UNIVERSITY OF SUSSEX

IT Services

INFORMATION TECHNOLOGY (IT) SECURITY RISK MANAGEMENT POLICY (ISP20)

1. Overview and Purpose

1.1 Digital information is a valuable asset and must be managed with care.

1.2 All IT-based information systems and services require an appropriate level of controls to protect them against accidental or criminal and deliberate loss or damage.

1.3 It is not possible to protect fully against all threats and eliminate all IT and cyber security risks in absolute terms. Controls to protect IT assets must be based on an assessment of the risk posed to the University aligned to the University's Statement of Risk Appetite and Tolerance.

1.4 The objectives of IT security risk management are ensuring that:

- University IT security risks are identified and considered.
- All identified IT security risks are managed in a consistent manner, in accordance with the University's Risk Appetite and specifically the Risk Management Framework.
- Controls (e.g., physical, environmental, procedural, and technical) are implemented and are proportionate, balancing the management of the identified threat with the need to operate to meet the overall objectives of the University; whilst conforming with information security best practices and standards.

1.5 This policy aims to ensure that ensure that the University's approach to managing IT security risk, including cyber, is undertaken consistently and in the interest of protecting the institution's reputation, people, assets and intellectual property.

2. Scope

2.1 The policy applies to all IT-based information and physical assets[1] owned and managed by the University.

2.2 This policy applies to all staff users of university IT equipment and services[2].

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

- Employees, whether permanent, fixed-term, temporary, or casual, and those with Emeritus status
- Contract, seconded, and agency staff

[1] Hardware, Software, digital assets and licences.
[2] 'Services refers to any digital information or service provided or procured by the University and accessible through the University networks or over the Internet

- Volunteers, apprentices, and interns; and
- Others performing services for or on behalf of the University (for example, agents and consultants).

3. Responsibilities

3.1 **The University's Chief Information Security Officer (CISO)** – the most senior officer within IT Services, i.e. CIO, CDTO, etc – will be accountable for institutional IT security and cyber response. This officer will own the IT Services Risk Register and ensure that relevant risks are escalated to the institutional risk register (IRR) when applicable. The CISO will report periodically to Audit and Risk Committee on cyber risk.

3.2 **The IT Leadership Team (ITLT)** will individually take responsibility for the identification and consideration of IT security within their respective areas and will collectively meet monthly to consider risk at a divisional and institutional level. ITLT will maintain the Risk Assurance Platform for IT Services and ensure that Risk Assessments are considered in respect of whether new assessments need to be added to the Risk Register.

3.3 **The IT Service Desk** will triage and assess threats across the IT estate and escalate them to relevant teams within IT Services for resolution where necessary. If the IT Service Desk, consider a threat to be significant they will notify the Cyber Security team and CISO with immediate effect. The IT Service Desk will maintain a record of incidents in the IT Service Management software application along with past resolution actions and lessons learned.

3.4 **The Change Advisory Board (CAB[3])** will consider the requirement for an IT Security Risk Assessment as a part of Service Transition and when introducing a new or significantly changed business application into the production IT environment. If a Risk Assessment is required, the relevant member of ITLT will be notified.

3.5 The IT Services-based **Cyber Security team** will support ITLT in the production of Risk Assessments and commission Risk Assessments immediately following Penetration Testing activity or when required for adherence to cyber security standards auditing.

3.6 **All Staff Users** (as defined in section 2.3) are responsible for completing compulsory information security training provided by the University to raise awareness of potential cyber and IT risk, and for reporting any IT or cyber security-related risks and issues they become aware of via to ITservicedesk@sussex.ac.uk.

4. Policy

4.1 The University must ensure that its IT assets are appropriately secured to protect the University and its stakeholders from the consequences of breaches of confidentiality[4],

[3] Change Advisory Board (CAB) is a change management team that consider/advise on requested changes, assisting in the assessment and prioritisation of changes. The body is made up of IT and Business representatives.

[4] Where information could be made available or disclosed to unauthorised individuals

failures of integrity[5] or interruption to the availability[6] of information, while allowing users to have access to University information and/or information technology services they require in order to carry out their studies and/or work.

4.2 As such, the University will:

4.2.1 Identify IT/cyber security threats which can affect the confidentiality, integrity or availability of IT assets through its cyber security tools (firewalls, event management systems, etc), various log entry files, Service Desk tickets and configuration databases.

4.2.2 Consider the potential threats applicable to IT assets, whether natural or human, accidental or malicious.

4.2.3 Assess the likelihood of IT security threats occurring and their potential impact.

4.2.4 Employ appropriate and proportionate measures to manage IT security threats in accordance with the Risk Management Framework, as well as any other relevant methodology (see section 3.5).

