Edge Hill University

Document Title	Information Security Policy
Document Owner	IT Services
Approved By	Information Strategy Group
Date Approved	June 2017
Date of Review	June 2018

1. **Scope and Purpose**

    a. Information Security is the practice of ensuring that information is stored, read, heard, edited, accessed and otherwise used by only those who have the right to do so.

    b. Information Security is often seen as a highly technical matter that requires specialist IT equipment and support. While there are many situations that do need this type of approach, the most sensible and effective first steps are based on common sense and sound information management practices. Assessing and understanding the risks for the University will help to establish the appropriate information management processes and procedures and, in turn, this should ensure appropriate incident management and recovery if security is compromised.

    c. The range of potentially undesirable consequences associated with breaches of information security includes:

        i. Information and/or systems being unavailable
        ii. Unauthorised access to personal data
        iii. Fraud
        iv. Bad publicity / reputational risk

    d. Information security can be achieved through the following:

        i. A pragmatic approach to policy and standards, resulting in an Information Security Policy which is supported by realistic and workable processes and procedures.
        ii. The rigour of security measures applicable to any information system, proportional to the assessed risk of the confidentiality, integrity or availability of its information becoming compromised.
        iii. A well-informed and, where appropriate, well-trained workforce exercising an appropriate level of vigilance.

    e. This Information Security Policy is applicable to, and will be communicated to staff, students and other relevant parties. The policy will be reviewed by the Information Strategy Group, the Risk Management Group and by other relevant University groups and committees.

2. **Information Security Policy**

    a. It is the policy of the University that information is managed and secured appropriately in order to protect the University and its members from the consequences of potential breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

    b. This Information Security Policy provides the framework for information security across the University and shall be reviewed and updated to ensure it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

    c. This Information Security Policy is applicable to, and will be communicated to staff, students and other relevant parties.

    d. The Information Strategy Group shall ensure that there is clear direction and visible management support for information security initiatives and, together with the Risk Management Group, shall ensure that appropriate business risks are assessed and monitored to identify the likelihood and impact of information related threats.

    e. The responsibility for ensuring the protection of individual information systems, and that associated system-specific security processes are in place, shall reside with the Director, Dean or Head of Area responsible for managing that information system.

3. **Business Continuity Planning**

   a. The University's Emergency Management Plan (EMP) is overseen by the Facilities Management Department, with contributions from all relevant areas of the University, and is reviewed annually by the Institutional Health, Safety and Environment Committee. The EMP focuses on the University's response to an emergency, and outlines how the University will liaise with internal and external agencies to coordinate actions in response to the requirements of the event.
   b. Specific departmental Business Continuity Plans (BCPs) are maintained and regularly reviewed by the individual departments and faculties where there is a greater understanding of, and responsibility for, managing the risks associated with their local operations, systems and business activities.
   c. The University Risk Management Group monitors and maintains a Risk Register of business critical risks, and this is reviewed regularly by the Governors Audit Committee.
   d. The software source code for each corporate business information system (Student Records, Finance, Payroll and Human Resources) is held under Escrow agreements with the National Computer Centre.

4. **Compliance**

   a. The University will only store, process, retain and disclose personal information in accordance with the requirements of the Data Protection Act and the University's Data Protection Registration and Data Protection Policy.
   b. The University has established policies and procedures to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of relevant information security requirements.
   c. All users of the University's computer based information systems are informed of their responsibilities under the University IT Acceptable Use Policy (AUP) and the Information Security Policy, and any suspected breach will be investigated and may be dealt with under the University's disciplinary procedures.
   d. Further specific guidance is available to computer users of corporate information systems.

5. **Outsourcing and Third Party Access**

   a. External suppliers who are contracted to supply goods or services to the University should, where appropriate, be informed of the University's Information Security Policy and Data Protection Policy, and may be required to agree to adhere to the policy, and to protect its information assets.
   b. 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.

