UNIVERSITY OF ABERDEEN

INFORMATION SECURITY SUPPORTING POLICIES

1. Purpose

The purpose of these supporting policies is to augment the Information Security Policy, set out the University of Aberdeen's approach to Information Security Management and support the protection of University information and digital assets. It provides the guiding principles, requirements and responsibilities to ensure information security objectives are achieved and that data confidentiality, integrity and availability are preserved.

2. Scope

This policy 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 is 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 the management responsibilities for maintaining information security.
- Enable compliance with legal, regulatory and contractual obligations.

- Provide assurance to information owners, individual and organisational, 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. Supporting Policies

4.1. Supplier and partner relationships

Objective: To maintain the security of the University's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties. It is important for the University to understand, manage and reduce cyber security and data risk associated with supplier relationships.

- All third parties who are given access to the University's information systems, whether suppliers, customers, or otherwise, must be provided with, and agree to follow, the University's information security policies.
- The University will assess the risk to its information and, where deemed appropriate because of the confidentiality, sensitivity, or value of the information being disclosed or made accessible, the University will require external suppliers of services to sign a confidentiality agreement to protect its information assets.
- Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are compliant with the University's information security policies.
- All contracts with external suppliers for the supply of services to the University must be reviewed to ensure that information security and data governance requirements are being satisfied. Contracts must include appropriated provisions to ensure the continued security of information and systems if a contract is terminated or transferred to another supplier.

4.2. Personnel security

Objective: To ensure that all staff, contractors and third-party users are aware of information security threats, 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.

- All those in scope must comply with the University's information security policies.
- Any information security incidents resulting from intentional non-compliance may result in disciplinary action.

- The Terms and Conditions of Employment of the University include requirements to comply with information security policies.
- The University is committed to providing training to all users of new systems to ensure that their use is both efficient and does not compromise information security.
- All individuals within scope of this policy must complete the mandatory information security awareness training.
- Where staff change jobs, their information security needs must be reassessed, and any new training provided as a priority.
- Training in information security threats and safeguards for IT technical staff is mandatory, with the extent of technical training to reflect the job holder's individual responsibility for configuring and maintaining information security safeguards. Where IT staff change jobs, their information security needs must be reassessed, and any new training provided as a priority.
- The Information Security training, awareness and guidance program will be assessed for effectiveness and new requirements annually by the Information Security team.
- Upon notification of staff resignations, Line Management must consider whether the member of staff's continued system access rights constitutes an unacceptable risk to the University and, if so, revoke all access rights during the period of notice.
- Departing staff will have all system access revoked on day employment is terminated.
- Departing staff must return all information assets and equipment belonging to the University.

4.3. Operational security

Objective: To prevent unauthorized physical access, damage and interference to the University's premises and information and ensure the correct and secure operation of information processing facilities.

- Areas and offices where sensitive or critical information is processed will be given an appropriate level of physical security and access control. Staff with authorisation to enter such areas are to be provided with information on the potential security risks and the measures used to control them.

- The procedures for the operation and administration of the University's business systems and activities must be documented, with those procedures and documents being regularly reviewed and maintained.

- Duties and areas of responsibility will be segregated to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to the University.

- Procedures will be established and widely communicated for the reporting of security incidents and suspected security weaknesses in the University's business operations and information processing systems. Mechanisms will be in place to monitor and learn from those incidents.

- Procedures will be established for the reporting of software malfunctions and faults in the University's information processing systems. Faults and malfunctions will be logged and monitored, and timely corrective action taken.

- Changes to operational procedures must be controlled to ensure ongoing compliance with the requirements of information security and must have management approval.

- Development and testing facilities for business-critical systems will be separated from operational facilities, and the migration of software from development to operational status will be subject to formal change control procedures.

- Acceptance criteria for systems, upgrades and new versions, will be established and suitable tests of the system conducted prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place.

- Procedures will be established to control the development or implementation of all operational software. All systems developed for or within the University must follow a formalised development process.

- The security risks to the information assets of all system development projects will be assessed and access to those assets will be controlled.

- Security assessments and penetration testing will be conducted on a regular basis, at least annually and when there are major updates to critical systems processing sensitive data.

