UNIVERSITY OF ABERDEEN

INFORMATION SECURITY POLICY

1. Purpose

The purpose of this policy is to set out the University of Aberdeen's approach to Information Security Management. This policy, and the supporting Information Security Management System (ISMS), support the protection of University information and digital assets. It provides the guiding principles, statements and responsibilities to ensure information security objectives are achieved and that data confidentiality, integrity and availability are preserved. The policy and supporting ISMS support the University strategy and demonstrates the commitment to protecting digital assets.

2. Scope

This policy, and the supporting ISMS, applies to:

- All individuals, including staff, students, contractors and visitors, who have access to the University of Aberdeen digital services, information, login credentials and technologies.
- All facilities, technologies, and services that are used to process the University of Aberdeen information.
- All information processed, accessed, manipulated or stored by the University of Aberdeen.
- Internal and external processes that are used to store, transfer or process the University of Aberdeen information.
- External parties and suppliers that provide information storage, hosted systems, transferal or processing services to the University of Aberdeen.

3. Objectives

This policy and the ISMS, are designed to:

- Protect the confidentiality, integrity and availability of University digital assets, services and data.
- Establish a positive information security and data governance culture across the University.
- Ensure controls and mitigations are appropriate and effective by identifying and managing the information security threats and risks.
- Reduce information related risk to appropriate and acceptable levels.
- Establish a clear governance structure for information security at the University.
- Clearly define responsibilities for maintaining information security.

- Enable compliance with legal, regulatory and contractual obligations.
- Provide assurance to IGC, senior management, information owners, individuals and organisations, both within and outside of the University that their information is appropriately protected.
- Support secure information sharing and collaboration.
- Support the University of Aberdeen's strategic objectives.

4. Roles and responsibilities

- **All users, including staff, students, contractors and third parties** at all levels are responsible for protecting the University's information, adhering to all relevant policies, guidelines and procedures and making informed decisions to protect the information that they process. Users are expected to familiarise themselves with the relevant policies governing the information and systems they access.
- **Heads of Schools and Directors of Professional Services** are accountable for the effective implementation of this information security policy, and supporting information security rules and standards, within their areas of managerial responsibility.
- **University Officers and Managers** are accountable for ensuring that information in their category is not put at undue risk. They will approve all use and sharing of information in their category, having considered the risks and benefits.
- **The Information Governance Committee** has executive responsibility for information governance and security within the University of Aberdeen. Specifically, The Information Governance Committee has responsibility for overseeing the management of the security and governance risks to the University of Aberdeen's staff and students, its infrastructure and its information.
- **The Director of Digital and Information Services** has delegated responsibility for establishing and maintaining the University of Aberdeen's ISMS to ensure the availability, integrity and confidentiality of the University of Aberdeen's information. The Director of Digital and Information Services will lead on the definition and implementation of the University of Aberdeen's information security and governance arrangements and make judgement calls when situations arise that are not covered by the current information security management framework.
- **The Information Risk Working Group (IRWG)** is responsible for reviewing information governance and security risk, advising on risk treatment efforts and ensuring consistent implementation of this policy.
- **The Operational Security Group (OSG)** is an internal Digital and Information Services group responsible for compliance monitoring and improvements, information security maturity assessment, policy review and assessment of security risk and issues.
- **The Information Security Manager** is responsible for the development and improvement of the University Information Security posture.

5. Policy

The University manages information that is confidential or sensitive in nature, and information that is regarded as being available for general sharing. The University recognises that it is imperative that all information is protected from compromise of confidentiality, integrity and availability. All within the scope of this policy must comply with the following statements:

5.1. Information will be classified and protected in accordance with the University's classification scheme.

5.2. Processes, technology, services and facilities will be protected through information security controls as detailed in the ISMS.

5.3. Users will be made aware of the risks to information and how they should react to them through comprehensive awareness raising activities which will include formal training where appropriate. Specialist advice on information security will be made available throughout the University.

5.4. All individuals within scope of this policy should complete the relevant security awareness training.

5.5. Where a third-party provider is utilised for any services which involves contact with University information, an information security risk assessment is carried out to ensure they comply with the appropriate University's Information Security Policy and ISMS.

5.6. External testing and risk assessments are conducted on a regular basis to provide assurance that information security controls are fit for purpose and effective.

5.7. Appropriate security controls are in place for remote and offsite working.

5.8. Back-up and disaster recovery plans, processes and technology are in place to lower the risk of loss or destruction of information and/or services and to ensure that processes are in place to maintain availability of data and services.

