Document Reference Number	**UoG/ILS/IS 001**
Title	Information Security and Assurance Policy
Owning Department	Information and Library Services
Version	1.7
Approved Date	07/02/2024
Approving Body	IT Management Board (IM)
Review Date	12/12/2024
Classification	Public – Non-sensitive

Information Security and Assurance Policy

1.0 Introduction

1.1 The University is committed to strengthening its information security capabilities by maintaining a strategy that draws on a framework of best practices. This is to assure the security of the University's information assets and fulfil relevant legal and statutory obligations.

1.2 The Information Security suite of policies and procedures set out the expectations for information security within the University. They also provide guidelines to users on their responsibilities for the appropriate use and safety of the University's information assets, and their professional and legal obligations to comply with the policies and related legislation.

2.0 Objectives

a) To ensure the University's information assets are appropriately safeguarded to meet and support its operational and strategic objectives.
b) To establish and enforce an information security programme that provides controls and safeguards commensurate with the risks to the University.
c) To ensure all users of the University's information assets are aware of and understand their responsibilities for protecting the confidentiality, integrity and availability of these assets.
d) To ensure that threats and risks to the University's information assets are appropriately managed.
e) To ensure all projects that involve processing the University's data, acquisition of IT systems and engagements with third parties are implemented in line with the Information Security Policies.
f) To ensure information security incidents are resolved promptly and appropriately to minimise the impact on the University.
g) To ensure there is a robust disaster recovery plan in place and that information security is captured in the disaster recovery planning.
h) To ensure the University continues to satisfy relevant statutory requirements.

3.0 Scope

3.1 The Information Security Policy and supplementary policies apply to all forms of information processing by or on behalf of the University, including but not limited to all paper records and information held on electronic devices.

3.2 The policy applies to all staff, students, contractors and third-party agents who access, use, process or manage the University's information assets.

3.3 The policy also applies to all information systems owned or leased by the University including information systems managed by third parties on behalf of the University.

4.0 Reference to the International Organisation for Standardisation (ISO) 27001

4.1 This policy complies with the University's Information Security Strategy and draws upon the ISO 27002 Code of Practice.

5.0 Principles

a) The University will continue to adopt information security best practices and will ensure continuous assessments and maturity of its Information Security program.
b) The University will continue to support activities to ensure that the data, people, devices, systems and facilities that enable the University to achieve its business purposes are identified and managed in a manner that is consistent with applicable data protection and privacy obligations, as well as with relative importance to its strategic objectives and its risk strategy.
c) The University will continue to implement policies that will strengthen access controls to its information assets and reduce information security risks.
d) The principle of "least privilege" will be implemented in the development and implementation of technology, regardless of whether it is internally developed or acquired from a third party.
e) Classification of data (information) will continue to drive the implementation of administrative and technical controls to safeguard these assets.
f) Information security responsibilities will be communicated to all users via relevant policies, job descriptions, terms and conditions of employment, contractual agreements.
g) The University will continue to promote an information security awareness culture through various user awareness and training activities.

h) The University's incident management plan will continue to ensure prompt and appropriate incident response and resolution, and apply lessons learned to inform risk management activities.
i) The Disaster Recovery Plan (DRP) will be maintained to ensure prompt and appropriate response and recovery activities in the event of a disaster.
j) All relevant contractual, legal and statutory requirements will continue to inform compliance strategies and related activities; and compliance with the Information Security Policies and relevant legislation will be monitored.
k) All cloud services that will process, transmit or store University data must undergo a compliance review through an Information Security Checklist, Privacy Impact Assessment and Contract Review.

6.0 Compliance

6.1 The University has an obligation to comply with relevant legal and statutory requirements. The Information Security Policies are to facilitate and underpin compliance with the applicable legislation.

The applicable laws include but are not limited to:

a) Data Protection Legislation
b) Copyright, Designs and Patents Act (1988)
c) Computer Misuse Act (1990)
d) Counterterrorism and Security Act 2015 and Prevent Duty Guidance: for Higher Education Institutions in England and Wales
e) Public Interest Disclosure Act

6.2 Relationship with other policies

The Information Security Policies are implemented in association with the University's Risk and Information Compliance Policies to facilitate the implementation of activities that will satisfy compliance with the statutory laws that govern these policies.

7.0 Responsibilities for Information Security

7.1 Vice Chancellor's Executive (VCE)

The Vice Chancellor's Executive is ultimately responsible for information security and compliance with related legislation. This includes:

a) Ensuring the Information Security Strategy aligns with the University's objectives.
b) Supporting the implementation of approved policies.
c) Resourcing and supporting information security initiatives.
d) Ensuring risk acceptance is commensurate with the defined risk appetite.

7.2 IT Management Board (IM)

The IT Management Board will be responsible for:

a) Ensuring that information security is implemented across the University.
b) Directing the allocation of resources and supporting the implementation of information security initiatives.
c) Engaging with the Information Assurance and Security Committee (IAS) to facilitate an information security awareness culture in the University.
d) In collaboration with the Information Assurance and Security Committee, advise the Vice Chancellor's Executive on matters relating to information security management and compliance assurance.

7.3 Information Assurance and Security Committee (IAS)

The Information Assurance and Security Committee provides strategic leadership and governance oversight of information security and data protection compliance within the University and serves as an advisory body to the Vice Chancellor's Executive (VCE) via the IT Management Board on information security matters. The Committee's remit is documented in its Terms of Reference.

