OCTOBER 31, 2017

THE UNIVERSITY *of* EDINBURGH

INFORMATION SECURITY POLICY

INFORMATION SECURITY DIVISION
UNIVERSITY OF EDINBURGH

1. Purpose and Scope

1.1. The Information Security Policy (the "Policy") sets out the University of Edinburgh's (the "University") approach to information security management. The Policy, and the supporting Information Security Framework set out in section 3 of this Policy (the "Framework"), is in place to support the strategic vision of the University and to facilitate the protection of the University's information and technology services against compromise of its confidentiality, integrity and availability. Whilst doing this, it recognises the ability to discover, develop and share knowledge must be maintained.

1.2. This Policy and the Framework advocates a holistic approach to information security and risk. This is achieved by identifying and assessing information security threats and developing and implementing a combination of people, process and technology controls to mitigate information security risks according to the University's defined level of risk and the desired objectives. This Policy is owned, managed and developed by the Chief Information Security Officer (CISO) on behalf of the University.

1.3. This Policy and the Framework applies to:

- Everyone within the University of Edinburgh who accesses University information assets or technology. This includes users[1], students and alumni.
- Technologies or services used to access or process University information assets.
- Information assets processed in relation to any University function, including by, for, or with, external parties.
- Information assets that are stored by the University or an external service provider on behalf of the University.
- Information that is transferred from and/or to the University for a functional purpose.
- 3rd party, public, civic or other information that the University is storing, curating or using on behalf of another party.
- Internal and/or external processes that are used to process, transfer or store University information.

2. Objectives

2.1. This Policy and the Framework are designed to:

- Promote a holistic approach to information security management.
- Protect the University's information and technology against compromise of confidentiality, integrity (including non-repudiation[2]) and availability.
- Support the University's strategic vision through an approach which effectively balances usability and security.
- Facilitate a 'security aware' culture across the University and promote that Information Security is everyone's responsibility.

[1] Users are defined as all staff, contractors, visitors, consultants and any third parties engaged to support University activity and who have any authorised access to any University information assets.

[2] Non-repudiation implies that in a transaction one party cannot deny having received a transaction nor can the other party deny having initiated it. It is often included within integrity but is expanded here for completeness.

- Protect the University's information assets, and 3rd party data assets being processed or held by the University on behalf of another party, and technology by identifying, managing and mitigating information security threats and risks.
- Define security controls that are effective, sustainable and measurable.
- Assist in the compliance of contractual, legal or regulatory obligations.
- Identify, contain, remediate and investigate information security incidents to maintain and assist in improving the University's information security posture.
- Develop an informed approach, with regard to information security, in their daily activities across all areas of the University, including teaching, research, support staff and students.
- Ensure the University is compliant with its information security obligations – especially those related to the hosting, curation or processing of 3rd party data.
- Provide assurance to other parties that we have a robust control environment in place to protect their data through an effective information security management system.

3. Framework

3.1. The University's information security is managed through the below Framework which comprises: (i) this Policy, (ii) Standards and (iii) Procedures, alongside supporting Governance processes. This Framework provides a flexible and effective platform upon which the University's information security objectives are met. The Framework is detailed below:

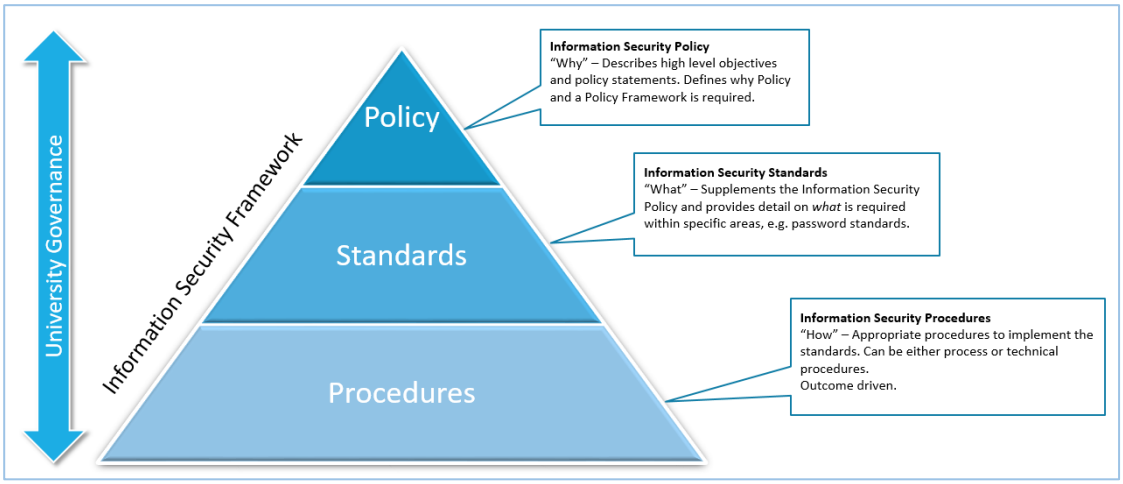

Figure 1 Information Security Framework

3.2. This Policy can be met by adopting and complying with the associated Standards. However, the Framework is designed to be flexible and allow a range of methods to meet this Policy. It enables local autonomy in how the outcomes and objectives of this Policy are met, by allowing local procedural methods and/or controls to be implemented. At the same time, it allows those who require further advice from the Information Security Division to meet this Policy through the methods detailed in the Procedures. Regardless of the approach, all within scope of the Policy are required to meet this Policy and the Standards using appropriate methods.

3.3. It is important to note that the Standards, as outlined in the associated documentation, must be considered the minimum requirements for information security (or the 'baseline'). Where additional information security controls are required for research, legal, regulatory or governance purposes, the controls must be enhanced accordingly. The Information Security Division can provide advice on how to comply with additional security requirements, where required.

4. Policy Statement

4.1. The University manages and produces information that is private, confidential or sensitive in nature, together with information that is regarded as being readily available for general sharing. The University recognises that it is imperative that all information is protected from compromise of confidentiality, integrity and availability. All within the scope of the Policy must therefore ensure that:

i. Information assets are identified, classified and protected in accordance with the associated documentation and Standards (listed below). Any security controls which are implemented must be proportionate to the defined classification. Key information assets are governed by an appointed Data Steward in accordance with the key responsibilities defined in 'The Data Steward role' document.
   - Associated documents and Standards: Information Classification Standard, Data Protection Policy, The Data Steward role.

ii. All processes, technology, services and facilities are protected through information security controls as detailed in the associated Standards.
   - Associated Standards: Access Management Standard, Operational Security Standard, Asset Management Standard, Secure Configuration Standard, Security Testing Standard, Physical Security Standard, Human Resource Security Standard.

iii. Information security incidents are identified, contained, remediated, investigated and reported in accordance with the Incident Management Standard.
   - Associated Standards: Incident Management Standard.

iv. Where a third party provider is utilised for any services which involves contact with University information, an information security risk assessment is carried out to ensure they comply with the appropriate University's Information Security Policy and Standards.
   - Associated Standards: Third Party Standard, Cloud Security Standard.

v. Where appropriate, a risk assessment is carried out on all processes, technology, services and facilities in accordance with the associated Standard to manage risk within appetite.
   - Associated Standards: Risk Management Standard.

vi. Back-up and disaster recovery plans, processes and technology, are in place in accordance with the Business Continuity Standard to mitigate risk of loss or destruction of information and/or services and to ensure that processes are in place to maintain availability of data and services.
   - Associated Standards: Business Continuity Standard.

vii. Where off-site working takes place, appropriate security controls are implemented in accordance with the associated Standards.
   - Associated Standards: Mobile Device Standard, BYOD Standard, Travelling Overseas Standard, Policy on the Storage, Transmission and Use of Personal Data and University Information Outside the University.

In addition, all individuals within scope of the Policy must:

viii. Complete the Information Security Awareness Training.

ix. Ensure that reasonable effort is made to protect the University's information and technology from accidental or unauthorised disclosure, modification or destruction.

