UNIVERSITY OF SUSSEX

IT Services

INFORMATION SECURITY POLICY

1. OVERVIEW AND PURPOSE

1.1 The University of Sussex's Information Technology Services (ITS) underpin all of the University's activities and are essential to the University's primary purpose, i.e. to advance learning and knowledge through teaching and research for the benefit of the wider community.

1.2 It is crucial that University staff, students, and others working with the University have access to the information[1] and/or technology they require in order to carry out their work and study.

1.3 The University also acknowledges that the information it holds and processes, and systems and devices used to carry out work and study, must be appropriately secured in order to meet relevant legal and compliance obligations, and to protect the reputation and integrity of the institution.

1.4 As such, appropriate and necessary information security[2] measures must be in place and their effectiveness must be monitored accordingly, in order to maintain business continuity and ensure compliance, and to enable adherence to other relevant policies and procedures.

1.5 The aim of this policy is to define the principles and framework in place to manage and implement information security across the institution, to lay out responsibilities in relation to information security at all levels within the University, and promote a 'security aware' culture.

2. SCOPE

2.1 This policy applies to all users of University information and University Information Technology Services[3] including software, computers and/or networks, whether on-campus, via remote connections or in cloud services.

2.2 For the purposes of this policy, 'all users' includes the following, whether remunerated or not:

- Students (any person enrolled on a course or module of study at the University, including open courses and summer schools, as well as mainstream undergraduates and postgraduates, taught and research);

[1] 'Information' refers to information and data processed by the University

[2] Preservation of confidentiality, integrity and availability of information

[3] 'University information and Information Technology Services' refers to any digital information or service provided or procured by the University and accessible through the University networks or over the Internet

- Senior managers, officers, and directors;
- Employees (whether permanent, fixed-term, temporary, or casual);
- Contract, seconded, and agency staff;
- Volunteers, apprentices, and interns; and
- Others associated with (i.e. performing services for or on behalf of) the University (for example, agents and consultants).

2.3 Use of devices not owned or supplied by the University are also covered when connecting in any way to University-provided Information Technology Services.

2.4 This policy underpins the University's suite of other technical and information security-related policies; these documents and additional guidance linked at the end of this policy should all be considered in conjunction with this policy.

3. RESPONSIBILITIES

3.1 All Users

3.1.1 All users (as defined in section 2.2 of this policy) are responsible for complying with this policy as well as all other related policies and guidance and for completing any compulsory information security training provided by the University.

3.1.2 All users are also responsible for reporting any information security-related risks and issues they become aware of via the appropriate route(s), as outlined in this policy and/or other related policies.

3.2 University Leadership Team (ULT)

3.2.1 ULT members are accountable for driving a culture that values, protects, and uses information for University success and for the benefit of its staff and students, and for ensuring that their area of responsibility complies accordingly with this policy and other related policies.

3.3 Senior Information Risk Owner (SIRO)

3.3.1 The SIRO is a ULT member who is familiar with the strategic objectives of the University and understands how these objectives may be impacted by information security risks, helping to determine and implement the most appropriate risk mitigation accordingly.

3.4 Chief Digital Transformation Officer (CDTO)

3.4.1 The CDTO has overarching accountability for performance, security, and availability of technology services provided across the University and the strategic leadership of

Sussex Projects, the University's Portfolio, Programme and Project Management team.

3.4.2 The CTDO delegates day to day responsibility for the multiple facets of this information security and related matters to the IT Leadership team (i.e. Deputy and Assistant Directors within ITS).

3.5 IT Leadership Team

3.5.1 The IT Leadership team is responsible for ensuring – via management of appropriately skilled technical teams – that appropriate technical security controls are in place throughout the institution, for implementation and monitoring of information security-related policies, and for advising the institution on information security-related matters.

3.6 Director of Estates, Facilities and Commercial Services

3.6.1 The Director of Estates, Facilities and Commercial Services has responsibility for physical and environmental security measures across the University campus.

3.7 Data Protection Officer (DPO)

3.7.1 The DPO assists in the monitoring of internal compliance with data protection requirements, 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 relevant supervisory authority, the Information Commissioner's Office.

3.8 Information Asset Owners (IAOs)

3.8.1 IAOs have been appointed in each of the individual Schools and Professional Services Directorates across the University and act as local points of contact in relation to data protection and information security matters, supported by the Information Management and ITS teams accordingly.

3.8.2 IAOs are expected to have a general overview of the data held within their area and a broad understanding of the usage of the information and any associated risks.

3.9 Information System Owners/Administrators (ISOs/ISAs)

3.9.1 Working closely with the IAOs, the ISOs/ISAs are responsible for maintaining system performance, security and availability of technology services provided across the University.

