Information Security Policy

This policy recognises that a core aim of the University is the dissemination of knowledge, and that any policy will fail if it assumes that access to that knowledge must, by default, be denied. Instead, our concern is with ensuring that the steps taken to ensure the integrity of our information and, where necessary and appropriate, its confidentiality, are both proportionate and effective.

1. Introduction

1.1 The aims of this Information Security Policy are to:
   i. protect against the potential consequences of breaches of confidentiality, failures of integrity or interruptions to the availability due to attack of that information.
   ii. ensure that all the University’s information assets and computing and network facilities are protected against damage, loss, misuse or unauthorized access.
   iii. ensure that all users of the University’s computing facilities are aware of and comply with UK and EU legislation which applies to the processing of information.
   iv. increase awareness and understanding across the University of the requirements of information security, and the direct responsibilities of users for protecting the confidentiality and integrity of the data which they handle.

1.2 This document includes a glossary which clarifies (and partly redefines) the meanings of words like “user” and “system owner”. For the avoidance of doubt, when such words are used in this document, it is the meaning described in the glossary that is intended.

1.3 Section 1 to 4 pertains to all users. Section 5 should be read by system owners and system controllers.

1.4 This policy provides overall management direction for information security across the University. ‘Codes of Practice’ (CoPs) have been published for individual key services, by the teams responsible for those services. These CoPs should be considered as part of this policy with references to such services.

1.5 Other CoPs will be developed for new services that come in to use.
1.6 Information and services in the University can be categorised as either open to the public or restricted to a set of people by some mechanism. Therefore this policy also addresses the prevention of unauthorised access.
2. Policy Authorisation and Compliance

2.1 It is the University’s policy that the information it is responsible for shall be appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information and to protect it against damage, loss or misuse.

2.2 This policy has been ratified by the University Court, via the Knowledge Strategy Committee and forms part of its policies and procedures, including its Computing Regulations. It is applicable to all users.

2.3 This policy shall be regularly reviewed to ensure that it remains appropriate.

2.4 A Head of College/Support Group has overall responsibility for ensuring the security of IT services offered by their units.

The responsibility for ensuring the protection of information systems and ensuring that specific IT security processes are carried out shall lie with:

(a) Head of School, or
(b) Head of Support Unit

The Head is responsible for IT systems in any subsidiary unit, for example, associated Institutes, research groups and multi-disciplinary organisations within the line management.

A definitive list can be found at https://www.org.planning.ed.ac.uk/browser/

2.5 Specialist advice on information security shall be made available, throughout the University, from Information Services and drawing on appropriate expertise within the wider University community.

2.6 An information system’s compliance with the information security policy shall be reviewed in line with the assessed security criticality (defined below) of the system independently of the system owner.

2.7 The University's Computing Regulations and other documents (such as the Contract of Employment for staff, and disciplinary codes for students) set out responsibilities of staff and students. This Information Security Policy further clarifies their responsibilities with respect to information security.

2.8 In exceptional circumstances the Chief Information Officer may elect to waive particular clauses of this policy for particular systems after due regard is taken of risks and benefits. A Head of College or Support Group can request with appropriate reasons that security policies be varied in specific cases with the approval of the University CIO.

3. Security Criticality

3.1 For security purposes, the level of criticality depends on the system concerned. Criticality is an assessment of the impact and likelihood of a security failure for a particular system. When assigning a level to criticality, issues that should be
considered include, but are not limited to: inconvenience, distress or damage to personal reputation, financial loss, harm to organisational programmes or reputation, legal violations and personal safety.

3.2 This policy contains requirements across the range of "low", "medium" and "high" criticality systems.

3.3 Individual system controllers should determine the criticality of their system as part of a general risk assessment process. This process should also consider system dependencies - any system upon which the security of a high criticality system depends is also a high criticality system, regardless of its own nature.

4. Information Security for All

4.1 General

4.1.1 All users are to be provided with a summary of the information security policy.

4.2 Information Handling

4.2.1 All users of information systems, including those of servers and personal devices must manage the creation, storage, amendment, copying, archiving and disposal of information in a manner which safeguards and protects its confidentiality, integrity and availability.

4.2.2 Any username and password or any other access credential shall be used in accordance with the appropriate Code of Practice and, where applicable, any requirements of the central authentication service.

4.2.3 All users must ensure they comply with the guidance for users for the appropriate services in relation to physical security.