4.4. Information Handling

Objective: To maintain the integrity and availability of information and information processing facilities, and prevent loss, damage, theft or compromise of assets and interruption to the University’s activities.

- An inventory will be maintained of all the University's major information assets and the ownership of each asset will be clearly stated.

- Within the information inventory, each information asset will be classified according to sensitivity using the University's agreed information security classification scheme.

- It is the responsibility of individuals who have permission to access information to handle it appropriately to the assigned level of security classification.

- Classified information and outputs from systems handling classified data must be appropriately labelled according to the output medium.
- When permanently disposing of equipment containing storage media, all sensitive data and licensed software will be irretrievably deleted before the equipment is moved off site using procedures authorised by the Information Security Officer.
- Damaged storage devices containing sensitive data will undergo appropriate risk assessment, to determine if the device should be destroyed, repaired, or discarded. Such devices will remain the property of the University and only be removed from site with the permission of the information asset owner.
- This University advocates a clear desk and screen policy, particularly when employees are absent from their normal desk and/or outside normal working hours. In addition, screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons.
- Removal off site of the University's sensitive information assets, either printed or held on computer storage media, should be properly authorised by management. Prior to authorisation, a risk assessment based on the criticality of the information asset should be conducted.
- Information owners must ensure that appropriate backup and system recovery procedures are in place.
- Backup of the University's information assets and the ability to recover them is an important priority.
- Management is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business.
- The archiving of information and documents must take place with consideration for legal, regulatory, and business issues, with liaison between technical and business staff, and in keeping with the University's Retention Policy.
- Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.
- All users of information systems must manage the creation, storage, amendment, copying and deletion, or destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files. The degree to which software techniques and disciplined user procedures are necessary should be applied by management and determined by the classification of the information in question.

- Day to day data storage must ensure that current information is readily available to authorised users and that archives are both created and accessible in case of need.

- Highly sensitive or critical documents should not rely upon the availability or integrity of (external) data files over which the author may have no control. Key documents and reports should normally be self-contained and contain all the necessary information.

- Hard copies of sensitive or classified material must be protected and handled according to the distribution and authorisation levels specified for those documents.

- All employees to be aware of the risk of breaching confidentiality associated with the photocopying (or other duplication) of sensitive documents. Where documents are classified as Confidential or above, authorisation from the document owner should be obtained.

- All business-critical information used for or by the University, must be filed appropriately and according to its classification.

- All signatures authorising access to systems or release of information must be properly authenticated.

- All hardcopy documents of a sensitive or confidential nature are to be shredded, or similarly destroyed, when no longer required. The document owner must authorise or initiate this destruction.

- Any third party used for external disposal of the University's obsolete information bearing equipment or hardcopy material must be able to demonstrate compliance with this University's information security policies and, where appropriate, provide a service level agreement which documents the performance expected and the remedies available in case of non-compliance.

- Prior to sending sensitive information or documents to third parties, not only must the intended recipient be authorised to receive such information, but the procedures and information security measures adopted by the third party must also be seen to continue to assure the confidentiality and integrity of the information.

- Sensitive data or information may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be assured throughout the transfer.

- All parties are to be notified in advance whenever telephone conversations or videoconference events, such as lectures, are to be recorded.

- Recipient details must be checked carefully prior to dispatch, especially where the information content is sensitive or personal.

- The identity of recipients or requesters of sensitive or confidential information over the telephone must be verified and they must be authorised to receive it.
- When buying or selling goods or services, staff must use e-commerce systems in accordance with appropriate technical and procedural measures. Staff authorised to make payment by credit card for goods ordered over the telephone or internet, are responsible for safe and appropriate use.
- Important transaction and processing reports should be regularly reviewed by trained and qualified staff.
- Email should only be used for business purposes in a way which is consistent with other forms of business communication. The attachment of data files to an email is only permitted after confirming the sensitivity of the information being sent and then having scanned and verified the file for the possibility of a virus or other malicious code.
- Information received via email must be treated with care due to its inherent information security risks. File attachments should be scanned for viruses or other malicious code.