5.9. All Information Systems will be designed, built and operated to appropriate technical standards to ensure the appropriate protection of information stored, processed, and transferred by them.

5.10. An Information Governance Committee, chaired by the Senior Vice-Principal and comprising senior University managers will ensure effective oversight, clear strategic direction and visible senior management support for information governance, information risk management and information security initiatives, across the University.

5.11. An Information Risk Working Group, comprising management representatives from all relevant parts of the University, will review information governance and security risk, advise on risk treatment efforts and ensure consistent implementation of this policy.

5.12. Information Security incident management processes will be defined to ensure that all Information Security incidents are identified, contained, eradicated, recovered, and recorded.

5.13. In respect of ensuring the security of the information it manages, the University will establish and maintain appropriate relationships with other organisations, law enforcement authorities, regulatory bodies, and service providers.

5.14. All individuals within scope of this policy must make reasonable effort to protect the University's digital assets from accidental or unauthorised disclosure, modification or destruction.

6. Legal & Regulatory Obligations

6.1. The University of Aberdeen has a responsibility to adhere to all current UK legislation and a variety of regulatory and contractual requirements such as:

- Computer Misuse Act 1990
- Investigatory Powers Act 2016
- Data Protection Act 2018 and UK General Data Protection Regulation
- Privacy and Electronic Communications (EC Directive) Regulations

6.2. The requirements of this legislation are reflected in this policy and the supporting policies, procedures and guidance. By adhering to these instructions, users will ensure that the University complies with its obligations.

7. Information Security Management System

7.1. The University ISMS comprises of this policy with supporting Policies, Guidelines, Standards and Procedures to elaborate and strengthen this policy statement. These, along with associated codes of practice, procedures, and guidelines are published together and are available for viewing on University of Aberdeen's Policy Zone.

7.2. All users and any third parties authorised to access University of Aberdeen's network or computing facilities are required to familiarise themselves with these Policies, Guidelines, Standards and Procedures and to adhere to them in the working environment.

7.3. Supporting documents in the ISMS will cover information security requirements in the following areas (not an exhaustive list):

- Conditions of using Information Systems
- Supplier and partner relationships
- Personnel security
- Operational security
- Information handling
- User and Access Management
- Security Architecture

- Systems Management
- Communications security
- System acquisition, development and maintenance
- Use of Personal Devices
- Cryptography
- Cyber Incident Response
- Physical and environmental security
- Remote Working
- Asset Management and Lifecycle
- Backup
- Disaster Recovery
- Vulnerability Management
- Mobile Devices

8. Compliance

8.1. The University of Aberdeen shall conduct information security and risk audit, compliance and assurance activities to ensure information security objectives and the requirements of this policy, IGC and agreed targets for The Scottish Government Cyber Resilience Framework are met.

8.2. The University of Aberdeen's Internal Audit function will undertake independent reviews of the implementation of the Information Security Policy and the supporting policies, Codes of Practice, Procedures and Guidelines.

8.3. Non-compliance with this policy will be treated extremely seriously by the University of Aberdeen and may result in enforcement action on a group and/or an individual.

9. Review

This policy and the ISMS are reviewed on at least an annual basis, or more frequently if required, to ensure they:

- Remain fit for purpose and accurate.
- Reflect changes in technologies.
- Are aligned to industry best practice.
- Support continued regulatory, contractual, and legal compliance.

Approval/Review History

Version	Date	Action
2	University Court, 25 March 2014	Approved
3	Operating Board, 6 March 2019	Approved
4.0	Information Governance Committee, 1st June 2020	Approved
4.1	Information Governance Committee, 2nd March 2021	Approved

Policy Metadata

Title	University of Aberdeen Information Security Policy
Author / Creator	Gary Fisher, Information Security Manager
Owner	Information Security Manager
Date published / approved	2nd March 2021
Version	V 4.1
Reviewed	March 2021
Date of next review	March 2022
Audience	All staff, students, partners, suppliers and contractors who work for or on behalf of the University
Related documents	Information Security Supporting Policies Data Protection Policy Records Management Policy
Subject / Description	A statement detailing that the University values the information entrusted to it and it will take appropriate measures to protect that information.
Document status	Policy
Equality Impact Assessment	N/A
Theme	Information Security Management
Keywords	Information Security, corporate, governance, data, information, risk, breach, security, employment, controls, compliance, access