in collaboration with individual system owners. All network management staff will be given relevant training in information security issues.
- 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
- 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 business systems.
- Access to the resources on the network must be strictly controlled to prevent unauthorised access and 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.
- 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.
- Moves, changes and other reconfigurations of users' network access points will only be carried out by staff authorised by IT Services according to procedures laid down by them
- Networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised intrusion

User Management

- Procedures for the registration and deregistration of users 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.
- Password management procedures shall be put into place to ensure the implementation of the requirements of the information security policies and to assist both staff and students in complying with best practice guidelines.
- 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 activities to be carried out without undue hindrance. A review period will be determined for each information system and access control standards will be reviewed regularly at those intervals.
- Access to all systems must be authorised by the manager responsible for the system and a record must be maintained of such authorisations, including the appropriate access rights or privileges granted.
- Procedures shall be established for all information systems to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, staff change their role, or staff or students leave the University. Users' access rights will be reviewed at regular intervals.

Software Management

- 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.
- Business requirements for new software or enhancement of existing software shall specify the requirements for information security controls.
- 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.
- 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.
- The implementation, use or modification of all software on the University's business systems shall be controlled.
- All software shall be checked before implementation to protect against malicious code.
- The need for systems to support mobile code (applets, scripts, etc.) shall be reviewed. Where the use of mobile code is necessary, the environment shall be configured so as to restrict its ability to harm information or other applications.

Personnel

- All employees are required to abide by University policies.
- Any information security incidents resulting from non-compliance should result in appropriate investigation. If a user is found to have violated the University's information security policy and/or procedures, they may be disciplined in line with the University's formal disciplinary process.
- All employees are required to sign a formal undertaking concerning the need to protect the confidentiality of information, both during and after their employment with the University.

- Non-disclosure agreements must be used in all situations where the confidentiality, sensitivity or value of the information being disclosed is important.
- New employees' references must be verified appropriately, and the employees must undertake to abide by the University's information security policies.
- All external suppliers who are contracted to supply services to the organisation must agree to follow the information security policy of the University. An appropriate summary of the information security policies must be formally delivered to any such supplier, prior to any supply of services
- The University's systems shall be managed by suitably authorised and qualified staff to oversee its day to day running and to preserve its security and integrity. All systems management staff shall be given relevant training in information security issues.

Cryptography

- A policy on cryptographic controls will be developed with procedures to provide appropriate levels of protection to sensitive information whilst ensuring compliance with statutory, regulatory and contractual requirements.
- Confidential information will only be taken for use away from the University in an encrypted form unless its confidentiality can otherwise be assured
- Procedures shall be established to ensure that authorised staff may gain access, when needed, to any important business information being held in encrypted form
- The confidentiality of information being transferred on portable media or across networks, must be protected by use of appropriate encryption techniques
- Encryption shall be used whenever appropriate on all remote access connections to the University's network and resources.
- A procedure for the management of electronic keys, to control both the encryption and decryption of sensitive documents or digital signatures, must be established to ensure the adoption of best practice guidelines and compliance with both legal and contractual requirements.
- Important business information being communicated electronically shall be authenticated by the use of digital signatures; information received without a digital signature should not be relied upon

Business Continuity

- The University Senior Management Team will review business continuity requirements and identify appropriate areas for further action.
- A formal risk assessment exercise will be carried out on an annual basis to review the classification of all systems according to their level of criticality to the University and to determine where business continuity plans require amendment.
- A business continuity plan will be maintained for each system or activity. The nature of the plan and the actions it contains will be commensurate with the criticality of the system or activity to which it relates.
- All business continuity plans will be periodically tested. The frequency of testing will be as defined for the appropriate criticality level 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 appropriate criticality level...
- Management is responsible for ensuring that the frequency of such backup operations and the procedures for validating the recovery meet the needs of the business.

Compliance

- The University's IT Acceptable Use policy sets out all employees' responsibilities with respect to their use of computer based information systems and data. Line managers must provide specific guidance on legal compliance to any member of staff whose duties require it.
- The student regulations incorporate the University's IT Acceptable Use Policy which sets out all students' responsibilities with respect to their use of computer based information systems and data.
- All members of the University will comply with the Information Security Policy, I.T. Acceptable Use Policy, Portable Data Device Policy, Communications Policy and the Data Protection Policy and, where appropriate, their compliance will be monitored.
- Before any new systems are introduced, a risk assessment process will be carried out which will include an assessment of the legal obligations that may arise from the use of the system. These legal obligations will be documented and a named system controller, with responsibility for updating that information, will be identified.
- Guidance documents will be made available to all computer users through the I.T. website covering the key aspects of the law of copyright, in so far as they relate to the use of information systems. Guidance is also available on the key aspects of computer misuse legislation.
- The University's IT Acceptable Use Policy forbids the use of information systems to send or publish derogatory remarks about people or organisations.
- The University's data retention policy defines the appropriate length of time for different types of information to be held. Data will not be destroyed prior to the expiry of the relevant retention period and will not be retained beyond that period. During the retention period appropriate technical systems will be maintained to ensure that the data can be accessed
- Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities. Examples of this are records that may be required as evidence that the University operates within statutory regulations or to confirm the financial status of the University.
- Records may also need to be disclosed in compliance with the provisions of the Freedom of Information Act.
- An inventory of sources of key information should be maintained
- Appropriate measures should be implemented to protect essential records and information from loss destruction and falsification
- The University will only process personal data in accordance with the requirements of the data protection legislation. Personal or confidential information will only be disclosed or shared where an employee has been authorised to do so.
- Where it is necessary to collect evidence from the information systems, it shall be collected and presented to conform to the relevant rules of evidence. Expert guidance will normally be sought.
- All of the University's systems will be operated and administered in accordance with the documented procedures.
- Regular compliance checks will be carried out by the Internal Auditor to verify this compliance.

