Information Security Policy

1. INTRODUCTION

Whilst the University of Northampton (UON) expects its employees and staff to comply with this policy, it does not confer contractual rights or form part of any contract of employment. The policy may be amended by the University or replaced at any time following appropriate consultation and negotiation with recognised trade unions. Breach of this policy may be addressed via the University's Disciplinary Policy and Procedure, and Code of Conduct Policy.

This policy will be reviewed by the IT Services department on an annual basis or amended in response to changes in future legislation and/or case law.

2. OWNERSHIP

The IT Services department owns and manages this policy on behalf of The University.

3. ORGANISATIONAL SCOPE

This is a University policy that applies to all employees, students, and contractors of the UON, and any applicable 3rd parties working on behalf of the UON. This also includes any wholly owned subsidiaries unless an alternative applicable policy exists. Those in scope will be referred to as 'Users' for the purpose of this document.

4. POLICY STATEMENT

The University manages, handles, and stores large volumes of data relating to learning, teaching, research, and professional and administrative activities. The purpose of this policy is to ensure that this data, and the IT Resources that process it, are appropriately secured to mitigate risks which impact confidentiality, integrity, and availability. Failure to adequately secure data can increase the risk of financial and reputational loss, breach of compliance, impacted operations, and legal implications.

Information Security is an important part of the University's culture, and therefore it is the responsibility of all Users of UON data to read, understand, and comply with this policy and the associated policies related to their activities and Information Security.

5. DEFINITIONS

Availability
To ensure that data and IT Resources are available to authorised Users as and when required.

Confidentiality
To protect data from unauthorised access and/or disclosure.

Data
Includes but is not limited to any information accessed, stored, and/or processed on/by IT Resources, stored either digitally or hardcopy, in formats including, but not limited to text, graphics, images, sound, and video.

General Data Protection Regulation (GDPR)
A regulation in EU law on data protection and privacy for all individuals within the EU and EEA.

Information Security Management System (ISMS)
An ISMS represents a set of policies, procedures, controls, and responsibilities that set the information security rules of an organisation.

Information Security Risks
Risks to operations, assets, and individuals due to potential unauthorised access, use, disclosure, disruption, modification, or destruction of information and/or information systems. Risks that could cause the loss of confidentiality, integrity, and/or availability of UON data or IT Resources.

Integrity

To safeguard the accuracy and completeness of data.

ISO/IEC 27001:2022

An international standard for information security management published by the International Organisation for Security (ISO) and the International Electrotechnical Commission (IEC). The standard contains requirements for establishing, implementing, maintaining, and continually improving an ISMS.

IT Resources

All assets that connects to the UON network, and/or contains, accesses, stores, and/or processes UON data. This includes, but is not limited to desktop computers, laptops, smartphones, tablets, servers, printers, data and voice networks, networked devices, software, applications, electronically stored data, portable data storage devices, hardcopies, third party networking services, telephone handsets, and video conferencing systems.

Payment Card Industry Data Security Standard (PCI-DSS)

An information security standard created by the PCI SSC to reduce payment card fraud by increasing security controls around cardholder data.

Risk

The likelihood and impact of a threat exploiting a vulnerability.

Sensitive Data

There are three main types of sensitive data, including but not limited to: **personal** (this is data from which an individual/individuals are personally identifiable. It includes names, contact details (phone, address, email), initials, financial information. It can include any identifier of an individual, e.g. a job title can be personal data if it alongside other information that would allow someone to identify the individual), **special category** (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, generic data, biometric data, or data concerning health, a person's sex life, or a person's sexual orientation) and **confidential** (information which is confidential to the University for example for business reasons. This can include meeting papers and minutes, proposals for discussion, research and intellectual property, financial information like individual bank details or details of contracts. If you are unsure about the confidentiality of data, check with your line manager or the person/team which originated the data). This data must be protected from unauthorised access to safeguard its privacy and the security of individuals and the organisation.

Threat
An adversary or attacker that has the opportunity, capability, and intent to exploit a vulnerability to cause harm.

Vulnerability
A weakness, flaw, or misconfiguration in a system, process, or control that can be exploited by a threat. Can be both technical and human error.

6. KEY PRINCIPLES

6.1. Policy Structure

- The University of Northampton's Information Security Policy constitutes this top-level policy, and the sub-policies documented on SharePoint under IT Policies. All constituting policies are of equal standing, whereby this top-level policy takes precedence if inconsistencies are found.
- This Information Security Policy and relevant constituting policies should be communicated to in scope Users either on an ad-hoc basis, or via Information Security awareness and training.

6.2. Information Security Objectives

- The University's Information Security objectives should be established by the Head of Cyber Security & Compliance and regularly reviewed to ensure they continue to align to the strategy of the IT Security Team, the IT Services Department, and the University as a whole.
- The Information Security objectives should be set every 2 years and be based on the current risks to the University, documented in the IT Risk Register.
- The Information Security objectives should be documented and monitored, including a plan on how and when they will be achieved.

