UNIVERSITY OF ABERDEEN

INFORMATION SECURITY SUPPORTING POLICIES

1. Introduction

In March 2019 a new revised University of Aberdeen Information Security Policy and Framework was approved and published by the University Operating Board. The Framework includes an overarching Information Security Policy and a number of Supporting Policies, Codes of Practice, Procedures and Guidelines.

Several of these supporting policies had previously been incorporated into the now superseded Information Security Policy. These supporting policies are in the process of being revised and re-published, until each policy is re-published, the original supporting policy remains in force and is published in this document.

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. Supporting Policies:

The Supporting Policies Codes of Practice, Procedures and Guidelines defined in the Information Security Policy are listed below, along with their status, either issued as a separate document, included in this document or scheduled for production.

a) **Conditions of using Information Systems.**
   Published as a separate document.

b) **Supply Chain - Information Security.**
   Included below.

c) **Personnel - Information Security.**
   Included below.

d) **Operations - Information Security.**
Included below.

e) **Information Handling.**
Included below.

f) **User Management.**
Included below.

g) **Use of Computers.**
Included below.

h) **System Planning - Information Security.**
Included below.

i) **Systems Management Information Security.**
Included below.

j) **Network Management - Information Security.**
Included below.

k) **Software Management - Information Security.**
Included below.

l) **Working Away - Information Security.**
Scheduled for production.

m) **Use of Personal Devices - Information Security.**
Scheduled for production.

n) **Cryptography.**
Included below.

4. Supporting Policies

Numbering of this section is the same as the list above and in the Information Security policy, only these sections listed as "included" are here.

b) Supply Chain – Information Security Policy

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.

i. All third parties who are given access to the University's information systems, whether suppliers, customers, or otherwise, must agree to follow the University's information security policies. A summary of the information security policies and the third party's role in ensuring compliance will be provided to any such third party, prior to their being granted access.

ii. 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.

iii. Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the content and spirit of the University's information security policies.

iv. All contracts with external suppliers for the supply of services to the University must be reviewed to ensure that information security requirements are being satisfied. Contracts must include appropriated provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.

c) Personnel – Information Security Policy

Objective:

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.

i. Terms and conditions

1. All employees must comply with the University's information security policies.

2. Any information security incidents resulting from non-compliance may result in disciplinary action.

3. The Terms and Conditions of Employment of the University include requirements to comply with information security policies.

ii. Training and awareness

1. A summary of the information security policies must be formally delivered to any external contractor, prior to any supply of services.

2. A summary of the information security policies must be formally delivered to, and accepted by, all temporary staff, prior to their starting any work for the University.

3. 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.

4. All staff will receive mandatory information security awareness training. Where staff change jobs, their information security needs must be reassessed and any new training provided as a priority.

5. 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.

iii. Disaffected and departing staff

1. 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.

2. Departing staff will have all system access revoked on day employment is terminated, unless otherwise agreed.

3. Departing staff must return all information assets and equipment belonging to the University, unless agreed otherwise with the designated owner responsible for the information asset.

d) Operations – Information Security Policy

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.

i. 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.

ii. 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.

iii. 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.

iv. 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.

v. 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.

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

vii. 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.

viii. Acceptance criteria for new information systems, upgrades and new versions, will be established and suitable tests of the system carried out 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.

ix. 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.

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

e) 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.

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

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

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

iv. Classified information and outputs from systems handling classified data must be appropriately labelled according to the output medium.

v. 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.

vi. 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.

vii. 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.

viii. 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 carried out.

ix. Information owners must ensure that appropriate backup and system recovery procedures are in place.

x. Backup of the University's information assets and the ability to recover them is an important priority.

xi. Management is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business.

xii. The archiving of information and documents must take place with due consideration for legal, regulatory, and business issues, with liaison between technical and business staff, and in keeping with the University's Retention Policy.

xiii. 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.

xiv. 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.

xv. 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.

xvi. 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.

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

xviii. 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.

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

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

xxi. 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.

xxii. 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 also, where appropriate, provide a service level agreement which documents the performance expected and the remedies available in case of non-compliance.

xxiii. 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.

xxiv. 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 reasonably assured throughout the transfer.

