University of Essex

INFORMATION SECURITY POLICY

The University of Essex is a knowledge organisation; our contribution to society is through the knowledge that we explore, create and convey. Information is the currency for our production and propagation of knowledge; credible academic or professional activity cannot be conducted without reference or access to it.[1]

1. Purpose and Scope

1.1 This policy provides a framework for the management of information security throughout the University. It applies to:

a) All those with to University information systems, including staff, students, visitors and contractors;
b) any systems attached to the University computer or telephone networks and any systems supplied by the University;
c) all information or data[2] processed by the University pursuant to its operational activities, regardless of whether it is processed electronically or in paper (hard copy) form, any communications sent to or from the University and any University information or data held on systems external to the University's network;
d) systems or information accessed remotely or via mobile devices;
e) all external parties that provide services to the University in respect of information processing facilities and business activities; and
f) principal information assets including the physical locations from which the University operates.

1.2 The policy applies equally to all areas of the University, although some areas will have their own additional requirements.

1.3 The policy is supported by other relevant University polices and guidance (see Section 7, below). Help and advice on the practical implementation of this policy is available.

2. Aims and Commitments

2.1 The University recognises the role of information security in ensuring that users have access to the information they require in order to carry out their work. Information underpins all the University's activities, and is essential to its research, teaching, commercial and administrative functions. People working with information need to be skilled and supported in handling it correctly. Much information is handled electronically and the University makes extensive use of information systems to manage its information.

2.2 There are two key areas of risk related to information. The first is any reduction in the confidentiality, integrity or availability of information which could prevent the University from functioning effectively and efficiently. The second is the loss or unauthorised disclosure of information has the potential to damage the University's reputation and cause financial loss. Loss of information in some circumstances may attract financial penalties.

---

[1] Information Supporting Strategy 2014-25. University of Essex. p2.
[2] Information and data are not synonymous terms, although they are often used interchangeably. The security of both is important: security of data often underlies and informs security of information since data underlies information. This document generally uses the term "information" but that should be taken to include data.

2.3 To mitigate these risks, information security must be an integral part of information management, no matter what form the information is held in.

2.4 The University is committed to protecting the security of its information and information systems in order to ensure that:

a) The integrity of information is maintained, so that it is accurate, up to date and fit for purpose;
b) information is available to those who need it, when they need it;
c) confidentiality is not breached, so that information is accessed only by those authorised to do so;
d) the University meets all of its legal and statutory requirements; and
e) the reputation of the University is safeguarded.

2.5 In order to meet these aims, the University is committed to implementing risk-based security controls. Information and information systems both feature in the University's approach to risk management and are listed in the University's operational risk register.

2.6 Information security risk assessments will be performed for all information assets on a regular basis in order to identify key information risks and determine the controls required to keep those risks within acceptable limits.

2.7 As part of the University's information culture all University students and staff will know how to access information, and understand their responsibilities towards it. They will be supported to be able to assess risk, take responsibility when things go wrong, and put things right quickly.

2.8 The ICT Steering Group, which includes members from relevant parts of the University, advises on and coordinates the implementation of this information security policy.

2.9 Mechanisms are in place to assess and address any breaches of information security.

3. Responsibilities

Council

3.1 Council has ultimate responsibility for information security within the University and determines the approach and policy for safeguarding personal, commercially or other sensitive information. Specifically, it is responsible for ensuring that the University complies with relevant external requirements, including legislation.

USG

3.2 The Registrar and Secretary is the principal officer of the senior executive team (University Steering Group - USG), with responsibility for Information Security and is the owner of this policy. The Registrar and Secretary is advised on relevant matters by the ICT Steering Group. The Registrar and Secretary is responsible for: The integrity of information is maintained, so that it is accurate, up to date and fit for purpose;

a) ensuring that users are aware of this policy;
b) seeking adequate resources for its implementation;
c) monitoring compliance;
d) overseeing regular reviews of the policy, having regard to any relevant changes in legislation, organisational policies and contractual obligations; and
e) ensuring there is clear direction and visible management support for security initiatives.

Heads of Section, Schools, Departments and Centres

3.3 Heads of Section and Heads of Departments, Schools, Centres and Institutes are responsible for ensuring that their department complies with the University's information security requirements and has effective systems in place for the managing of information security in accordance with this policy and the supporting documentation and guidance.

Information Champions

3.4 Each section, department or school has a designated information champion. Information champions may be members of academic or professional services staff. This University-wide network provides a focal point for information security in sections and departments, sharing good practice, providing practical advice, signposting staff to further advice and support, and monitoring problems. Information champions support Heads in meeting their information security responsibilities.

University Members

3.5 Every member of the University, including staff and students, and others granted access to University information or systems, has a responsibility for the safe use of that information and those information systems, and for working within the appropriate policies, procedures and structures that are in place to safeguard the security of information.