3.10 Senior Risk and Resilience Manager

3.10.1 The Senior Risk and Resilience Manager is responsible for ensuring that information security risks and recommended mitigations are recorded and maintained on the risk register, working in conjunction with Cyber Security colleagues in ITS, IAOs and ISOs/ISAs.

3.10.2 The Senior Risk and Resilience Manager is also esponsible for presenting the risk register to the SIRO and Audit and Risk Committee (ARC).

3.11 Cyber Security team

3.11.1 The Cyber Security team, located within ITS, is responsible for the protection of devices, services and networks – and the information on them – from theft or damage via electronic means.

3.11.2 The team is also responsible for identifying, analyzing, and managing potential threats and for mitigating risks, working in in conjunction with ISO/ISAs and other technical colleagues.

3.12 Human Resources (HR)

3.12.1 HR are responsible for managing the personnel aspect of information security, e.g. by supporting ITS staff and facilitating the delivery and monitoring of institutional training where required, as well as ensuring that new starter and leaver processes reflect information security-related requirements accordingly.

3.13 Auditor(s)

3.13.1 Internal/external auditors are responsible for conducting audits to determine the overall health and integrity of the University's Information Security programme and providing the associated formal reports to the University's Executive Group (UEG).

3.14 University Executive Group (UEG)

3.14.1 UEG is responsible for approving the University's information security strategies, policies and related documentation, and essential architectures, ensuring they are aligned with the University's Statement of Risk Appetite and Tolerance.

3.15 Audit and Risk Committee (ARC)

3.15.1 ARC provides assurance to the University's Council on the overall effectiveness of information security risk management within the University.

3.16 Council

3.16.1 As the governing body of the University, Council has overall responsibility for the performance of institutional information security risk management and for ensuring that appropriate risk and resilience measures are in place, with a focus on avoiding and proactively mitigating information security risks.

3.17 More granular detail relating to specific roles and responsibilities is provided in the Information Security Roles and Responsibilities Matrix (linked at the end of this policy).

4. POLICY

4.1 Information Security Principles

4.1.1 The University will protect information assets[4] through consistent application of a process of risk assessment and the implementation of appropriate controls[5] to manage and mitigate risk.

4.1.2 The University will ensure that information is handled legally, securely, efficiently and effectively, in order to deliver the best outcomes, accountability and ensuring compliance with all statutory and regulatory requirements.

4.1.3 Information will be appropriately secured, in accordance with the University's Statement of Risk Tolerance and Appetite, in order to protect the University and its stakeholders from the consequences of unauthorised access or disclosure, and specifically the consequences of breaches of confidentiality[6], failures of integrity[7] or interruption to the availability[8] of information.

4.1.4 The University will ensure that all users have access to the information and/or Information Technology Services they require in order to carry out their studies or work and will facilitate appropriate training and support to ensure that they are able to adhere to their information security responsibilities.

4.1.5 Incidents will be effectively managed and resolved, lessons identified will be implemented to continuously improve information security controls and maturity.

4.2 Organisation and Governance

4.2.1 An appropriate framework, detailing roles and responsibilities, is in place in order to manage, oversee and monitor compliance with information security requirements.

4.2.2 Security controls must be put in place to ensure that confidentiality, integrity and availability of information is assured.

4.2.3 Controls should be commensurate with risk but must always adhere to minimum standards set by University policies, legal and regulatory standards.

4.2.4 Security controls must be maintained when information is taken off-site, accessed from off-site or accessed using mobile technologies regardless of who owns the device.

[4] IT infrastructure refers to servers, network switches, etc, and systems
[5] A measure that is modifying risk
[6] Non-public information is only available to authorised users
[7] Information is complete, accurate, and fit for purpose
[8] Information is available when and where it is needed

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

4.3 Training, Awareness, and Personnel

4.3.1 Information security awareness training will be made available to all users.

4.3.2 Information security awareness and education campaigns will be delivered throughout the year and measured for effectiveness in order to deliver continuous improvement.

4.3.3 Where appropriate, pre-employment screening is in place.

4.3.4 Users that hold specific responsibility for security (e.g. ISOs) will have role-specific information security training.

4.4 Risk and Asset Management

4.4.1 Information security risks will be managed in accordance with the University's Risk Management Framework.

4.4.2 Appropriate risk assessments will be carried out for information and IT assets in order to determine the level of control required to keep risks within acceptable levels.

4.4.3 Risk assessments will be included in the business case for any new IT systems and will be repeated periodically and when significant changes occur.

4.4.4 Identifying and implementing security controls will be achieved by an appropriate mix of risk assessments, policies, standards, guidelines, technical measures, training, support, audit and review.

4.4.5 Policies are in place to ensure the information and information assets are classified and processed in line with relevant requirements. Considerations must be made to the classifications assigned to information and implement restricted access controls as necessary both with regard to storage and access.