4.2.4 It is the responsibility of system owners to ensure appropriate compliance guidance for users is provided. This guidance is derived from the relevant Code of Practice. (See 5.1.4)

4.3 Mobile Working, off-site working, and use of unsupported computers

4.3.1 It is recognised that mobile and off-site computing is a normal part of University business. However, this entails additional risk and users must take additional precautions.

4.3.2 Users who work using equipment outside the University and/or remove data from the University must be aware of the additional risks and take appropriate steps to mitigate them. See the policy on the storage, transmission and use of personal data and sensitive business information out with the University computing environment in the regulations and policies part of the Information Security Website. Advice on security for mobile devices can be found at www.ed.ac.uk/is/security

4.3.3 Users of unsupported or personally owned devices should comply with relevant policies published on the Information Security website
4.3.4 When accessing services from unsupported, mobile, or personally owned devices, users should take particular care to ensure they minimise the risk by following all the relevant policies including Mobile Data Security and the Guidelines for the specific service that they are accessing. Advice on remote working can be found on the Information Security website.

4.3.5 Users must take all steps to mitigate the risks associated with 3rd party networks or computer equipment they may use while engaged in mobile or off site working.

5. Information Security for System Owners and System Controllers

5.1 General

5.1.1 The University's information systems shall be managed and run by suitably trained and qualified staff.

5.1.2 All staff involved in managing information systems shall be given access to IT security training, and advice.

5.1.3 It is the responsibility of a system owner whether a central system or a school/college system, potentially in conjunction with a system operator, to produce a risk assessment for their system.

5.1.4 It is the responsibility of the System Owner to ensure that users are provided with appropriate guidance for users to enable them to comply with sections 4.2.2 and 4.2.3.

5.1.5 It is the responsibility of The Head of School or Support Unit to maintain a register of at least their medium and high critical information systems. As a minimum, this register should contain a unique identifier for each information system, a business contact, an assessment of risk from the range "low", "medium" and "high" and an indication if Code of Practice has been produced. A template to assist in constructing a Code of practice can be found in the regulations and policies part of the Information Security Website. Following a request by the Head of School, a Head of College may elect to maintain the register for a specific business area.

5.1.6 Information and guidance for the production and maintenance of Codes of Practice can be found in the regulations and policies part of the Information Security Website.

5.2 Operations

5.2.1 Areas and offices which contain medium/high criticality systems or information shall be given an appropriate level of physical security and access control, including protection from unauthorised access, and, for high criticality systems, protection from environmental hazards and electrical power failures.
5.2.2 The procedures for the operation and administration of all information systems and activities must be documented at a level appropriate for their criticality. These documents should be subject to regular maintenance and internal review.

5.2.3 Duties and areas of responsibility, appropriate to the criticality of the system, shall be segregated to reduce the risk, and consequential impact, of information security incidents.

5.3 System Planning and Development

5.3.1 The information assets associated with any new, or updated, high criticality service must be identified, classified and recorded and maintained within its Code of Practice.

5.3.2 The development, use or modification of all software on the University's critical systems for their complete lifecycle shall be appropriately controlled and a risk assessment performed to protect against the introduction of security risks.

5.3.3 Acceptance criteria for new high criticality information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to migration to operational status. This includes ensuring compliance with the University’s information security policies, access control standards and requirements for ongoing information security management.

5.4 Systems Management

5.4.1 The user account management process must be handled in a secure manner over its lifecycle.

5.4.2 Access controls for all systems shall be set at an appropriate level in accordance with the value of the assets being protected, and the criticality of the system. Access controls shall be regularly reviewed, with any changes in access permissions being authorised by the system owner. A record of permissions granted must be maintained.

5.4.3 Access to all information systems shall use an appropriate access mechanism with security appropriate to the criticality of the system. Access to parts of high criticality systems may be augmented by requiring stronger assurance, further authentication, or controlled by time of day or location of initiating system.

5.4.4 All access to high criticality services is to be logged and appropriately monitored to identify potential misuse of systems or information. Logs must be retained and access granted according to the appropriate legislation.

5.4.5 Formal change control procedures, with audit trails, shall be used for all changes to high criticality systems.

5.4.6 Security event logs, operational audit logs, error logs, transaction and processing reports must be properly reviewed and managed by the system controller.

5.4.7 System clocks must be regularly synchronised across all University high and medium criticality machines.
5.5 Network Management

5.5.1 A register of known externally facing services is used to configure the University network perimeter firewall. This firewall blocks much of the Internet noise and low level vulnerability probing attacks but ingress to the registered services.