Information Handling

- An inventory will be maintained of all the University's major information assets and the ownership of each asset will be clearly stated

- Within the information inventory, each information asset will be classified according to sensitivity using the University's agreed information security classification scheme
- Classified information and outputs from systems handling classified data must be appropriately labelled according to the output medium
- 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 using procedures authorised by the University Secretary
- Damaged storage devices containing sensitive data will undergo appropriate risk assessment, to determine if the device should be destroyed, repaired or discarded. Such devices will remain the property of the University and only be removed from site with the permission of the information asset owner.
- A University wide clear desk and locked screen policy is advocated, particularly when employees are absent from their normal desk and outside normal working hours. In addition, 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.
- Removal off site of the University's sensitive information assets, either printed or held on computer storage media, should be properly authorised by management. Prior to authorisation, a risk assessment based on the criticality of the information asset should be carried out.
- Information owners must ensure that appropriate backup and system recovery procedures are in place and are executed
- 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 business.
- 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
- The archiving of information and documents must take place with due consideration for legal, regulatory and business issues, with liaison between technical and business staff, and in keeping with the University's Retention Policy Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.
- All users of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files. The degree to which software techniques and disciplined user procedures are necessary should be applied by management and determined by the classification of the information in question.
- Day to day data storage must ensure that current information is readily available to authorised users and that archives are both created and accessible in case of need
- Highly sensitive or critical documents should not rely upon the availability or integrity of (external) data files over which the author may have no control. Key documents and reports should normally be self-contained and contain all the necessary information.
- Hard copies of sensitive or classified material must be protected and handled according to the distribution and authorisation levels specified for those documents.
- All employees to be aware of the risk of breaching confidentiality associated with the photocopying (or other duplication) of sensitive documents. Authorisation from the document owner should be obtained where documents are classified as Confidential or above.
- All information used for, or by the University, must be filed appropriately and according to its classification
- All signatures authorising access to systems or release of information must be properly authenticated
- Unsolicited mail should not receive serious attention until and unless the sender's identity and authenticity of the mail have been verified

- All hardcopy documents of a sensitive or confidential nature are to be shredded or similarly destroyed when no longer required. The document owner must authorise or initiate this destruction.
- Any third party used for external disposal of the University's obsolete information bearing equipment or hardcopy material must be able to demonstrate compliance with this University's information security policies and also, where appropriate, provide a service level agreement which documents the performance expected and the remedies available in case of non-compliance.
- Prior to sending sensitive information or documents to third parties, not only must the intended recipient by authorised to receive such information, but 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
- 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 throughout the transfer
- Web browsers are to be used in a secure manner by making use of the built-in security features. Management must ensure that staff are made aware of the appropriate settings for the software concerned.
- Staff participating in conference and video conference must be made aware of the information security issues involved and be notified in advance if they are to be recorded.
- All parties are to be notified in advance whenever telephone conversations or video conference events, such as lectures, are to be recorded
- Email addresses and faxes should be checked carefully prior to dispatch, especially where the information content is sensitive; and where the disclosure of email addresses or other contact information, to the recipients is a possibility
- Any fax received in error is to be returned to the sender or destroyed. Its contents must not be disclosed to other parties without the sender's permission
- Unsolicited or unexpected faxes should be treated with great care until the sender has been identified
- The identity of recipients or requesters of sensitive or confidential information over the telephone must be verified and they must be authorised to receive it
- Electronic commerce systems, whether to buy or to sell goods or services, may only be used in accordance with appropriate technical and procedural measures. Staff authorised to make payment by credit card for goods ordered over the telephone or internet, are responsible for safe and appropriate use
- Important transaction and processing reports should be regularly reviewed by properly trained and qualified staff
- Email should only be used for business purposes in a way which is consistent with other forms of business communication. The attachment of data files to an email is only permitted after confirming the classification of the information being sent and then having scanned and verified the file for the possibility of a virus or other malicious code
- Information received via email must be treated with care due to its inherent information security risks. File attachments should be scanned for possible viruses or other malicious code