UNIVERSITY OF SUSSEX

IT Services

INFORMATION SECURITY POLICY

1. OVERVIEW AND PURPOSE

1.1. The University of Sussex's information technology services underpin all of the University's activities and are essential to the University's objectives to advance learning and knowledge through teaching and research to the benefit of the wider community.

1.2. The University recognises the need for its staff, students, associates and visitors to have access to the information and/or information technology services they require in order to carry out their work and study and recognises the role of information security in enabling this.

1.3. The University also recognises the information it manages must be appropriately secured in order to protect the institution and its stakeholders from consequences of breaches of confidentiality, failures of integrity or interruption to availability of information, and to maintain its reputation for trustworthiness.

1.4. Security of information must be an integral part of the University's management structure in order to maintain business continuity, legal compliance and adherence to the University's own regulations and policies, including the Regulations for the Use of Information Technology.

1.5 The University is committed to maintaining a safe, welcoming and inclusive environment. Encouraging debate and discussion, and upholding freedom of speech is to be balanced with our legal obligations. The Counter-Terrorism and Security Act 2015 places an obligation on the University 'in the exercise of its functions, have due regard to the need to prevent people from being drawn into terrorism'. This is known as the Prevent duty. Further details can be found on our website.

1.5. **Objectives**

1.5.1. To define the framework within which information security will be managed across the University.

1.5.2. To demonstrate management direction and support for information security throughout the University.

1.5.3. To facilitate a 'security aware' culture across the University and promote information security as everyone's responsibility.

1.6. **Principles**

1.6.1. Security controls must be put in place to ensure that confidentiality, integrity and availability of information is assured. Controls should be commensurate with risk but must always adhere to minimum standards set by University policies and legal/regulatory standards. Security controls must be maintained when information is taken off-site, accessed from off-site or accessed using mobile technologies.

1.6.2. Information must be processed in accordance with the Data Protection Policy and the Records Management Policy. Consideration should be given to classifications assigned to

information (see Information Classification and Handling Policy) and the consequent access granted to staff, students and associates of the University and third parties.

1.6.3. Transfers of information to third parties must be made adhering to relevant policies and must be authorised at an appropriate level. A data sharing agreement must be in place unless the data transfer is defined and constrained in a contract. Minimum agreed levels of security controls must be maintained. Transfer to third parties includes use of cloud or third party hosted services by individual users.

1.6.4. The University shall ensure its information technology services and third-party arrangements are designed and configured with sufficient and appropriate measures implemented to minimise the risk of information security breaches.

1.6.5. All incidents involving actual or potential breaches of information security must be reported and managed in accordance with the Information Security Incident Reporting Process. The University will investigate all security incidents and take appropriate action in accordance with this policy, University Regulations, and English Law.

1.6.6. All information security measures, and policies defining them, will be regularly reviewed and tested, including use of annual internal audits and penetration testing.

2. SCOPE

2.1. This policy applies to all use of University information technology services including software, computers and/or networks, whether on-campus, via remote connections or in cloud services.

2.2. Use of devices not owned or supplied by the University is also covered if connecting in any way to University provided information technology services.

2.3. This policy applies to all users of University provided information technology services including staff, students, associates and visitors of the University.

2.4. This policy applies at all times.

3. RESPONSIBILITIES

3.1 The Council of the University

3.1.1. Ensuring appropriate technical and organisational measures are in place to safeguard its processing of personal data and other information.

3.1.2. Ensuring compliance with all legislative and regulatory requirements relating to data protection and information security.

3.2 Information Governance Committee (IGC)

The IGC supports and drives the broader information security and governance agenda for the University. It acts as advocate to provide assurance to the University Executive Group (UEG)

and the Audit and Risk Committee (ARC) that effective best practice mechanisms are in place across the University.

3.2.1. Regularly reviewing, approving and renewing the Information Security and subsidiary policies.

3.2.2. Reviewing information security risk status, agreeing mitigations as necessary.

3.2.3. Monitoring performance against agreed information security key performance indicators based on agreed metrics.

3.2.4. Reviewing the operational status of information security, data protection, cybersecurity, automation and control systems, physical security, business continuity, information risk management and records management.

3.2.5. Reviewing the status of high priority information security, data protection and cyber security incidents.

3.2.6. Ensuring regular, independent audits of implementation of the Information Security policy are undertaken, and appropriate actions are taken to correct any deficiencies found.

3.2.7. Ensuring organisational training to support information security requirements is identified and implemented.

3.3. Senior Information Risk Officer

The Senior Information Risk Owner (SIRO) is a University Leadership Team (ULT) member who is familiar with information risks and provides focus for the management of information risk at that level.

3.3.1. Driving a culture valuing, protecting and using information for University success and for the benefit of its staff and students.

3.3.2. Owning the University's information risk and incident management framework; ensuring information risks and incidents are appropriately managed.

