Kingston University London

Information Security Policy

Prepared by the University Secretary's Department

Approved by the Executive Board in April 2011

Contents

1. Definitions

In the policy document that follows the terms below are to be understood as indicated.

1.1 ‘Business Critical’ – Assessed as essential to the ongoing operation of the University’s core functions. The failure of a system rated as business critical will risk a serious detrimental impact to the University.

1.2 ‘Information Asset’ – A specific and defined body of information that supports, or is generated in the course of, University business. Information assets are often associated with particular systems and include, but are not limited to, data in databases and data files, system documentation, user manuals, training materials, operational and support procedures, continuity plans and archived information.

1.3 ‘Personal Data’ – As defined in section 1 of the Data Protection Act 1998, i.e. information about a living individual which is biographical in nature, and from which the individual concerned is potentially identifiable as the subject of the information.

1.4 ‘System’ – Equipment and/or software providing defined functionality in respect of one or more business areas.

1.5 ‘Service Manager’ – Staff member who has been given delegated authority by the Service Owner to carry out system management functions.

1.6 ‘Service Owner’ – Staff member with the final authority for any item of equipment, software or set of information.

1.7 ‘University’ – Kingston University and all of its subsidiary companies, including Kingston University Service Company Limited (KUSCO), at River House, 53-57 High Street, Kingston upon Thames, Surrey, KT1 1LQ and all associated locations.

2. Policy Statement

2.1 Information is fundamental to the effective operation of the University and is an important business asset. The purpose of this Information Security Policy is to ensure that the information managed by the University is appropriately secured in order to protect against the possible consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

2.2 ISO27002:2005 states that 'Information is an asset that, like other important business assets, is essential to an organisation's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected. Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.'

2.3 This document has been approved by the University Information Committee and the Executive Board as containing the high level policies necessary to provide direction and support for information security across the University. It has been based on the templates contained within the third edition of the UCISA Information Security Toolkit, which was itself developed to accord with the guidelines set out in ISO27001:2005; reference was also made to the Information Security Policy of the University of Birmingham, which is also based on the UCISA Toolkit.

2.4 This Policy forms part of the policies and procedures of the University. It is applicable to, and is to be communicated to, staff, students, and other parties who will have access to University held data or systems. Specific, subsidiary guidelines and codes of practice that have been or will be produced to support it should be considered part of this Policy and shall have equal standing with it.

2.5 This Policy and associated guidance shall be reviewed and updated regularly to ensure that they remain appropriate in the light of any changes in technology, the law, University policy or contractual obligations.

2.6 Specialist advice on information security shall be made available throughout the University by Information Services and the University Secretary’s Department.

3. Compliance

3.1 This Information Security Policy, in conjunction with the ICT Security Policy, sets out the responsibilities of all staff, students and third parties, including those based at collaborative partner institutions, in relation to their use of Kingston University information systems and data. Any individual who accesses the University's systems and/or data agrees, in so doing, to comply with the Information Security Policy, and where appropriate their compliance may be monitored.

3.2 All activities of the University must be conducted in accordance with current legislation. Line managers are responsible for ensuring that any member of staff whose duties require it receives specific guidance on legal compliance. If any user of information is unsure as to their responsibilities in relation to the law, they should seek advice from their line manager.

3.3 The use of information is governed by a number of different Acts of Parliament, together with various statutory instruments and other pieces of legislation. These currently include, but are not limited to:

Copyright, Designs and Patents Act 1988

Data Protection Act 1998

Human Rights Act 1998

Computer Misuse Act 1990

Regulation of Investigatory Powers Act 2000

Freedom of Information Act 2000

Electronic Communications Act 2000

Digital Economy Act 2010

3.4 Before any new system is 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 service manager, with responsibility for updating that information, will be identified.

3.5 Guidance is available through the University's website covering the key aspects of the law of copyright: http://www.kingston.ac.uk/library/copyright/index.html, and Freedom of Information: http://extranet.kingston.ac.uk/freedom_of_info/.

3.6 The acceptable use policies appended to the ICT Security Policy specify any uses of the University's information systems that are prohibited and in relation to which disciplinary action may be taken.

3.7 Information will be retained for appropriate periods of time that are consistent with business needs and relevant legislation. During retention periods appropriate technical systems will be maintained to ensure that data can be accessed.

3.8 The University will only process personal data in accordance with the requirements of data protection legislation. Personal or confidential information will only be disclosed or shared where a member of staff has been authorised to do so.

