Policy Name	**Information Security Policy**
Subject	Information Security
Approving Authority	IMSSC and UEB
Accountable Person	Chief Information Security Officer
Responsible Team	Information Security and Compliance
First approved	January 2018
Last updated	29 January 2024
Version Number	Version 4.1

1 Introductory Purpose and Background

The University of Nottingham (hereinafter referred to as "the University") recognises the importance of information security in maintaining the confidentiality, integrity, and availability of its information systems and digital resources. This Policy sets out the University's overall approach to Information Security, its sub-policies, standards, and guidance provide detailed approaches for specific areas. This Policy overarches the University's Information Security Strategy. Additionally, this Policy establishes the responsibilities of key individuals and departments in ensuring the security of the University's information systems and digital resources.

2 Scope

This Policy applies to all University staff, students, associates, and other individuals who access, use, or manage University information systems and digital resources.

3 Definitions

Assurance Team	A team that provides confidence that a system or setup complies with a set of established guidelines or standards.
Data Assets	These include data collected, processed, stored, transferred, and disposed of by the University, regardless of the medium or format.
Data Asset Register	A record of data assets owned or managed by the University.

Digital Technology Services (DTS)	The department responsible for providing and maintaining technology services and infrastructure within the University.
Compliance	Adherence to established rules, regulations, standards, and laws relevant to the University's operations.
Information Security	The process of protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.
Risk Assessment	The process of identifying and analysing potential issues that could negatively impact key business initiatives or critical projects to help organisations avoid or mitigate those risks.
System Owner	The individual or group that is primarily responsible for the operation, functionality, and efficiency of a specific information system.

4 Policy

4.1 Key Principles

The University will ensure all data assets and systems are resilient to threats, whether internal or external, deliberate, or accidental.

All University staff, students and associates must ensure that University information and systems:

- Are known and appear on the appropriate data asset register;
- Are used in a controlled manner and only by authorised individuals;
- Are configured, stored, processed, and transmitted in a manner that maintains the confidentiality, integrity and resilience of the information and system;
- Are shared only with authorised parties;
- Have security controls applied based on risks posed to the University as well as the University’s contractual, regulatory, and legislative requirements; and
- Where a university information system is hosted within a DTS maintained environment, the system owner must comply with the minimum baseline security controls, as specified by DTS Head of Cyber Security.

Additionally, all University staff, students and associates must ensure that any incidents are effectively reported to the DTS Service Desk.

Any service or IT (Information Technology) equipment which cannot meet the requirements of this Policy must be appropriately segregated from other IT systems in the network to ensure they cannot compromise the overall security position.

4.2 Key Roles and Responsibilities

4.2.1 The **Chief Information Security Officer (CISO)** is responsible for the creation and maintenance of this policy. In support of the effective operation of this policy the CISO will:

- Support DTS, system owners and data owners to ensure that information security controls are implemented;
- Monitor the implementation of the controls required by this and related policies;
- Provide information security training and awareness programmes for University staff, students and third parties; and
- Coordinate incident response and management in the case of major information security breaches or incidents.

4.2.2 The **Chief Digital Officer (CDO)** is accountable for the oversight and management of DTS at the University. The CDO shall ensure that DTS implements and maintains appropriate security measures to protect the University's information systems and digital resources.

4.2.3 **DTS Head of Cyber Security** is responsible for securing DTS owned systems within the University, including but not limited to hardware, software, networks, and devices. In support of the effective operation of this Policy the Head of Cyber Security will:

- Develop, implement, and maintain sub-policies, procedures, and guidelines in line with this policy, industry best practices and applicable legal and regulatory requirements;
- Establish and maintain appropriate security controls to protect the confidentiality, integrity, and availability of University data assets;
- Ensure regular monitoring, testing, and assessment of the University's information systems to identify and address potential vulnerabilities and threats;
- Provide additional specific information security training and awareness programs for DTS staff as appropriate; and
- Assist system owners in the implementation of security controls as required for their systems.

4.2.4 **Faculty Pro-Vice Chancellors, Directors of Professional Service Departments** are accountable for the Information Security of information and systems within their faculty or department, they will:

- Nominate an individual who is responsible for deploying this policy within their faculty or department;

- Ensure that staff and students within their department comply with this Policy and related procedures and guidelines; and
- Ensure any information security incidents or concerns are raised with DTS Service Desk for investigation and resolution.
- Ensure that any areas of non-compliance with this policy are investigated and actions taken to manage the associated risks to an acceptable level – See 4.4.1 - Exceptions

4.2.5 **The Information Management and Security Steering Committee (IMSSC)** is responsible for overseeing the maintenance, implementation, and performance of this Policy.