6.3. Information Security Principles

- Users must handle data and IT Resources in an appropriate manner that complies with the Acceptable Use Policy.
- Sensitive data should be classified and handled in an appropriate manner in accordance with its classification.
- Sensitive data should only be disclosed to authorised Users that have a legitimate need.
- The installation of software on IT Resources should be restricted to only approved applications.
- Privilege access to data and IT Resources should be appropriate to a User's role, approved, reviewed on a regular basis, and revoked where appropriate.
- Data and IT Resources should be monitored and protected against unauthorised access.
- Appropriate security controls and tools should be in place to protect data and IT Resources, for example anti-malware/Endpoint Detection and Response (EDR), cryptography, web filtering, email filtering, network segregation, firewalls, multi-factor authentication.
- Appropriate logging and monitoring tools should be in place, for example Security Information and Event Management (SIEM).
- Appropriate physical and environmental controls should be in place to protect data and IT Resources.
- Appropriate Mobile Device Management (MDM) solutions should be in place to protect data on mobile devices.
- Sensitive data and critical IT Resources should be backed up to reduce the risks against availability, integrity, and data loss.
- Vulnerabilities and risks should be adequately assessed and treated on a regular basis.
- An IT Services managed anti-malware/EDR solution should be installed on all applicable University IT Resources, should be a supported version, and should monitor endpoint telemetry in real time. Users must not be able to disable the solution without approval/approved privilege access.
- IT Resources should be appropriately sanitised before reuse or secure disposal.

6.4. Breaches of Security

- If Users suspect a security or data breach has occurred, they must immediately inform IT Services via the IT Service Desk on 01604 893 333 (Ext. 3333), at the Learning Hub, or using the Service Desk Portal (https://uon.saasiteu.com/Modules/SelfService/#home).
- In the event of loss or theft of a UON device or device containing UON data, the User must act promptly to minimise the risk of compromise by immediately notifying IT Services. Theft of the device should also be reported to the police. Failure to report a loss may be dealt with under the appropriate disciplinary and GDPR policies.
- In the event of a suspected or actual information security breach, the Cyber Security Team may require that an information asset or User account be made inaccessible, with or without prior consultation with the owner/User.
- Breaches of information security that occur outside of working hours should be reported to the on-call Major Incident Manager for investigation and incident response. Contact details can be found via the on-call notification/rota.
- Information security breaches that involve the confidentiality of sensitive data should be reported to the Data Protection Officer (DPO@northampton.ac.uk).
- Breaches of physical security should be reported to the Campus Security Team.

6.5. Awareness and Training

- Users should be provided with a range of awareness and training materials in relation to Information Security and relevant UON policies and procedures.
- Awareness and training should take place on a regular basis, including during induction before the end of a User's probation period, and then periodically afterwards.
- The primary awareness course should include an assessment activity to test the effectiveness of the material.
- An awareness programme/plan should be in place to schedule awareness and training materials and should adapt to current incidents and risks affecting the University.

- Managers should discuss and share Information Security policies with Users at the earliest opportunity and offer support, help, and appropriate training where appropriate for the User's role.
- IT Services/high privilege Users should be provided with additional training in regards to Information Security.

6.6. Compliance

- A robust Information Security Management System (ISMS) should be implemented, which aligns to the University's approach to Information Security as defined within this policy. The ISMS should ensure that adequate protections are in place against known and emerging threats.
- A Gap Analysis against relevant Information Security frameworks should be conducted and reviewed on an annual basis and feed into continual improvement actions.
- A Statement of Applicability should be completed to evaluate the implementation of ISO27001:2022 controls and risk treatment controls.
- Any Information Security requirements or improvements to the ISMS, highlighted off the back of audits or assessments, should be assessed and addressed within either the Audit Action Log or the Continual Improvement Log.
- Compliance to the Payment Card Industry Data Security Standard (PCI-DSS) should be managed as per the PCI-DSS Policy.

7. ASSOCIATED DOCUMENTS

Acceptable Use Policy
BYOD Policy
Cyber Security Awareness Programme
Information Security Objectives
ISMS – Gap Analysis
ISMS – Statement of Applicability
PCI-DSS Policy

8. EQUALITY IMPACT ASSESSMENT

There is no adverse equality impact within this policy. All responses to breaches of rights will be dealt with in accordance with this Policy and relevant Appendices irrespective of an individual's specific characteristics.

9. VERSION CONTROL

Version Control	1.0	**Approval record**	
Author:	Katie Holman	Approval:	IT Strategy Board – 24/01/2024 TU Liaison – 12/03/2024
Date written:		March 2024	
Current status:		Live	
Record of Amendments			
Date	Version number	Details of Change	Approval