3.6 Users of University information will be made aware of their own individual responsibilities for complying with University and departmental policies on information security.

Third Parties

3.7 Agreements with third parties involving accessing, processing, communicating or managing the University's information, or information systems, should cover all relevant security requirements, including compliance with this policy, and be covered in contractual arrangements.

4. Integrity and availability of information

Integrity of Information

4.1 Integrity refers to the accuracy, consistency and completeness of information across its life cycle. Accurate information supports good decision making. For personal data ensuring data accuracy is a legal requirement.

4.2 Loss of integrity can occur at any stage in the lifecycle of information, particularly when it is being updated or transferred. Training and support for those handling information, and an awareness of the need for accuracy, are as important as technological checks or validation methods for maintaining integrity. It is the responsibility of those using data to check that care is taken to ensure that errors are not introduced at any stage.

4.3 The integrity of electronic data can also be compromised through viruses, malware, hacking, and other cyber threats, as well as though hardware errors, such a hard disk or memory device failure. Information systems will be protected by appropriate virus-check software, firewalls and other mechanisms, and through user-training to help individuals identify and deal with viruses, phishing and other attacks.

4.4 The integrity of paper information can be compromised through poor quality copies, inaccurate labelling, inadequate version control, poor filing practice, or storage.

Availability of Information

4.5 The University's Information Supporting Strategy requires that "data and information should be made available and accessible to all, as relevant, in a timely manner, via appropriate channels and in the right formats". Timely access supports efficient working, good decision making and service delivery. Availability is about more than just remote access: it includes paper items being clearly labelled and promptly and correctly filed to aid speedy retrieval.

4.6 IT Services, or others providing systems, software or services, should ensure that systems are robust, backed-up, and that business continuity arrangements are in place.

4.7 Individuals also have responsibility for availability of information or data, including ensuring that data that needs to be shared is placed where other users have access.

Incident Reporting

4.8 Any loss of integrity or availability should be reported to the relevant system owner.

5. Information Classification and the Assessment of Risk

Information Classification

5.1 Information will be classified as open or restricted. Information may be restricted for a number of reasons. It might be personal information, information provided in confidence, commercially sensitive information, or information that, if shared beyond a particular group of people could pose a regulatory or other risk. Some information will only need to be restricted for a fixed period of time. Some items such as forms or spreadsheets may be only need to become restricted at a certain point when specific types of information are added. Information which is restricted must be labelled and handled accordingly.

Risk Assessment of Information Held

5.2 The degree of security control required depends on the sensitivity or criticality of the restricted information. The first step in determining the appropriate level of security therefore is a process of risk assessment, in order to identify and classify the nature of the information held, the adverse consequences of security breaches and the likelihood of those consequences occurring. Information owners will be supported in assessing the risks associated with the information.

5.3 Risk assessment identifies the University's information assets; defines the ownership of those assets; and classifies them, according to their sensitivity and/or criticality to the department or University as a whole. In assessing risk, consideration is given to the value of the asset, the threats to that asset and its vulnerability.

5.4 Some information assets will be principally owned and used by a specific department or area. Assessment of risk relating to those assets is the responsibility of the relevant department, although guidance on this will be available centrally.

5.5 A register of major information assets will be held and maintained by the Information Assurance Manager.

Personal Data

5.6 Personal data will normally be restricted and must be handled in accordance with the Data Protection Act 1998 (DPA), and, after May 2018, in accordance with the EU General Data Protection Regulations (GDPR) and related UK legislation, and in accordance with the University's policy and guidance on personal data.

5.7 A higher level of security should be provided for sensitive personal data, which is defined in the DPA as data relating to ethnic or racial origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership, or the commission or alleged commission of criminal offences. This higher level will apply also to the special categories of personal data, which is defined in GDPR as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the genetic data, biometric data fused to uniquely identify an individual, data concerning health, sex life or sexual orientation.

6. Protection of Restricted Information

6.1 Identifying restricted information is a matter for assessment in each individual case. Broadly, however, information will be restricted if it is of limited public availability; is confidential in its very nature; has been provided on the understanding that it is confidential; and/or its loss or unauthorised disclosure could have one or more of the following consequences:

a) financial loss, e.g. the withdrawal of a research grant or donation, a fine by a regulatory body, a legal claim for breach of confidence, disclosure of commercially confidential information compromising competitiveness;
b) reputational damage, e.g. adverse publicity, demonstrations, complaints about breaches of privacy; and/or

c) an adverse effect on the safety or well-being of members of the University or those associated with it, e.g. increased threats to staff or students engaged in sensitive research, embarrassment or damage to benefactors, suppliers, staff and students

Storage

6.2 Some areas will be required to implement additional controls such as clear desk policies or data encryption in order to provide adequate protection for personal or restricted data.