7.4 Information Security Management and Data Protection Functions. The responsibilities of these functions are to:

a) Develop, communicate, implement and maintain Information Security and Information Compliance Policies and supplementary documents.
b) Implement and maintain the Information Security Awareness and Data Protection Training Programme and promote the adoption of best practices.
c) Identify risks, coordinate and implement risk management activities.
d) Coordinate prompt and appropriate incident management and ensure continuous improvement.
e) Liaise with relevant teams to implement effective security controls and ensure compliance with regulatory requirements.
f) Liaise with relevant teams to maintain an effective Disaster Recovery Plan.
g) Manage internal information security audits.

h) Monitor information security trends, propose and implement initiatives to strengthen the University's information security posture.
i) Implement continuous review and improvement of the Information Security Programme.

7.5 All Users (staff, students, guests, affiliates, contractors and third-party agents)

The responsibilities of all individuals who access, handle, store or manage the University's information assets include:

a) Familiarising themselves with the Information Security Policies, related policies, procedures and guidelines and complying with them.
b) Familiarising themselves with their information security responsibilities and carrying out these responsibilities.
c) Completing mandatory information security awareness and training courses.
d) Reporting information security incidents via the appropriate procedure promptly.

8.0 Risk Management

8.1 In line with the University's Risk Management Policy, Faculties and Directorates in collaboration with ILS will implement appropriate controls to mitigate internal and external risks to the security of the University's information assets they are responsible for. The relevant assessments must be completed to assess data privacy and information security risks.

8.2 Internal information security audits will be carried out to assess compliance with policies and will inform relevant recommendations and implementations of new or additional risk mitigation controls.

8.3 Audit and Risk Committee: Information security risk management operates within the framework of the University's Risk Management Strategy overseen by the Audit and Risk Committee.

8.3.1 To keep under review the effectiveness of risk management, control and governance arrangements, information security risk management plans and activities will be reported to the Audit and Risk Committee regularly. This would include recommendations for independent audits, monitoring of audit-outcomes and implementation of audit recommendations; presenting and providing regular information security reports to the Committee.

9.0 User Awareness and Training

9.1 The University will continue to provide information security awareness and training to staff and students to enable them to carry out their information security responsibilities effectively.

9.2 Specialist training will be provided to members of staff that require specific information security skills to carry out their job functions or for those who have access to sensitive data.

9.3 Contractors and third parties will be responsible for providing necessary awareness and training for their members of staff working with the University.

10.0 Data Classification and Information Handling

10.1 The Policy for Secure Data Handling and the associated procedures will continue to set out how University data is to be handled and the suitable controls to implement commensurate to the sensitivity and criticality of such data.

10.2 All users of the University's data are required to familiarise themselves with the Policy for Secure Data Handling and the associated procedures to protect the University's data from unauthorised access, disclosure, modification, loss, theft or damage.

11.0 IT Disaster Recovery Plan (DRP)

11.1 The University's Business Continuity Plan (BCP) covers all essential and critical business activities including the IT systems that support them. The IT DRP supplements the BCP and details the activities to be followed to maintain continuity of IT services and facilitate return to normal operations in the event of a disaster. The IT DRP will continue to be reviewed considering changes to business requirements and the IT environment in line with the University's Business Continuity Plan.

12.0 Incident Management

12.1 The management of information security incidents (including data breaches) promptly and appropriately will enable the University to efficiently mitigate the risks that may be associated with information security incidents.

The University's Policy for Managing Information Security Incidents (including Data Breaches) will set out the procedures and guidelines for reporting and managing data breaches and other information security incidents.

13.0 Policy Compliance

13.1 All users of the University's information assets must comply with the Information Security Policies and must keep abreast of updates to these policies.

13.2 The necessary steps to verify compliance to this policy shall be undertaken. This includes, but is not limited to, business tool reports, internal and external audits and feedback to the policy owner.

13.3 Failure to adhere to this policy will be addressed under the University's disciplinary processes and relevant contractor and third-party contractual clauses relating to non-conformance with the Information security policies.

14.0 Exception to policy

14.1 Any exception to this policy can be authorised only by the IASC, or the Executive Director and Chief Information Officer in consultation with the IASC chair.

15.0 Policy Review and Maintenance

15.1 This policy shall be reviewed annually and where necessary will be updated as part of the continual improvement process.

16.0 Definitions

Authorised Users (in the context of this policy and related documents)	All users who access, handle, process, store, share or manage the University's information assets based on a valid business need. These are University staff, students, contractors and third-party agents.
Availability	Information assets are accessible to authorised users when required.
Business Impact Analysis	A process for determining the impact of a loss or unavailability of an information asset or service to an organisation.
Confidentiality	Access to and sharing of sensitive or personal information is restricted only to authorised users based on a valid business need.
Data - Information Assets (in the context of this policy and related documents)	A collection of information (paper or digital format), hardware, software, infrastructure and services that support the implementation of University strategic and operational activities.
Information Systems - Information Assets (in the context of this policy and related documents)	Information processing computers or data communication systems.
Information Processing Facilities	IT system or service, location, building or infrastructure that houses information processing systems and services.
Integrity	The preservation of the complete, accurate and valid state of information assets.
Risk	The probability of an exploited weakness and its resulting consequence leading to an adverse event.
Risk Assessment	A process for identifying and evaluating risks.

17.0 Links

- Links to University-related information security policies, standards, procedures and guidelines.
- Links to the Information Compliance Policies.