3.9 The University reserves the right to access data within information systems where this is necessary for management purposes specified in the ICT Security Policy. In cases where investigation of traffic or content of user accounts is necessary, Information Services technical staff will carry out such work under direct instruction from the Infrastructure Security Manager following authorisation from the Director of Human Resources/Director of Information Services (staff) or the Director of Student Services and Administration/Director of Information Services (students), and the University Secretary. The University will involve the police in all cases where it believes that illegal activity may have taken place.

3.10 All of the University's information systems will be operated and administered in accordance with relevant procedures, and the University may at any time monitor compliance with written authorisation of the Vice-Chancellor/Director of Human Resources/Director of Information Services (staff) or the Director of Student Services and Administration/Director of Information Services (students), and the University Secretary, if there are reasonable grounds to believe that a violation of University policy has taken place.

4. Human Resources

4.1 Terms and Conditions

4.1.1 All employees must comply with the University's Information Security Policy and ICT Security Policy. This requirement forms part of the University's Terms and Conditions of Employment, and new employees will be notified of the Policies when they sign their contract with the University.

4.1.2 Breaches of the University's Information Security Policy and/or associated procedures are potentially disciplinary issues, and may lead to action being taken in accordance with the University's disciplinary procedures.

4.1.3 All staff have a responsibility to ensure the security of information which they use or to which they have access. Staff must maintain the confidentiality of any information (both during and following their employment by the University) which comes into their possession in the course of their work and which is sensitive or confidential in nature. Such information must not be disclosed unless authorised or required by law. It is the responsibility of line managers to ensure that their staff receive adequate training in the secure use of information.

4.2 Recruitment and Contracts

4.2.1 All offers of employment will be subject to receipt of satisfactory references.

4.2.2 All third party organisations or individuals who are contracted to supply services to the University that require access to University information systems or to confidential or sensitive data must agree to follow the Information Security Policy of the University. An appropriate summary of the Information Security Policy as it applies to third parties must be provided to any such supplier, prior to supply of services.

4.3 Training and Awareness

4.3.1 All staff are to be provided with information security awareness tools to enhance awareness and educate them regarding the range of threats, the appropriate safeguards, and the need for reporting suspected problems.

4.3.2 The University is committed to providing training to all users of new systems to ensure that their use is both efficient and does not compromise information security.

4.3.3 Training will be made available to the Infrastructure Security Manager where appropriate to support them in maintaining their knowledge of current threats and information security techniques.

4.3.4 All new staff are to receive appropriate information security awareness training as part of induction. Where staff change jobs, their information security needs must be reassessed and any new training provided as a priority.

4.3.5 Appropriate training in information security threats and safeguards will be provided for staff involved in the installation and maintenance of IT systems, with the extent of technical training to reflect the job holder's individual responsibility for configuring and maintaining information security safeguards.

4.4 Staff Leaving the University

4.4.1 By default staff IT accounts will be disabled immediately the staff member leaves the University, on notification by HR; unless a separate temporary agreement is in place.

4.4.2 Leaving staff are to be treated sensitively, particularly with regard to the termination of their access privileges.

4.4.3 Leaving staff must return all information assets and equipment belonging to the University prior to departure, unless otherwise agreed with the service owner responsible for the asset.

5. Use of Computers and Access Control

5.1 User Management

5.1.1 The University's Application Access Policy specifies procedures for the registration and deregistration of users and for managing access to all information systems to ensure that all users' access rights match their authorisations. These procedures shall be implemented only by suitably trained and authorised staff.

5.1.2 All users shall have a unique identifier (user ID) for their personal and sole use to access University information services as appropriate. Personal user IDs must not be used by anyone else, and associated passwords shall not be shared with any other person for any reason. Shared accounts will only be allowed for special purposes, and with restricted functionality, on the written approval of the Infrastructure Security Manager. Such accounts will be disabled when deemed necessary by the Infrastructure Security Manager in conjunction with the service owner.

5.1.3 Password management procedures will be maintained to ensure the implementation of the requirements of the Information Security Policy and to assist both staff and students in complying with best practice guidelines.

5.1.4 Access control standards will be maintained 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. Access control standards will be reviewed for each information system at regular, pre-determined, intervals.

5.1.5 Access to all information 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.

5.1.6 Procedures will be maintained 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.

5.2 Use of Computers

5.2.1 IT equipment and other physical resources, including hard copy data, must be safeguarded appropriately – especially when left unattended.

5.2.2 Staff must take reasonable steps to ensure that data held electronically are not vulnerable to theft or inadvertent disclosure to unauthorised users. These include locking a workstation if it is to be left unattended. Each session of use must be terminated in accordance with published instructions.