5.5.2. Units or Schools maintaining their own sub-network firewall may apply to opt out from protection via the University network perimeter firewall according to 5.4.4 below.

5.5.3. In addition to the perimeter firewall, some network ranges hosting the University’s most critical services, or hosting data services that are not consumable outside that network sub-range are protected by port-blocking or an additional firewall.

5.5.4 Moves, changes and other reconfigurations of firewalls, port blocks and users’ network access points will only be carried out by staff authorised to perform such functions according to defined procedures. Networks, hosted services, and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised intrusion.

5.6 Business Continuity

5.6.1 All business continuity plans must comply with the appropriate sections of the Information Security Policy.

5.7 Outsourcing and Third Party Access

5.7.1 Persons responsible for agreeing contracts will ensure, after a risk assessment, that the contracts being signed are in accord with the content and spirit of the University's information security policies.

5.7.2 The School or Unit 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 or non-disclosure agreement to protect its information assets.

5.7.3 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.

5.7.4 Where personal data, that is, information about living identifiable individuals, are being transferred to any external organisation then the appropriate University policy must be followed. See http://www.ed.ac.uk/schools-departments/records-management-section/data-protection/guidance-policies/transferring-data/overview.

5.8 Incident Reporting
5.8.1 All security incidents must be handled as described in the Information Security Incident Management Policy to be found in the University Information Security Website. This describes how to report security incidents, data protection breaches and suspected security weaknesses in the University’s systems. It also describes the mechanisms in place to monitor and learn from those incidents. Anonymous reporting is allowed where it is in line with University policy.
Glossary/Definitions

<table>
<thead>
<tr>
<th>Computing facilities</th>
<th>Includes central services as provided by UoE Information Services, UoE School or College computers; personally owned computers and peripherals, and all programmable equipment; any associated software and data, including data created by persons other than users, and the networking elements which link computing facilities.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Staff, students and any other person authorized to use computing facilities.</td>
</tr>
<tr>
<td>System</td>
<td>A computer that provides a service, other than simple desktop use, to more than a single person</td>
</tr>
<tr>
<td>System owner</td>
<td>The person (or persons) with overall responsibility for a system and its data as a University asset.</td>
</tr>
<tr>
<td>System controller</td>
<td>The person (or persons) with the responsibility for the day to day operation, control and maintenance of an information system.</td>
</tr>
<tr>
<td>Code of Practice</td>
<td>The codes of practice provide a detailed description as guided by the draft template to describe a systems conformance with this policy..</td>
</tr>
<tr>
<td>Information Systems</td>
<td>Any system which processes the University of Edinburgh’s information assets or any data or information belonging to others that we use or process on their behalf.</td>
</tr>
<tr>
<td>Process</td>
<td>Any action on data including, but not limited to, creation, amendment, deletion, storing and dissemination by any means.</td>
</tr>
<tr>
<td>Information Security Website</td>
<td>The set of relevant support pages with content for all Users, and for System Owners and Controllers found at <a href="http://www.ed.ac.uk/is/security">http://www.ed.ac.uk/is/security</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Policy Version</th>
<th>Author</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 Aug 12</td>
<td>V1.1</td>
<td>BG</td>
<td>General Update</td>
</tr>
<tr>
<td>19 Sep 12</td>
<td>V1.2</td>
<td>BG</td>
<td>Following IT Sec WG</td>
</tr>
<tr>
<td>4 Oct 12</td>
<td>V1.3</td>
<td>BG</td>
<td>Following ITC on 4 Oct</td>
</tr>
<tr>
<td>26 Oct 12</td>
<td>V1.4</td>
<td>BG</td>
<td>Following comments</td>
</tr>
<tr>
<td>16 Nov 12</td>
<td>V1.5</td>
<td>BG</td>
<td>Following CMG, KSC</td>
</tr>
<tr>
<td>16 Jul 14</td>
<td>V2.0</td>
<td>BG</td>
<td>New Version</td>
</tr>
<tr>
<td>2 Sep 14</td>
<td>V2.1</td>
<td>BG</td>
<td>Following IT Sec WG</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QA Date</th>
<th>QA Process</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Dec 2012</td>
<td>ITC, CMG, Court</td>
<td>Final approval by Court</td>
</tr>
<tr>
<td>9 Feb 15</td>
<td>ITC, KSC, Court</td>
<td>Final approval by Court</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Suggested date for Revision of the Policy</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>BG</td>
</tr>
</tbody>
</table>