3.3.3. Owning the overall information risk policy and risk assessment processes and ensuring consistent implementation by Information Asset Owners.

3.3.4. Ensuring information risk is further mitigated through suitable organisational awareness of, and training in, the Information Security and subsidiary policies.

3.3.5. Providing status updates to Information Governance Committee on high priority information risks to the University.

3.4. Director of IT Services

The Director of IT Services is responsible for overall technology security measures protecting the University, including proactive defence, monitoring and incident response.

3.4.1. Proposing required changes to the Information Security and subsidiary policies to the Information Governance Committee for approval.

3.4.2. Overall implementation management of the Information Security and subsidiary policies.

3.4.3. Ensuring information technology services used by the University are procured, designed, implemented and maintained in such a way as to support the Information Security policy.

3.4.4. Ensuring that IT-related training is delivered, and advice is available as required on information security matters.

3.4.5. Investigating any reported information security incidents or risks and responding appropriately.

3.4.6. Authorising access to personal or restricted information for specific operational reasons.

3.4.7. Undertaking risk assessments of information technology services to determine the probability and impact of security failures and recommending appropriate mitigation.

3.5. Data Protection Officer (DPO)

The DPO assists in the monitoring of internal compliance with data protection regulations, informs and advises on data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the supervisory authority.

3.5.1. Authorising legal access to users' personal data to investigate suspected breaches of University regulations or the law.

3.5.2. Providing advice and guidance to ensure personal and special category data is always handled and processed correctly.

3.5.3. Monitoring any personal data breaches and, where appropriate, passing notice of data breaches to the supervisory authority – Information Commissioners Office (ICO).

3.6. University Officers, Heads of Schools, Directors of Professional Services Divisions

3.6.1. Ensuring all information in their area is managed in conformance with this policy.

3.6.2. Familiarising themselves with risk assessments for information technology services used within their area of responsibility and ensuring relevant mitigation measures are implemented as appropriate.

3.6.3. Ensuring all staff, students, associates and visitors who make use of University information technology services are made fully aware of the Information Security and subsidiary policies and are given appropriate support and resources to comply with these.

3.7. **Staff, Students and other users of the University's information technology services / information**

3.7.1. Complying with the Information Security and subsidiary policies.

3.7.2. Completing any information security training as required by the University.

3.7.3. Reporting any personal data breach immediately to the Data Protection Officer.

3.7.4. Reporting any information security incidents or risks to the IT Service desk immediately.

4. POLICY

4.1 Definitions:

4.1.1. *Staff:* Any person employed directly by the University

4.1.2. *Student:* Any person enrolled on a course or module of study at the University, including open courses, summer schools as well as mainstream undergraduate and postgraduates (taught and research).

4.1.3. *Associate:* Any person who is not staff or a student of the University who requires a University information technology services username as part of their relationship with the University. Includes contractors, some third-party organisation staff, interns, agency staff, researchers, external examiners, visiting academics etc.

4.1.4. *Visitor*: Any person visiting the University campus

4.2. It is the policy of the University that information it manages shall be appropriately secured to protect the University and its stakeholders from the consequences of breaches of confidentiality, failures of integrity or interruption to the availability of information, while allowing staff, students, associates and visitors of the University to have access to the information and/or information technology services they require in order to carry out their studies or work. These facets are defined thus: information and/or information technology services they require in order to carry out their studies or work. These facets are defined thus:

4.2.1. Confidentiality – non-public information is only available to authorised users

4.2.2. Integrity - information is complete, accurate and fit for purpose

4.2.3. Availability - information is available when and where it is needed

4.3. This will be achieved by an appropriate mix of policies, standards, guidelines, technical measures, training, support, audit and review.

4.4. This policy is the primary policy under which all other technical and information security related polices reside. This document, together with subsidiary policies and guidance comprise the University's Information Security Policy.

5. BREACH OF THIS POLICY

5.1 Where there is a deliberate misconduct or behaviour amounting to wilful breach of this Policy, or gross negligence causing a breach of the Policy, the matter may be considered under the University's Disciplinary Procedure under Regulation 31.

University policy is that criminal activity will be referred to the Police.

Review / Contacts / References	
Policy title:	Information Security Policy
Date approved:	20 October 2020
Approving body:	Information Governance Committee
Last review date:	20 June 2019
Revision history:	5.0
Next review date:	October 2021
Related internal policies, procedures, guidance:	Information Security Policies Regulations for the Use of Information Technology Guidance Notes on the Regulations for the Use of Information Technology (Acceptable Use) ITS Top 10 Security Tips Payment Card Industry Data Security Standard Policy Data Protection Policy and Guidance Records Management Policy and Guidance Regulations of the University Breach Reporting process Information Classification and Handling Policy University information on counter-terrorism safeguards (Prevent)
Policy owner:	IT Services
Lead contact / author:	Pete Collier, Assistant Director, Strategy and Architecture