Information Security Policy

Originator name:	David Sharkey, COO and Chair of Information Security and Governance Group (ISAGG)
Section / Dept:	N/A
Implementation date:	11 February 2014
Date of next review:	31 December 2017
Related policies:	See Information Security Policy Framework
Policy history:	

Version History

Version	Author	Revisions Made	Date
0.1	James Newby	First Draft	8/10/2013
0.2	James Newby	Second draft	22/10/2013
0.3	James Newby	Third draft – EB feedback	11/02/2014
0.4	James Newby	Annual review (2016) inclusion of mandatory training and other minor revisions	10/10/2016

Approval History

Equality Analysis

Version	Reviewed by	Comments	Date
1	Equality & Diversity Staff Member's Name	No negative equality impact identified	29/09/2014

Committee Sign Off

Version	Committee Name	Date of Sign Off
1	Executive Board Committee (or other)	11/02/2014

1	**Introduction**
	The University's information is an important asset. It must be protected from the consequences of breaches of confidentiality, failures of data integrity and interruptions to its availability. The University must therefore take appropriate organisational and technical measures to protect its information.
1.1	**Purpose**
1.1.1	This policy provides the management direction to ensure that information security is considered appropriately and embedded into all University processes and systems and that individual responsibilities for achieving adequate levels of information security are established. The policy aims to minimise potential damage to the University by reducing the number and impact of information security incidents. The measures set out in this policy, including training requirements, are mandatory.
1.2	**Scope**
1.2.1	The policy provides a high level overview of the definitions, management responsibilities and principles of good information security practice. It therefore focuses on the high level measures required to achieve adequate information security. More detailed organisational and technical requirements will be set out in subordinate policies designed to deal with specific aspects of information security. Detailed procedures for complying with the provisions of this policy are therefore not included but will be covered by the subordinate policies included in the Information Security Policy Framework.
1.3	**Equality Analysis**
1.3.1	The University is strongly committed to equality of opportunity and the promotion of diversity for the benefit of all members of the University community. The University's approach is to promote equality across the full range of its activities, in employment, teaching and learning and as a partner working with and within local, national and international communities. Equality Analysis is a process which examines how the impact of the policy has been considered on the diverse characteristics and needs of everyone it affects. This policy has been reviewed and no negative impact on equality has been identified.
1.4	**Definitions**
1.4.1	**Information security**: the preservation of confidentiality, integrity and availability of information. **Information**: data which has meaning. **Information asset**: all data with meaning that can be exploited to advance the University's objectives or confer competitive advantage. **System owner**: Head of department or Faculty with prime responsibility for managing and maintaining an information system, database or network; this includes the day to day operation of that system.
1.5	**Legislative context**
1.5.1	The following legislation is, or may be, relevant to information security: Data Protection Act, 1998 Computer Misuse Act 1990 Copyright, Designs and Patents Act, 1988
1.6	**Health & Safety Implications**
1.6.1	This policy is unlikely to have direct Health & Safety implications. For further information, please see the University Health & Safety policy.

2	**Policy**
2.1	**Principles**
2.1.1	All information for which the University is responsible shall be appropriately secured to protect against the consequences of breaches of confidentiality, failures in data integrity or interruptions to availability and to protect it against damage, loss or misuse. Consistent with this principle: • All staff shall follow University policies and system instructions to ensure that no breaches of information security result from their actions • All staff shall retain data in accordance with the Data Protection policy and the provisions of the Records Management Strategy. Particular consideration should be given to the classification of data (confidential, restricted or unrestricted) and the consequent access granted to colleagues, students or third parties. • IT Services shall provide appropriate technical measures to ensure digital data is backed up and guidance for staff to ensure the measures are effective. • The University shall provide adequate Information Security training and guidance for all staff appropriate to the information security risks involved in their roles. This training is mandatory. • The University shall provide adequate data retention capacity and technical security measures to enable staff to comply with the published data retention schedules and other system specific information security requirements. • CSAS department heads and Faculty Managers shall ensure that adequate departmental business continuity arrangements are in place in their departments to prevent failures of compliance, operational disruption or reputational damage following an information security incident. • CSAS department heads and Faculty Managers shall ensure that all equipment capable of storing or transmitting data is held securely and that the risk of theft or misuse is minimised. • The University shall ensure that its systems, networks, databases and third party arrangements are designed and installed with appropriate measures implemented to prevent information security breaches. • The University shall prepare, test, publish and occasionally review protocols for responding to suspected information security breaches.
2.2	**Procedures**
2.2.1	Detailed procedures for achieving appropriate standards of information security are included in the subordinate policies making up the Information Security Policy Framework. See supporting documentation for more details.
3	**Governance Requirements**
3.1	**Responsibility**
3.1.1	Overall responsibility for the University's strategic plans for information security rests with the Executive Board member serving as the Chair of the Information Security and Governance Group (ISAGG). The ISAGG will supervise the development of an appropriate policy framework and suitable operational procedures to comply with all the principles detailed in section 2.1. Detailed responsibilities for delivering each aspect of the information security principles outlined in section 2.1 will be incorporated into the various related policies and procedures making up the Information Security Policy Framework. The following responsibilities for information security principles apply:

	• The Chief Information Officer is responsible for ensuring that the arrangements for governing the scoping, development, implementation and maintenance of University IT systems, networks and databases comply with the principles of good information security. • System owners are responsible for ensuring that IT systems they manage are configured appropriately and used effectively to ensure that the risks of an information security incident are minimised. These owners are assumed to be responsible for the organisational and technical measures necessary to ensure that good information security practice is built into their system's day to day operation. • All staff who are users of information systems must manage the creation, storage, amendment, copying, archiving and disposal of information in a manner which safeguards and protects its confidentiality, integrity and availability. This includes engaging with University provided information security training.
3.2	**Implementation / Communication Plan**
3.2.1	As this policy sets out overarching responsibilities, definitions and principles of the University's approach to information security, its implementation will be limited to awareness raising via the Leaders' Alert communication channel and publication on SurreyNet. The related policy framework and detailed subordinate policies will be implemented via a range of methods to be determined separately. (see Information Security Policy Framework)
3.3	**Exceptions to this Policy**
3.3.1	The principles of information security are underpinned by legislation and the consequences of a serious breach of information security are severe. Therefore exceptions to the principles outlined in this policy are not expected to be allowed. In highly exceptional cases, and with a very high level of justification, any request to relax the normal information security requirements must be authorised in writing by the Chair of the Information Security Steering Group.
3.4	**Supporting documentation**
3.4.1	Information Security Policy Framework Terms of Reference: Information Security and Governance Group

University of Surrey Information Security Policy Framework

1st tier: Determine principles, definitions and responsibilities relating to information security:

Purpose	Content covered	Required documents	Owner	Comments/next steps
Information security policy	Top level document defining responsibilities and refers to more detailed issue specific policies	Single concise policy	DS as Chair of Information Security Steering Group	Policy approved by EB (Jan14). Dissemination by Leaders' Alert due in Feb 14

2nd Tier: Determine principles for developing our systems, processes and people:

Purpose	Content to be covered	Required documents	Owner	Link to Risk Reg	Comments/next steps
Business continuity planning	Policies and processes for assessing and addressing risks to BC.	Policies, risk assessments and departmental plans	Estates & Facilities	3.2	IT disaster recovery plans reviewed by Internal Audit. BCP Plans updated periodically. Protocol for responding to data breaches in place and tested.
System design and planning	Statement of principles determining how information security requirements are incorporated into new project scopes and requirements. Generic guidance on how to assess IS risks in proposed new systems	Statement of system design principles to be applicable to all systems for inclusion in standard project initiation documentation. New patching policy to outline risk based approach to patching.	ITS	8.1 – 8.3 (ensuring secure configuration of systems)	Patching policy to be approved by April 14 Design principle statement by April 14
User and access management	Generic principles for setting the rules of access and for managing individual user accounts. Needs to set out principles for determining when/how accounts are cancelled and/or withdrawn.	New access policy. Will include (or be updated) with rules for privileged account access when management solution is implemented (Apr 14)	ITS	5.1 – 5.4 (managing user privileges) 4.4 (information risk management regime)	Access policy - April 14 (RS)
Network management	Statement of principles for ensuring consideration of information security implications arising from the connection of all new and existing systems to central networks (and each other)	Incorporation into standard project initiation documentation or statement of principles likely to be applicable to all new and proposed systems. EG approach and frequency of internal and external vulnerability scans	ITS	8.3 (systems config) 10.1 – 10.4 (network security)	
Data Protection	Policy covering definitions and responsibilities for meeting the 8 data protection principles and for responding to complaints, subject access requests and breaches.	Data Protection Policy approved by EB Guidance for managing subject access requests. Process/protocol for responding to a suspected data breach	BSS/Legal Counsel	Various	Policy in place since 2009. Full guidance published on BSS website
Personnel	Outlines minimum training requirements for induction and on-going training. Includes responsibilities at individual level for information security.	Individual responsibilities can be included as standard clause in JPs. Training to be included in new staff induction programme	HR	2.1 – 2.4 (user education & awareness)	Information security and data protection now included in standard induction package. HR will update standard JPs to include generic information security responsibilities

3rd Tier: Determine rules for using our systems and equipment and for exploiting and sharing our data:

Purpose	Content covered	Required documents	Owner	Link to Risk Reg	Comments
Information handling	Definition of classes of information and the handling, labelling, storage, transmission, processing and disposal requirements. Should include back up requirements, integrity requirements (validation processes).	Records management data retention schedules and publication schemes. Data Protection risk assessments. Most aspects of data management will be covered by projects in ITS and BSS to implement new data storage capacity and management systems	BSS/ITS		Confidential data classified for incident response purposes in response protocol. Records retention schedules for corporate data in place in all admin departments. New ICO model publication scheme will be implemented gradually during 2014
Use of computers	Document setting out responsibilities and behaviours required of all staff and students using University computing equipment	Acceptable Use Policy	Legal Counsel	2.1 Acceptable use policy	Policy in place and widely used. To be updated with new Information Security requirements by April 14
Mobile computing	Rules governing the use by staff (and students) of mobile devices with access to user accounts and University networks.	Mobile device policy to be published to incorporate new "good for enterprise" solution.	ITS Procurement	1.2 (Home/mobile working) 8.4 (Secure configuration)	Solution due by April 14 Policy to be published by June 14
Teleworking (home-working)	Document setting out systems measures to take and individual behaviours required during home-working.	Homeworking policy to include requirements for access to networks.	HR to lead.	1.2 – 1.3	May be incorporated into mobile device policy.
Cryptography	Document setting out rules and procedures for encryption and encryption requirements for any device connecting to University networks	Encryption policy	ITS	1.3	ITS currently developing standard laptop encryption and policy will be drafted to align with technical solution. Due April 14
Social Media policy	Rules for contributing to and management of, University hosted social media sites.	Social media policy	Comms and PR		Draft out for consultation – Feb 14

Version history

Version	Author	Revisions made	Date
1	JN	First draft – following sub group work	Oct 13
2	JN	Changes following ISSG feedback	Nov 13
3	JN	Changes following EB feedback	Feb 14