5.2.3 The University installs protection against malicious software and computer viruses, where appropriate, on its computer systems. Users of these systems must not interfere with or prevent the operation of anti-virus protection. Care must be taken in this regard when transferring data to or from systems outside of the University network – including the transfer of data from home machines.

5.2.4 Email must not be used to communicate confidential or sensitive information unless appropriate measures have been taken to ensure confidentiality, that it is correctly addressed, and that intended recipients are authorised to receive it.

5.2.5 Appropriate precautions must be taken by management and staff to ensure that the risk of loss or damage to information is minimised. These precautions must include adequate back up and contingency arrangements for individual, local and centrally run information systems. Where appropriate, physical backup media should be stored in a fireproof safe remote from the physical system that has been backed up.

5.2.6 Sensitive or confidential data should only be accessed from equipment in secure locations, and files should only be printed on networked printers that have a level of security commensurate to the confidentiality of the information that is to be printed.

5.2.7 Care must be taken when transporting files on removable media (e.g. disks, CD-ROMs and USB flash drives) to ensure that current files are not overwritten, or obsolete or incorrect information imported.

5.2.8 Staff are only permitted to load software onto University IT equipment where this is consistent with the University's ICT Security Policy.

5.2.9 The University will maintain guidelines for staff that use mobile devices for business activities advising them on how these should be used to conform to the University's Information Security Policy and other good practices.

5.3 Third Party Access

5.3.1 All third party organisations who are contracted to supply services to the University that require access to information systems or the transfer of datasets must comply with the University's Information Security Policy. A summary of the Information Security Policy as it applies to third parties will be provided to any such contractor prior to access being granted or data being transferred.

5.3.2 Where an external supplier of services is to function as a data processor under the terms of the Data Protection Act 1998 – i.e. processing personal data on behalf of the University and in accordance with its instructions – the supplier will be required to sign an agreement to do so securely and in accordance with the Act. Additionally, 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.

5.3.3 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 Policy.

5.3.4 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 appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.

6. Information Handling

6.1 Asset Inventory

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

6.2 Equipment Disposal

6.2.1 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 Infrastructure Security Manager.

6.2.2 Damaged storage devices containing sensitive or confidential 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 may only be removed from the site with the permission of the information asset owner.

6.2.3 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 the University's Information Security Policy and also, where appropriate, provide a service level agreement which documents the performance expected and the remedies available in case of non-compliance.

6.3 Data Integrity

6.3.1 The University advocates a clear desk and screen policy 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.

6.3.2 Removal off site of the organisation'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.

6.3.3 Service owners must ensure that appropriate backup and system recovery procedures are in place.

6.3.4 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 business needs of the University. Backup media must be removable and stored in a fire proof safe that is remote from the physical system that has been backed up. In the case of critical information systems where 24/7 service is required, consideration must be given to deploying fault tolerant equipment such as redundant power supplies and 'RAID' disk configurations.

6.3.5 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.

6.3.6 The archiving of information and documents must take place with due consideration for legal, regulatory and business issues, and following liaison between technical and non-technical staff.

6.3.7 Storage media used for the archiving of information must be appropriate to the anticipated retention period. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.

6.3.8 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 determined by management with regard to the classification of the information in question.

6.3.9 Day-to-day storage must ensure that current information is readily available to authorised users and that archives are both created and accessible in case of need.

6.3.10 Highly sensitive or business critical documents should not rely upon the availability or integrity of (external) files over which the author may have no control. Key documents and reports should normally be self-contained and contain all necessary information.

6.3.11 Hard copies of sensitive or confidential material must be protected and handled appropriately.

6.3.12 All staff should be made aware of the risk of breaching confidentiality associated with the photocopying, scanning or other duplication of sensitive documents. Authorisation for copying should be obtained from the document owner where documents are classified as confidential or above.

6.3.13 All information used by the University must be stored appropriately.

6.3.14 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.

6.3.15 Prior to sending sensitive information or documents to third parties, not only must the intended recipient be authorised to receive such information, but the procedures and information security measures adopted by the third party must also continue to assure the confidentiality and integrity of the information.

6.3.16 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.

6.4 Communication by Telephone, Fax and Email

6.4.1 Staff participating in telephone or video conferencing must be aware of the information security issues involved.

6.4.2 All parties are to be notified in advance whenever telephone conversations, meetings or events are to be recorded.

6.4.3 Email addresses and fax numbers should be checked carefully prior to sending, and a risk assessment conducted, especially where the information content is sensitive or confidential or where the disclosure of email addresses or other contact information to recipients is a possibility.

6.4.4 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.

6.4.5 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.

6.4.6 Email should only be used for business purposes in a way which is consistent with other forms of business communication.