4.2. The table in Appendix 1 details the Policy statements and their associated Standards.

5. Compliance/review

5.1. This Policy and the Framework are reviewed on a periodic basis by the Information Security Division to ensure they remain accurate, relevant and fit for purpose.

5.2. The Information Security Division may carry out periodic compliance and assurance activities (e.g. assessment of security controls) to ensure they are aligned with this Policy and the Framework.

5.3. Failure to meet requirements detailed within this Policy and the Framework may result in the user being subject to formal disciplinary action that will be dealt with under the appropriate disciplinary code or procedures. Additionally, where it is suspected that an offence has occurred under UK or Scots law, it may also be reported to the police or other appropriate authority. The rules applicable to investigating breaches or suspected breaches are detailed in the University Computing Regulations.

6. Responsibilities

6.1. The Head of College or Support Group is accountable for ensuring adequate and effective information security controls are in place within their area of responsibility. They are also accountable for compliance in any subsidiary unit, for example, associated Institutes, research groups and multi-disciplinary organisations within their management.

In addition, the following have information security responsibilities:

6.2. *Senior Management and associated Governance committees*

Senior Management[3] have executive responsibility for information security within the University. They must actively support the adoption and implementation of the information security requirements, Policy and Framework as well as ensuring compliance within their areas of responsibility.

This Policy is reviewed and approved by Senior Management through the Governance route of Information Technology Committee (ITC), Knowledge Strategy Committee (KSC) and Central Management Group (CMG).

6.3. *Data Steward*

The Data Steward is responsible for maintaining the security of their dataset; setting access requirements for the data; documenting the data made available to other services, and establishing processes to ensure the quality of the data. They have a duty to ensure that restricted and confidential data is managed securely and appropriately, that the data is made available only to those people and systems that need access, and that access is provided in keeping with legislation and the University's internal policies. If the data includes any personal data, they are also responsible for completing a Data Protection Impact Assessment.

The Data Stewards responsibilities are further defined in 'The Data Steward role'.

[3] Senior Management is defined as Heads of School and Senior Management teams of Support Groups.

6.4. *Users*

Users[1] are responsible for protecting the University's information and technology systems and for complying with the University Computing Regulations, this Policy and the Framework. If a user suspects or discovers any material breach of the requirements detailed within this Policy, they must report this in line with the Incident Management Standard.

Where an individual user suspects personal data may have been compromised, they must notify the Data Protection Officer (DPO) through the method detailed within the Incident Management Standard.

6.5. *Students*

Students must accept that they carry responsibility when utilising the University's facilities, technologies or services and will take all reasonable steps to protect the University's information and technology systems. Students will comply with the University Computing Regulations, this Policy and the Framework, where required.

6.6. *Alumni*

Alumni are expected to comply with the requirements of this Policy and Framework. Failure to do so may result in the withdrawal of access to University information assets and technology.

Version Control and Approval

Version	Date	Author / Editor	Version / Revision Comments
0.1	20/03/17	David McClelland	Document creation and draft
0.2	27/03/17	David McClelland	Document updates following feedback
0.3	12/04/17	David McClelland	Document updates following feedback
0.3	28/04/17	Alistair Fenemore	Review
0.4	02/05/17	David McClelland	Document updates following review
0.5	04/05/17	David McClelland	Document updates following InfoSec review
0.6	09/05/17	David McClelland	Document updates following Knowledge Management & Planning feedback
0.7	09/06/2017	David McClelland	Document updates following ISWG, HR and Legal Services feedback.
0.8	24/07/2017	David McClelland	Document updates following Senior Management, Union feedback. Inclusion of glossary.
0.9	08/09/2017	David McClelland	Document updates following feedback from CIO.
1.0	31/10/2017	David McClelland	Final version following approval from KSC and CMG.

