UNIVERSITY OF ABERDEEN

INFORMATION SECURITY POLICY

1. Purpose

This policy outlines the University of Aberdeen's approach to Information Security Management. Together with the supporting Information Security Framework set out in section 7, this policy provides the guiding principles and responsibilities to ensure the University of Aberdeen's information security objectives are met so as to actively support the University's vision of "Transforming the world with greater knowledge and learning".

2. Scope

This policy and the Framework are applicable across the University of Aberdeen and individually applies to:

- All individuals who have access to the University of Aberdeen information and technologies (users).
- All facilities, technologies, and services that are used to process the University of Aberdeen information.
- Information processed, in any format including paper, by the University of Aberdeen pursuant to its operational activities.
- Internal and external processes that are used to store, transfer or process the University of Aberdeen information.
- External parties that provide information storage, transferal or processing services to the University of Aberdeen.

3. Objectives

This Policy and the Framework are designed to:

- Ensure that the information entrusted to the University is appropriately secured to protect it against the consequences of breaches of confidentiality, failures of integrity, or interruptions to the availability of that information.
- Establish a culture of being "security aware" across the University.
- Ensure controls and mitigations are appropriate by identifying and managing the information security threats and risks.
- Establish a clear governance structure for information security at the University.
- Clearly define the management responsibilities for maintaining information security.
- Actively assist in the compliance of legal, regulatory and contractual obligations in this area.

- Provide assurance to information owners, individual and organisational, both within and outside of the University that their information is appropriately protected.

4. Roles and responsibilities

The roles that carry responsibilities under this policy are as follows:

- **Users** at all levels are responsible for adhering to all relevant policies and making informed decisions to protect the information that they process. Users will 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.
- **Information Risk Owners** 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. Information Risk Owners may delegate responsibility for this.
- **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 risks to the University of Aberdeen's staff and students, its infrastructure and its information.
- **The Director of Digital and Information Services** is responsible for establishing and maintaining the University of Aberdeen's information security management framework 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 arrangements and make judgement calls when situations arise that are not covered by the current information security management framework.
- **Information Security Working Group** are responsible for providing support to line management so as to ensure a consistent implementation of policy across all University sections. This working group will also support the Information Governance Committee making recommendations and reporting to them.

5. Policy

a) The main categories of information managed by the University will be identified. For each category an Information, Risk Owner (or owners) will be appointed, at a level not below Director, who will be charged with ensuring the appropriate security of the information in their category. In addition information will be classified and protected in accordance with the University's classification scheme.

b) 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.

c) To determine the appropriate levels of security measures applied to information systems, a process of risk assessment will be carried out for each system; to identify the probability and impact of security failures.

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

e) To manage information security within the University, an Information Governance Committee, chaired by the Senior Vice Principal and comprising senior University managers, has been established. The objective of the committee shall be to ensure effective oversight, clear strategic direction and visible senior management support for information governance, information risk management and information security initiatives, across the University.

f) An Information Security Working Group, comprising management representatives from all relevant parts of the University, will devise and coordinate the implementation of information security controls.

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

h) 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.

6. Legal & Regulatory Obligations

The University of Aberdeen has a responsibility to abide by and adhere to all current UK and EU legislation, as well as a variety of regulatory and contractual requirements.
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. Supporting Policies, Codes of Practice, Procedures and Guidelines

Supporting policies will be developed to strengthen and reinforce 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.

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

Supporting documents will include:

a) **Conditions of using Information Systems.**
To help ensure that UoA IT Facilities can be used safely, lawfully and equitably.

b) **Supply Chain - Information Security.**
To maintain the security of the University' information and information facilities that are accessed, processed, communicated to or managed by external parties.

c) **Personnel - Information Security.**
To ensure that all employees, contractors, and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human error.

d) **Operations - Information Security.**
To prevent unauthorised physical access, damage and interference to the University's premises and information, and ensure the correct and secure operation of information processing facilities.

e) **Information Handling.**
To maintain the integrity and availability of information processing facilities, prevent loss, damage, theft, or compromise of assets, and interruption to the University's activities.

f) **User Management.**
To control access to information, ensure authorised user access, and prevent unauthorised access to information systems.

g) **Use of Computers.**
To maintain the integrity and availability of information and information processing facilities through appropriate access control.

h) **System Planning - Information Security.**
To minimise the risk if systems failures and prevent unauthorised physical access, damage and interference to the University's premises and information.

i) **Systems Management Information Security.**
To ensure the correct and secure operation of information processing facilities and maintain their security of application systems software and information.

j) **Network Management - Information Security.**
To ensure the protection of information in networks and the protection of supporting infrastructure.

k) **Software Management - Information Security.**
To protect the integrity and security of software and information.

l) **Working Away - Information Security.**
To ensure the security of information when information is access or processed away from University premises.

m) **Use of Personal Devices - Information Security.**
To ensure the security of information and facilities where use is made of personal or third party devices.

n) **Cryptography.**

To protect the confidentiality, authenticity and integrity of information by cryptographic means.

8. Compliance

The University of Aberdeen shall conduct information security compliance and assurance activities, facilitated by the University of Aberdeen's Information Security Team, to ensure information security objectives and the requirements of the policy are met. Wilful failure to comply with the policy will be treated extremely seriously by the University of Aberdeen and may result in enforcement action on a group and/or an individual.

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.

9. Review and Development

This policy, and supporting documentation, shall be reviewed and, if necessary, updated by The Director of Digital and Information Services and approved by The Information Governance Committee on an annual basis to ensure that they:

- Remain operationally fit for purpose.
- 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 Mar 2019	Approved

Policy Metadata

Title	Information Security Policy
Author / Creator	Garry Wardrope, IT Security Manager
Owner	IT Security Manager
Date published / approved	
Version	V 3.0
Reviewed	December 2018
Date of next review	
Audience	All staff, partners, suppliers and contractors who work for or on behalf of the University
Related documents	Data Protection Policy Records Management Policy Information Rights 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 Management
Keywords	Information Security, corporate, governance, data, information, risk, breach, security, employment, controls, compliance, access