4.2.5 Monitor and review progress in managing threats.

4.3 **Statement of Risk Appetite and Tolerance**

4.3.1 The institutional Statement of Risk Appetite and Tolerance defines the amount and type of risk that the University of Sussex will take to achieve its objectives (risk appetite) and sets the parameters which determine the acceptance of risk (risk tolerance) without compromising legal or regulatory compliance. Digital and IT (inc cyber security and IT-related risks) form part of the Statement.

4.3.2 Within the parameters set by its Risk Tolerance, the University will manage IT-related risk by undertaking activities which support the fulfilment of its objectives and protection of institutional assets and intellectual property.

4.3.3 Particular objectives may carry various inherent and operating risks and within this context, such as administrative access to hardware and system. Risk tolerance may vary on a case-by-case basis and is continually assessed by the ITLT. Commentary on risk appetite can/will feature in the IT entries within the Risk Management Platform (RAP).

4.3.4 Risks will be assessed in proportion to the opportunities that they present and the controls that are necessary to protect the University from financial and reputational loss or non-compliance with legislative and regulatory requirements.

4.4 **Information Security Risk Assessments**

[5] Where accuracy or completeness of information or data could have been compromised
[6] Where a system, service or information is not accessible as it should be.

4.4.1 An IT Security Risk Assessment (RA Form) shall be completed by a member of the IT Services' Cyber Security Team:

- Whenever a cyber threat is discovered that is recorded as a Priority 1 classification in the University's IT Service Management (ITSM) solution,
- As part of the Service Transition to go-live for a new technical solution – particularly with a web-facing element - that may affect the cyber security defences of the University or hold Sensitive[7] data,
- Bi-annually (every two years) following external penetration testing,
- Whenever recommended by the Change Advisory Board upon consideration of a formal change request, or
- When there are changes to cyber security standards to which the University requires, or aspires to gain, certification, e.g. Cyber Essentials+.

4.4.2 The results of IT Security Risk Assessments may be recorded in the University Risk Management Platform (RAP) through the creation of a new (or updated) risk entry within the divisional risk register, or institutional risk register if deemed significant enough to warrant escalation. The ITLT review the RAP platform every month so they will consider entry of new risks as part of the process.

4.4.3 Where action is required as a follow up to the IT Security Risk Assessment, this will be owned by the most relevant member of the IT Leadership Team, e.g. an infrastructure risk will be owner by the Assistant Director Infrastructure. They will resolve all remediatory actions and update the RAP as necessary until the associated risk entry can be closed or all outstanding mitigating actions have been resolved.

4.5 Risk Management Methodology

4.5.1 Information security risks are managed in line with the University's Risk Management Framework. It outlines each step of the risk lifecycle, including how risks are identified, assessed, treated, monitored, reviewed and reported.

4.6 Principles for Information Security Risk Assessments

4.6.1 Information Security Risk Assessments shall be completed with an understanding of:

- Principles outlined in the Information Security Policy (ISP01);
- The University's Statement of Risk Tolerance and Appetite
- The University's Risk Management Framework

[7] Definition of 'Sensitive' information as specified in the *Information Classification and Handling Policy*

- The University's processes, e.g. Business Continuity, change, or incident management processes;
- The impact to the University of information security risks should they occur;
- The technical systems in place supporting University activities;
- Legislative and regulatory requirements, e.g. Data Protection Act; and
- Up-to-date threat and vulnerability assessments.

5. Breach of this Policy

5.1 Any actual or suspected breach of this policy must be reported to the CISO via email, telephone call or logging a ticket through the IT Service Desk, who will take appropriate action and inform the relevant internal and external authorities as relevant.

On all relevant breaches, the CISO will report the incident under the University's Counter Fraud Policy.

5.2 Where there is deliberate misconduct or behaviour amounting to a 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 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 This policy forms part of the suite of Information Security Policies and sits alongside the Data Protection Policy and the Risk Management Framework to provide the high-level outline of and justification for the University's risk-based information security controls in line with relevant legislation as detailed in the over-arching Information Security Policy (ISP1).

6.2 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 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.

UNIVERSITY OF SUSSEX

IT Services

Review / Contacts / References	
Policy title:	IT Security Risk Management Policy
Version:	1.0
Date approved:	03 October 2023
Approving body:	University Executive Team (UET)
Last review date:	N/A
Revision history:	N/A
Next review date:	3 years from date of approval
Related internal policies, procedures, guidance:	Information Security Policy (ISP01); IT Security Risk Assessment Form Statement of Risk Appetite and Tolerance Information Security Policies (including Regulations for the Use of IT) Payment Card Industry Data Security Standard Policy Data Protection Policy and Guidance Records Management Policy and Guidance Regulations of the University Janet Acceptable Use Policy
Policy owner:	Chief Information Security Officer
Lead contact / author:	Cyber Security Manager