6. **Human Resources**

   a. All members of the University must comply with the Information Security Policy of the University. Any Information Security incidents resulting from non-compliance may result in disciplinary action.
   b. The University will provide advice and guidance to users to ensure that their use is both efficient and does not compromise information security.
   c. Access privileges of staff will normally start on their first day of employment with the University (on completion, and approval, of the relevant Staff User Registration Form), and be terminated on their last day of employment. Access may be ceased / extended on application by a Dean / Director to the relevant PVC, who will refer the matter to the Director of IT Services where appropriate.

7. **Operations**

   a. Areas and offices where sensitive information is processed shall be given an appropriate level of physical security and access control to prevent unauthorised access, damage and interference.
   b. Software malfunctions and faults should be reported, logged and monitored via established procedures to ensure timely corrective action is taken.
   c. To ensure the correct and secure operation of information processing facilities, changes to operational procedures are controlled and, where appropriate, have management approval.
   d. Development and testing facilities for business critical corporate information systems are separated from 'live' operational instances, and the migration of software from development to operational status is subject to agreed change control procedures.
   e. User acceptance criteria for corporate information systems upgrades and new versions are required, and suitable tests of the systems carried out, prior to migration to 'live' operational status.

8. **Information Handling**

   a. The University has established a simple and pragmatic classification dividing information into two types: sensitive and non-sensitive.
   b. The removal or transfer of all sensitive information should be authorised by the appropriate line manager. In addition, sensitive information held on laptops, tablets, USB devices or other storage media must be encrypted using University prescribed software in accordance with the Information Handling Guidance.
   c. The University encourages a clear desk and screen policy, and screens on which sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons.
   d. Sensitive information should not rely upon the availability of systems or integrity of data files, and should normally be self-contained. Hard copies of sensitive information must be protected and handled according to the distribution and authorisation levels specified for those documents.
   e. Backup of the University's information assets and the ability to recover them is an important priority. Information owners, custodians and system administrators must ensure that appropriate backup and system recovery procedures are in place to meet the needs of the business, typically in liaison with IT Services staff.
   f. The archiving of information and documents must take place with due consideration for legal, regulatory and business issues, with liaison between IT Services staff and information owners, custodians and system administrators.
   g. All users of corporate 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.
   h. Appropriate measures should be taken when permanently disposing of sensitive information, be it paper-based or electronic, including the disposal of IT equipment or storage media containing sensitive information.
   i. Sensitive information may only be transferred across networks, transmitted by post or other similar means, or copied to other media, when the confidentiality and integrity of the data can reasonably be assured.
   j. All users must be aware of the risks of breaching confidentiality associated with the printing, photocopying or other duplication of sensitive information. All information used for, or by the University, must be stored, accessed and disposed of appropriately (see Appendix A – Information Handling Guidance).

9. **Cardholder Information**

    a. The University is committed to protecting confidential cardholder information.
    b. The purpose of this policy is to set out the basic requirements in respect of ‘cardholder data security’ and the associated transmission, processing and storage of cardholder data.
    c. Receiving and/or transmitting cardholder data

        - Cardholder data must never be accepted or sent by email or any other electronic method.
        - Cardholder data received on hard copy must only be transmitted to the processing location by hand delivery or secure courier, and must not be scanned or sent by internal post.

    d. Processing cardholder data

        - Cardholder data should be processed by appropriate methods only, preferably using Chip & PIN terminals, where the customer is present and able to enter their card details directly into the card terminal, or via the University’s approved online payment system.
        - Where the University uses approved third party payment service providers to process online card payments on its behalf, all such suppliers must be PCI compliant. Sanction must be obtained from the Director of Finance prior to using any alternative payment system.

    e. Storing cardholder data

        - Sensitive cardholder data must never be retained after being used for processing and must be permanently destroyed immediately after processing. This includes:
            - The Card Verification Code (CVC or 3 digit security code).
            - Track data (card electronic/stripe data)

10. **User Management**

    a. Established procedures for the registration and de-registration of users, and for managing access to corporate information systems, ensure that users’ access rights match their authorisations.
    b. Users shall have a unique identifier (user ID) for their personal and sole use for access to University 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 as defined within the University's IT Acceptable Use Policy.
    c. System password management criteria and access control standards are established to minimise information security risks and yet allow the University’s business activities to be carried out without undue hindrance.
    d. User access to corporate information systems must be authorised by the relevant line-manager, including the appropriate access rights or privileges granted. Users’ access rights must be adjusted appropriately, and in a timely manner, whenever there is a change in business need, staff change their role, or staff leave the University.