4.5 IT Security and Access Control

4.5.1 University IT Services will be protected by minimum technical procedures defined by University.

4.5.2 Information Technology Services must have security considerations integrated into each phase of the system life cycle, from the initiation of a project to develop or procure a system to its disposition. The process starts with the initiation, analysis, design, and implementation, and continues through the maintenance and disposal of the system.

4.5.3 Access to systems and information assets will be restricted to authorised users for appropriate and authorised activities only in accordance with organisational requirements. Access will be granted on a least privilege basis.

4.5.4 Appropriate systems and/or processes will be implemented in order to detect unauthorised access, modifications or malicious behaviour.

4.5.5 Accounts will be appropriately de-provisioned upon termination and user accounts will be reviewed regularly.

4.5.6 The University will ensure that its Information Technology Services, third-party arrangements and information sharing are designed, configured and facilitated with sufficient and appropriate measures implemented to minimise the risk of information security breaches.

4.6 Third Party Security

4.6.1 Information security provisions of vendors and third party service providers will be assessed to ensure they are robust.

4.6.2 Appropriate due diligence and information security risk assessments will be carried out when engaging with new third-party service providers.

4.6.3 A record of third party service providers and risks will be maintained and compliance of third parties against the University's security requirements will be monitored periodically.

4.6.4 Transfer of information to third parties (including use of cloud or third party hosted services by individual users) must comply to relevant policies and legislation and must be authorised at an appropriate level, i.e.:

- The appropriate data sharing agreement and/or contract clauses must be in place and reviewed accordingly by relevant colleagues (e.g. Data Protection Officer, Office of the General Counsel, IT Services); and

- Minimum agreed levels of security controls must be maintained.

4.7 Physical Security

4.7.1 The University campus and IT facilities will be protected by appropriate environmental and physical security arrangements.

4.7.2 Assurances that appropriate arrangements are in place will also be required where third parties have responsibility for hosting or processing University information held physically.

4.8 Incident Management

4.8.1 Information security incident management tools will be implemented to ensure incidents are detected, reported, investigated and appropriately managed.

4.8.2 All incidents involving actual or suspected/potential breaches of information technology security must be reported and managed in accordance with the Information Technology Security Incident Reporting Process.

4.8.3 Information security breaches must be reported immediately to the IT Service Desk through any available channel so that they can be reviewed as soon as possible.

4.8.4 Information security breaches involving personal data should be reported in line with the University's Data Protection Policy.

4.8.5 The University will investigate all security incidents and take appropriate action in accordance with this and other relevant policies, University Regulations, legal and regulatory requirements.

5. BREACH OF THIS POLICY

5.1 Any actual or suspected breach of this policy must be reported to the SIRO who will take appropriate action and inform the relevant internal and external authorities.

5.2 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.

5.3 University policy is that activity which relates to the prevention or detection of crime, or breaches legal, regulatory or compliance standards will be referred to the Police, or supervisory and regulatory bodies as required.

6. LEGISLATION AND GOOD PRACTICE

6.1 The Committee of University Chairs Higher Education Code of Governance requires that effective arrangements are in place for the management of information and to meet all relevant legal and regulatory requirements. Similarly, the Office for Students identifies Public Interest Governance Principles that include accountability and risk management and are applicable to information governance.

6.2 The University is also responsible for complying with relevant UK legislation, including data protection legislation, the Freedom of Information Act 2000, and the Counter-Terrorism and Security Act 2015 (i.e. its Prevent Duty)[9].

6.3 The Janet Network connects education and research organisations in the UK (including universities) to each other, as well as to the rest of the world. Users of the University of

[9] The Prevent Duty aims to safeguard people from becoming terrorists or supporting terrorism. The University's obligations include having suitable IT policies and procedures in place to meet the requirements of the Duty.

Sussex’s network must also abide by the regulations outlined in the Janet Acceptable Use Policy. Non-compliance with Janet regulations by University users could result in access to this service being suspended or withdrawn completely for the entire institution.

Document Control					
Document No	ISP01	**Version**	6.2	**Date Issued**	June 2024
Author	Cyber Security Manager	**Reviewed by**	UEG	**Department**	ITS

Review / Contacts / References	
Policy title:	Information Security Policy
Date approved:	September 2023
Approving body:	University Executive Group (UEG)
Last review date:	September 2023
Revision history:	6.0 – April 2022 5.0 – October 2021
Next review date:	September 2026
Related internal policies, procedures, guidance:	Information Security Roles and Responsibilities Matrix Information Technology Security Incident Reporting Process Information Security Policies (including Regulations for the Use of IT) 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 Finance Systems Access Policy Data Protection Policy and Guidance Records Management Policy and Guidance Regulations of the University Risk Management Framework and Guidance University information on counter-terrorism safeguards (Prevent) Exceptions Process
Policy owner:	IT Services
Lead contact / author:	Cyber Security Manager