6.3 Restricted information should be kept secure, using, where practicable, dedicated systems storage rather than local storage (e.g. a PC hard disk), and an appropriate level of physical security.

6.4 Data encryption should be considered as an additional security layer, where physical security is considered insufficient for electronic information. This is particularly relevant for information stored on or accessed through mobile devices.

Access

6.5 Restricted information must be stored in such a way as to ensure that only those authorised to do so can access it.

6.6 All users must be authenticated. Authentication should be appropriate, and where passwords are used, clearly defined policies should be in place and implemented. Users must follow good security practices in the selection and use of passwords.

6.7 Additional forms of authentication will be considered as appropriate on a risk basis.

6.8 Where needed, access records will be kept as appropriate for each system or operation, or as required by relevant regulation or legislation.

6.9 Users with access to restricted information should be security vetted, as appropriate, in accordance with existing policies.

6.10 Physical access should be monitored, and access records maintained, which could be via audit trails, CCTV, etc as required.

Remote Access

6.11 Where remote access is required, this must be controlled via a well-defined access control arrangements that allow the appropriate level of access.

6.12 Any remote access must be controlled by secure access control protocols using appropriate levels of encryption and authentication.

6.13 Restricted information in hard copy, whether already existing in that form, or printed from electronic sources, should be kept securely at all times if it needs to be removed from University premises

Copying

6.14 The number of copies made of restricted information, whether on portable devices or media or in hard copy, should be the minimum required to meet the purpose, and, where necessary, a record kept of their distribution. In general, providing access to a single version is to be preferred to creation and distribution of copies.

6.15 All copies should be treated with at least the same security considerations as the original. For example using encryption and physical security (e.g. stored in a locked cupboard drawer or filing cabinet). When no longer needed, a copy should be deleted or, in the case of hard copies, securely destroyed.

Disposal

6.16 Policies and procedures for the secure disposal or destruction of restricted information must be followed.

Use of Portable Devices or Media

6.17 This policy covers information and information systems however accessed, including when accessed on mobile devices, regardless of whether those devices are personally owned or issued by or through the University. Adequate protection for mobile devices and the information stored on or accessed through them should be in place, including encryption, where appropriate.

6.18 Use of mobile devices must comply with specific policies for their use as well as with the more general polices on use of IT.

Transfer and Sharing of Information , Including Email

6.19 Human error underlies the majority of inappropriate sharing of information at the University. Before sharing information through whatever channel or medium, individuals should note whether or not the information is restricted. They should ensure that the channel they are using offers an adequate level of protection and that the information is properly directed, by double checking email addresses, mailing labels, fax numbers etc.

6.20 When using email the appropriate guidance on the University's website should be followed. Senders of email should ensure that also recipients, including those on the CC or BCC list, are entitled to have the information shared with them, and that restricted information is not accidentally shared via long email trails.

Encryption

6.21 Guidance and support for encryption, and alternatives to encryption, are provided centrally.

System Planning and Acceptance

6.22 A risk assessment should be carried out as part of the business case for any new information system that may be used to store restricted information. The risk assessment should be reviewed periodically on existing systems. A privacy impact assessment should also be carried out where appropriate.

Resilience

6.23 Information must be handled and stored in such a way that its confidentiality, integrity and availability are safeguarded, that prevents any loss or unauthorised disclosure, and preserves business continuity. Information, and information systems, including hardware, should have appropriate levels of resilience. Information owners should determine, as part of their risk assessments, whether they have any requirement for higher levels of resilience than that which is centrally provided.

Enforcement

6.24 The University has established this policy to promote information security and compliance with relevant legislation and the University's statutory obligations. Any failure to comply with this policy may result in appropriate disciplinary procedures being followed.

6.25 Any loss or unauthorised disclosure of information in any form must be promptly notified. This will normally be to the information owner or to the Information Assurance Manager who will ensure that it is investigated as an information security incident, remedial action is taken promptly, and that it is reported as necessary. This may include reporting to the relevant group or committee, Head of department or section, Registrar and Secretary, Vice-Chancellor and to relevant external authorities.

7. Other Relevant University Policies and Guidance

7.1 Related and supporting policy is published on the University website.

Policy information

Title	Information Security Policy
Version number	2.1 revised draft
Author	Sara Stock, Information Assurance Manager
Owner	Bryn Morris, Registrar and Secretary
Approved by	Council February 2016, minor revision endorsed by ICT SG November 2017
Effective date	October 2016
Date of last review	Reviewed yearly. Last review November 2017. Next review November 2018
Document status	Published
Document classification	Public
Questions and queries	Email infoman@essex.ac.uk
Relevant policies and guidelines	Visit our website at www.essex.ac.uk/it/about/policies-and-guidelines
Comments	Based on Oxford University Policy, October 2015