11. **Use of Computers**

a. The University's IT Acceptable Use Policy (AUP) defines in detail the appropriate use of University computers. The AUP is applicable to, and will be communicated to staff, students and other relevant parties.
b. IT equipment, mobile devices and storage media must be safeguarded appropriately - especially when left unattended.
c. Central University systems and filestores should be used for the storage of digital information, where it will be protected by a regular automated backup service. The local storage of information on the hard drive of PCs and laptops, or on USB devices, is discouraged and should be reduced as far as possible.
d. All sensitive information stored on a laptop or USB device must be encrypted. It is the responsibility of the user to ensure that this takes place, and that the information is backed up appropriately.

e. Utmost care must be used when transporting data on removable devices or media. Sensitive information must be encrypted, and should only be accessed from equipment in secure locations.

f. Email should only be used to communicate sensitive information where appropriate measures have been taken to ensure authenticity and confidentiality, that it is correctly addressed, and that the recipients are authorised to receive it.

g. Users are not permitted to load unapproved software on to the University’s PCs, workstations, laptops or other IT devices.

12. **System Planning**

a. The implementation of new or upgraded software must be carefully planned and managed. Change control procedures shall be used for new corporate information systems, or additional enhancements to existing systems, jointly authorised by the Director(s) responsible for the information and the Director of IT Services (or nominated designates).

b. 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.

c. 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 and are given adequate protection from unauthorised access, environmental hazards and electrical power failures.

13. **System Management**

    a. The University's corporate information systems must 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 or application owners.

    b. Access controls for all information and corporate information systems must be set at appropriate levels, and access to operating system commands and application system functions is restricted to those authorised to perform systems administration or management functions.

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

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

    e. Security, operational and error logs must be reviewed and managed by qualified staff.

14. **Network Management**

    a. The University's network is managed by suitably authorised and qualified staff to oversee its day-to-day running and to preserve its security and integrity.
    b. The network should be designed and configured to deliver high performance and reliability to meet the University's business needs whilst providing a high degree of access control and a range of privilege restrictions.
    c. Networks and communication systems must be adequately configured and safeguarded against both physical attack and unauthorised intrusion.
    d. Moves, changes and other reconfigurations of users' network access points will only be carried by staff authorised IT Services staff.
    e. Access to the resources on the network will be strictly controlled to prevent unauthorised access and access control procedures must provide adequate safeguards through robust identification and authentication techniques.
    f. Remote access to the network will be subject to similarly robust authentication.

15. **Software Management**

    a. The University's corporate information systems and business applications will 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.
    b. The procurement or implementation of new, or upgraded, software must be carefully planned and managed and any development for or by the University should follow the established approval processes.
    c. Change control procedures will be used for changes or upgrades to corporate information systems. All changes must be properly authorised and all software must be tested before changes are applied to the live environment.
    d. Modifications to vendor supplied software and the development of interfacing software shall only be undertaken in a planned, authorised and controlled manner by suitably trained and qualified staff.

16. **Mobile Computing**

    a. Persons accessing information systems remotely must be authorised to do so by the appropriate authority within the University.

    b. Users of mobile computing equipment must comply with guidelines on the use of such equipment advising them on how to use these in ways that conform to the University's Information Security Policy and Information Handling Guidance , IT AUP and other good practices.

17. **Teleworking**

    a. Persons who undertake part or all of their work using dedicated equipment in a fixed location outside the University (teleworking) must be authorised to do so by the appropriate authority within the University.

    b. Teleworkers should be provided with appropriate computing and communications equipment, should use only this equipment for teleworking, and should do so in ways that conform to the University's Information Security Policy and Information Handling Guidance , IT AUP and other good practices.

Related Documents

IT Acceptable Use Policy (AUP)

Information Handling Guidance

Reviewed and approved by Information Strategy Group 07-Jun-2017