4.5. User and Access Management

Objective: To control access to information, ensure authorized user access, and prevent unauthorised access to information systems.

- Procedures for the registration and deregistration of users and for managing access to all information systems and data will be established to ensure that all access rights match their authorisations and are compliant with the principle of least privilege. These procedures will be implemented only by suitably trained and authorised staff.
- All users will have a unique identifier (user ID) for their personal and sole use for access to all the University's information services. The user ID must not be used by anyone else and associated passwords will not be shared with any other person for any reason.
- Password management procedures will be implemented to ensure the implementation of the requirements of the information security policies and to assist both staff and students in complying with best practice guidelines.
- Access control standards must be established for all information systems, at an appropriate level for each system, which minimises information security risks yet allows the University's business activities to be conducted without undue hindrance. A review period will be determined for each information system and access control standards will be reviewed regularly at those intervals.

- Access to all systems must be authorised by the manager responsible for the system and a record must be maintained of such authorisations, including the appropriate access rights or privileges granted.

- Procedures will be established for all information systems to ensure that user access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, staff changes their role, or staff or students leave the University. User access rights will be reviewed at regular intervals.

4.6. System acquisition, development and maintenance

Objective: To minimize the risk of systems failures and prevent unauthorized physical access, damage and interference to the University's premises and information.

- New information systems, or enhancements to existing systems, must be authorised by the manager(s) responsible for the information. The business requirements of all authorised systems must specify requirements for security controls.

- The implementation of new or upgraded software must be carefully planned and managed, to ensure that the information security risks associated with such changes are reduced using a combination of procedural and technical controls.

- The information assets associated with any proposed new or updated systems must be identified, classified and recorded, in accordance with the Information Handling Policy, and a risk assessment undertaken to identify the probability and impact of security failure.

- Equipment supporting business systems will be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment will be correctly maintained.

- Equipment supporting business systems will be given adequate protection from unauthorised access, environmental hazards and failures of electrical power or other utilities.

- Access controls for all information and information systems are to be set at appropriate levels in accordance with the value and classification of the information assets being protected.

- Access to operating system commands and application system functions is to be restricted to those persons who are authorised to perform systems administration or management functions. Where appropriate, use of such commands should be logged and monitored.

- Prior to acceptance, all new or upgraded systems must be evaluated to ensure that they comply with the University's information security policies, access

control standards and requirements for ongoing information security management.

- Cloud based services must comply with University information security requirements and be assessed on at least an annual basis.

4.7. Systems Management

Objective: To ensure the correct and secure operation of information processing facilities and maintain the security of application system software and information.

- Suitably trained and qualified staff will manage the University's systems to oversee their day to day running and to preserve security and integrity in collaboration with individual system owners. All systems management staff will be provided with relevant training in information security issues.

- Access controls will be maintained at appropriate levels for all systems by ongoing proactive management and any changes of access permissions must be authorised by the manager of the system or application. A record of access permissions granted must be maintained.

- Servers and end user devices must have appropriate malware and virus protections in place.

- Access to all information services will use a secure log on process and access to the University's business systems will also be limited by time of day or by the location of the initiating terminal or both. All access to information services is to be logged and monitored to identify potential misuse of systems or information.

- Password management procedures will be put into place to ensure the implementation of the requirement of the information security policies and to assist users in complying with best practice guidelines.

- Access to operating system commands is to be restricted to those persons who are authorised to perform systems administration or management functions. Use of such commands should be logged and monitored.

- The implementation of new or upgraded software must be carefully planned and managed. Formal change control procedures, with audit trails, will be used for all changes to systems. All changes must be evaluated and authorised before moving to the live environment.

- Capacity demands of systems supporting business processes will be monitored and projections of future capacity requirements made to enable adequate processing power, storage and network capacity to be made available.

- Security event logs, operational audit logs and error logs must be reviewed and managed by qualified staff.

- All systems default identities, secrets or passwords must be removed or changed.

- A secure standardised baseline build shall be developed for all device types, maintained, and reviewed periodically.
- All digital services and infrastructure will be designed in compliance with information security and resilience requirements.
- All digital services, infrastructure and processes will have design documentation which is maintained throughout the service lifecycle.
- System clocks must be regularly synchronised between the University's various processing platforms.