4.3 Key considerations of this Policy

4.3.1 Access Control

The University will provide controlled access to its IT systems and data for all approved users (staff, students, associates and third parties) and ensure that this access is appropriately managed. Access to IT systems and data must be restricted to the requirements of a user's role.

4.3.2 Anti-Malware

All University systems will be able to prevent, detect and recover from malware infections in a timely manner, with minimal disruption to normal operation.

4.3.3 IT Network Security

All University networks will be designed, architected, and managed in such a way that data assets and critical systems are appropriately resilient to all threats, whether internal or external, accidental, or deliberate.

A secure network is the foundation of the computing facilities at the University. Regardless of the controls applied at a network level, any service that is built on top of the network must implement its own security controls in line with the risk profile of the service and to comply with the University's wider Information Security policies.

Any service or IT equipment which cannot meet the requirements of the University's Information Security Policy must be appropriately segregated from other IT systems in the network to ensure they cannot compromise the overall security position.

4.3.4 Logging and Monitoring

Access to and use of University IT systems and data assets will be logged and monitored relevant to the risk to enable the University to maintain assurance over appropriate use and to enable malicious or inappropriate activity to be detected.

4.3.5 Mobile Device Policy

All University restricted data assets will be protected wherever they are held, including on mobile devices. Mobile devices are considered within the scope of this Policy whether they are owned and managed by the University or not.

4.3.6 System Configuration and Management

The University provides secure and resilient services by properly configuring and maintaining the systems used by University staff, students, associates, and others.

All University System Owners are responsible for ensuring that all Systems are known, documented, secured, and maintained in such a way that they:

- Provide continuing security for the data they hold and services they provide;
- Support the overall security of the University;
- Can be adequately restored without unreasonable loss of data in the event of an outage; and
- Have anti-virus software installed.

This Policy applies to all systems deployed on the University's network, including any private or public clouds, irrespective of System Owner.

4.3.7 Third Party Access

All third parties that require access to University systems and data must be approved and controlled, and they must follow the rules for access.

4.3.8 Website and Web App Security

All University websites and web applications, whether permanent or temporary, will be developed, maintained, and managed in a secure state appropriate to the sensitivity of the data they serve.

4.4 The consequences of non-compliance

All University employees, staff, students, contractors, and other individuals who access, use, or manage University data assets and digital technology services must comply with this Policy and related procedures and guidelines.

A failure to comply with the principles set out in this policy may amount to a disciplinary offence and may be addressed through the relevant procedures which includes, but is not limited to, the staff Disciplinary Policy and the Code of Discipline for Students.

4.4.1 Exceptions

The expectation is that policies are binding for all staff and/or students identified as within the policy's scope. The consequences of non-compliance can be significant for individuals and the University. However, there may be circumstances where IT systems cannot be configured to operate in compliance with this policy, due to technical limitations within the IT equipment, or other constraints bought about through their legitimate use.

If a Faculty or Professional Services Department has identified a legitimate requirement for an IT system to operate with an exception to this policy or to one or more of the specific provisions of this policy, the following must happen:

1. In the first instance, all reasonable steps must be taken to ensure compliance.

2. Where the Faculty or Department intends to adopt a position of non-compliance, a risk assessment must be carried out. The PVC or Director of Professional Service will assume accountability for the risks identified and these will be added to the local risk register.

3. The PVC or Director of Professional Service will provide formal notification of non-compliance to the Assurance Team, articulating the detail of the exceptions and a supporting rationale for the position taken.

4. The Assurance Team will provide reports of non-compliance to:

    i. The Accountable person for the policy; and
    ii. The Assurance Committee.

5. The exception(s) should be reviewed by the PVC or Director of Professional Service at least every 12 months and either reiterated or removed. Exceptions should be removed as soon as they no longer apply rather than at the conclusion of any relevant 12-month review period. Where exceptions are removed, the local risk register must be updated, and the Assurance Team notified.

4.5 How compliance with the Policy will be measured

This Policy comes within the scope of the Priority Controls of the Assurance Framework (see the Risk and Assurance SharePoint site for further information) and compliance will be assessed through the annual self-attestation cycle.

4.6 Provisions for monitoring and reporting relating to the Policy

All relevant updates related to this policy will be reported to IMSSC.

5 Review

This Policy will be reviewed biennially by the CISO and the IMSSC. It may also be revised as needed to ensure compliance with applicable laws, promote operational efficiencies, advance University strategy, and reduce institutional risks.

6 Related policies, procedures, standards, and guidance

Data Protection Policy
Information Security Policy Standards
DTS Acceptable Use Policy