6.4.7 Information received via email must be treated with care due to its inherent information security risks. File attachments will be scanned for possible viruses or other malicious code.

6.5 Encryption

6.5.1 A policy on encryption controls will be developed with procedures to provide appropriate levels of protection to sensitive information whilst ensuring compliance with statutory, regulatory and contractual requirements.

6.5.2 Confidential information and personal data shall only be taken for use away from the University in an encrypted form unless their confidentiality and security can otherwise be assured.

6.5.3 Procedures shall be established to ensure that authorised staff may gain access, when needed, to any important business information being held in encrypted form.

6.5.4 The confidentiality and security of information being transferred on portable media must be protected by use of appropriate encryption techniques.

6.5.5 Encryption shall be used whenever appropriate on all remote access connections to the University’s network and resources.

6.5.6 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.

7. Network Management

7.1 The University’s network shall be maintained 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.

7.2 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.

7.3 The network shall be segregated to create security zones, with routing and access controls operating between the zones, to reduce the possibility of internal or external users gaining unauthorised access to systems. Systems with particularly high security vulnerabilities shall be protected both from internal and external access. All other systems will be protected from external access by default. Appropriately configured firewalls shall be used to protect the network supporting the University’s systems.

7.4 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.

7.5 The implementation of new or upgraded software or firmware must be carefully planned and managed. 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.

7.6 Moves, changes and other reconfigurations of network access points will only be carried out by authorised Information Services staff according to agreed procedures.

7.7 The network infrastructure must be adequately configured and safeguarded against both physical attack and unauthorised intrusion.

8. Systems Operation, Management and Development

8.1 Operations

8.1.1 All areas where sensitive or business critical information is processed shall be given an appropriate level of physical security and access control. All staff and third parties with authorisation to enter such areas are to be provided with information on the potential security risks, control measures to be taken, and the necessity of complying with the Information Security Policy.

8.1.2 The procedures for the operation and administration of the University's information systems, together with associated activities, must be documented by the service managers responsible for them, with the procedures and documents being reviewed and maintained at regular intervals.

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

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

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

8.1.6 Proposed changes to operational procedures must be assessed to ensure ongoing compliance with the requirements of information security, and must have management approval.

8.1.7 Development and testing facilities for business critical systems shall be separated from operational facilities where viable to do so. The migration of software from development to operational status shall be subject to formal change control procedures.

8.1.8 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.

8.1.9 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.

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

8.2 System Management

8.2.1 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.

8.2.2 Access controls shall be maintained at appropriate levels for all systems by ongoing 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.

8.2.3 Access to all information systems, except those which are publicly accessible, shall use a secure logging-on process, and may also be limited by time of day, location of workstation, or through an automatic time-out after a defined period of inactivity, where appropriate. Access to information systems may be logged and monitored to identify potential misuse of systems or information.

8.2.4 Password management procedures shall meet the requirements of the Information Security Policy.

8.2.5 Systems administration or management functions shall only be performed by authorised staff. Use of such commands should be logged and monitored where appropriate.

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

8.2.7 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.

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

8.2.9 System clocks must be regularly synchronised by authorised staff between the University’s various processing platforms.

8.3 System Planning

8.3.1 New information systems, or upgrades to existing systems, must be authorised jointly by the (proposed) service owner and the appropriate committees within the University’s governance structure. This process must ensure that security requirements have been appropriately specified.

8.3.2 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.

8.3.3 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.

8.3.4 Equipment supporting information 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.

8.3.5 Equipment supporting information systems shall be given adequate protection from unauthorised access, environmental hazards and failures of electrical power or other utilities.

8.3.6 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.

8.3.7 Access to operating system commands and application system functions is to be restricted to those persons who are authorised to perform systems administration or management functions. Where appropriate, use of such commands should be logged and monitored.

8.3.8 Prior to acceptance, all new or upgraded systems shall be tested to ensure that they comply with the University’s Information Security Policy, access control standards and requirements for ongoing information security management.

8.4 Software Management and Development

8.4.1 Software 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 nominated individual application owners. All staff involved in software management shall be given relevant training in information security issues.

8.4.2 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.

8.4.3 Specifications for new software or enhancement of existing software shall specify the necessary information security controls.

8.4.4 Formal change control procedures, with comprehensive audit trails, must be used for all 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.

8.4.5 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.

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

8.4.7 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.

9. Business Continuity

9.1 The University will continue to assess business continuity requirements and to identify appropriate areas for further action.

9.2 A formal risk assessment exercise has been conducted to classify all systems according to their level of criticality to the University and to determine where business continuity planning is needed.

9.3 A business continuity plan will be developed 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.

9.4 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.

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

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