4.8. Network Security

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

- Suitably authorised and qualified staff will manage the University's network to oversee its day to day running and to preserve its security and integrity in collaboration with individual system owners. All network management staff will be provided with relevant training in information security issues.
- The network must be designed and configured to deliver high performance and reliability to meet the University's needs whilst providing a high degree of access control and a range of privilege restrictions.
- The network must be segregated into separate logical domains with routing and access controls operating between the domains. Appropriately configured firewalls will be used to protect the networks supporting the University's business systems.
- Access to the resources on the network must be strictly controlled to prevent unauthorised access, and access control procedures must provide adequate safeguards through robust identification and authentication techniques. Access to all computing and information systems and peripherals will be restricted unless explicitly authorised.
- Remote access to the network will be subject to robust authentication, and VPN (Virtual Private Network) connections to the network are only permitted for authorised users, ensuring that use is authenticated, and data is encrypted during transit across the network.
- Only approved remote access solutions, including those solely for support purposes, can be used. These must be reviewed on an annual basis by the Information Security team in collaboration with relevant teams, and there must be a method and process in place for detecting unauthorised solutions.

- The implementation of new or upgraded software or firmware must be carefully planned and managed. Formal change control procedures, with audit trails, will be used for all changes to critical systems or network components.

- All changes must be evaluated and authorised before moving to the live environment.

- Moves, changes, and other reconfigurations of users' network access points will only be conducted by staff authorised by IT Services according to procedures laid down by them.

- Networks and communication systems must all be configured and safeguarded against both physical attack and unauthorised intrusion.

4.9. Software Management

Objective: To protect the integrity and security of software and information.

- The University's business applications are to be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity in collaboration with nominated individual application owners. All business application staff will be given relevant training in information security issues.

- The procurement or implementation of new, or upgraded, software must be carefully planned and managed and any development for or by the University must always follow a formalised development process. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls.

- Business requirements for new software or enhancement of existing software will specify the requirements for information security controls.

- Formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to business software. All changes must be properly authorised and all software, including that which interacts with the amended software, must be tested before changes are moved to the live environment.

- Modifications to vendor supplied software is discouraged. Only strictly controlled essential changes will be permitted, and the development of interfacing software will only be undertaken in a planned and controlled manner.

- The implementation, use, or modification of all software on the University's business systems will be controlled.

5. Legal & Regulatory Obligations

5.1. 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 Regulations

5.2. 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.

6. Exceptions

Any exceptions to the requirements defined in this policy must be justified, risk assessed, documented and approved by the DDIS Senior Leadership Team or Information Security Manager in consultation with the data owner.

7. Compliance

7.1. Non-compliance with this policy could expose the University to accidental or deliberate misuse of information, breaches of confidentiality, malicious or accidental corruption of data, theft of intellectual property and a breach of statutory, regulatory and/or contractual requirements.

7.2. 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 and supporting policies, procedures and standards are met.

7.3. 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.

7.4 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.

8. Review

This policy is reviewed at least annually to ensure it:

- Remains fit for purpose and accurate.
- Reflects changes in technologies.
- Is aligned to industry best practice.
- Supports continued regulatory, contractual, and legal compliance.

Approval/Review History

Version	Date	Action
2	University Court 25 March 2014	Approved
2.1	Information Governance Committee, 2nd March 2021	Approved
2.2	Information Governance Committee, 6th April 2022	Approved
2.3	Information Governance Committee, 23rd March 2023	Approved
2.4	Information Governance Committee, 1 May 2024	Approved

Policy Metadata

Title	Information Security Supporting Policies
Author / Creator	Information Security Manager
Owner	Information Security Manager
Date published / approved	23 March 2023
Version	2.4
Reviewed	March 2024
Date of next review	March 2025
Audience	All staff, partners, suppliers and contractors who work for or on behalf of the University
Related documents	Information Security Policy Data Protection Policy Records Management Policy Information Rights Policy
Subject / Description	A statement detailing that the University values the information entrusted to it and will act appropriately 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