Approval

Version	Date	Authority	Approval Comments
0.9	14/09/17	ITC	-
0.9	13/10/17	KSC	-
0.9	31/10/17	CMG	-

Review / Approval list

#	Name	Role	Comments	Review / Approval
1	Alistair Fenemore	CISO		Creator, Reviewer
2	Information Security Working Group	-	Consists of representatives from all Colleges and Support Groups.	Reviewer
3	University Human Resource Services	-		Reviewer
4	Trade Unions	-	Consulted with Joint Unions Liaison Committee (JULC) and Combined Joint Consultative Negotiative Committee (CJCNC).	Reviewer
5	Information Technology Committee (ITC)	-		Reviewer
6	Knowledge Strategy Committee	-		Reviewer
7	Central Management Group	-		Reviewer, Approver

Appendix 1 – Policy Statement and associated Standards

		Standards and assoicated documentation																
		S.1. Information Classification Standard	S.2. Data Protection Policy	S.3. The Data Steward role	S.4. Access Management Standard	S.5. Operational Security Standard	S.6. Asset Management Standard	S.7. Secure Configuration Standard	S.8. Security Testing Standard	S.9. Physical Security Standard	S.10. Incident Management Standard	S.11. Third Party Standard	S.12. Cloud Standard	S.13. Risk Management Standard	S.14. Business Continuity Standard	S.15. Mobile Device Standard	S.16. BYOD Standard	S.17. HR Security Standard
Policy Statement	i. Information assets are identified, classified and protected in accordance with the associated documentation and Standards. Any security controls which are implemented must be proportionate to the defined classification. Key information assets are governed by an appointed Data Steward in accordance with the key responsibilities in the associated documentation.	x	x	x														
	ii. All processes, technology, services and facilities are protected through information security controls as detailed in the associated Standards.				x	x	x	x	x	x	x							x
	iii. Information security incidents are identified, contained, remediated, and reported in accordance with the Incident Management Standard.										x							
	iv. Where a third party provider is utilised for any services which involves contact with University information, an information security risk assessment is carried out to ensure they comply with the appropriate University's Information Security Policy and Standards.											x	x					
	v. Where appropriate, risk assessment is carried out on all processes, technology, services and facilities in accordance with the associated Standard to manage risk within appetite.													x				
	vi. Back-up and disaster recovery plans, processes and technology, are in place in accordance with the Business Continuity Standard to mitigate risk of loss or destruction of information and/or services.														x			
	vii. Where off-site working takes place, appropriate security controls are implemented in accordance with the associated Standards.															x	x	

Table 1 Policy Statement and associated Standards

Appendix 2 – Glossary

Term	Definition
Confidentiality	Information is not made available or disclosed to unauthorised individuals, entities or processes.
Integrity	Information's accuracy, validity and completeness is protected.
Availability	Information is accessible and usable upon demand by an authorised entity.
Threat	A threat is anything that is capable, by its action or inaction, of causing harm, either directly or indirectly, to a University information asset. A threat exploits a vulnerability to cause impact to a University information asset.
Control	Means of protecting the confidentiality, integrity and/or availability of University information, including policies, standards, procedures, processes or practices, which can be of administrative, technical, management or legal nature. Controls can be detective, preventative or reactive.
Information asset	A body of information that can be understood, developed or shared and has value to the University.
External	Anything which is not owned, managed, employed or provided by the University.
Internal	Anything which is owned, managed, employed or provided by the University.
Information security management	A systematic approach to managing information within a predefined acceptable range so that it remains secure. It includes people, processes and technology by applying a risk management process.
Risk	The chance or possibility of uncertainty on objectives, expressed as a combination the probability of an event occurring and the impact such an event would have on the achievement of one or more objectives.
Contractual obligation	Requirements set by the University when entering a contract with another party.
Legal obligation	Legal requirements, e.g. Data Protection Act 1998 or General Data Protection Regulation (GDPR), Computer Misuse Act 1990.
Regulatory obligation	Requirements set out by a Regulator, e.g. UK ICO, NHS, etc.
Information Security Incident	An event or series of events that compromises the confidentiality, integrity or availability of University information.
Risk assessment	Structured process for examining information security threats, vulnerabilities and impacts relating to a given system or situation to determine whether an individual control is required or operating as expected.
Risk management	The process of identifying and managing information security risks. Once identified risk are treated by mitigating them, accepting them, transferring them or stopping the process with which they are associated.