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

xxvi. Email addresses and faxes should be checked carefully prior to dispatch, especially where the information content is sensitive; and where the disclosure of email addresses or other contact information, to the recipients is a possibility.

xxvii. Unsolicited or unexpected faxes should be treated with great care until the sender has been identified.

xxviii. 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.

xxix. 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.

xxx. Important transaction and processing reports should be regularly reviewed by properly trained and qualified staff.

xxxi. 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.

xxxii. Information received via email must be treated with care due to its inherent information security risks. File attachments should be scanned for possible viruses or other malicious code.

f) User Management

Objective:

To control access to information, ensure authorized user access, and prevent unauthorized access to information systems.

i. Procedures for the registration and deregistration of users and for managing access to all information systems will be established to ensure that all users' access rights match their authorisations. These procedures will be implemented only by suitably trained and authorised staff.

ii. 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.

iii. Password management procedures will be put into place 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.

iv. 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 carried out without undue hindrance. A review period will be determined for each information system and access control standards will be reviewed regularly at those intervals.

v. 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.

vi. Procedures will be established for all information systems to ensure that users' 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. Users' access rights will be reviewed at regular intervals.

g) Use of Computers

Objective:

To maintain the integrity and availability of information and information processing facilities through appropriate access control.

i. All users will have a unique identifier (user ID) for their personal and sole use for access to all computing 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.

ii. The selection of passwords, their use and management must adhere to University best practice guidelines.

iii. Equipment must be safeguarded appropriately – especially when left unattended.

iv. Files downloaded from the internet, including mobile code and files attached to electronic mail, must be treated with the utmost care to safeguard against both malicious code and inappropriate material. Such files, or any others not known to come from a trusted source, must be scanned for possible malicious code before being opened.

v. Electronic mail must not be used to communicate confidential or sensitive information unless appropriate measures have been taken to ensure authenticity and confidentiality, that it is correctly addressed, and that the recipients are authorised to receive it.

vi. Any essential information stored on a laptop or on a PC's local disk must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis.

vii. Sensitive or confidential data should only be accessed from equipment in secure locations and files must never be printed on a networked printer that does not have adequate protection or security.

viii. Utmost care must be used when transporting files on removable media (e.g. disks, CDROMs and USB flash drives) to ensure that valid files are not overwritten or incorrect or out of date information is not imported.

ix. Employees are not permitted to load unlicensed software onto the University's PCs, laptops and workstations.

h) System Planning – Information Security Policy

Objective:

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

i. 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.

ii. 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 mitigated using a combination of procedural and technical controls.

iii. 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.

iv. 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.

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

vi. 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.

vii. 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.

viii. Prior to acceptance, all new or upgraded systems will be tested to ensure that they comply with the University's information security policies, access control standards and requirements for ongoing information security management.

i) Systems Management - Information Security Policy

Objective:

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

i. The University's systems will be managed by suitably trained and qualified staff 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 given relevant training in information security issues.

ii. 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.

iii. 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.

iv. 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.

v. 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.

vi. 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 properly tested and authorised before moving to the live environment.

vii. 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.

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

ix. System clocks must be regularly synchronised between the University's various processing platforms.

j) Network Management – Information Security Policy

Objective:

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

i. The University's network will be managed by suitably authorised and qualified staff 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 given relevant training in information security issues.

ii. 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.

iii. 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.

iv. 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.

v. 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.

vi. 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.

vii. All changes must be properly tested and authorised before moving to the live environment.

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

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

k) Software Management – Information Security Policy

Objective:

To protect the integrity and security of software and information.

i. 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.

ii. 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.

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

iv. 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.

v. Modifications to vendor supplied software will be 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.

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

n) Cryptography

Objective:

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

i. A policy on cryptographic controls will be developed with procedures to provide appropriate levels of protection to sensitive information whilst ensuring compliance with statutory, regulatory and contractual requirements.

ii. Confidential information will only be taken for use away from the University in an encrypted form unless its confidentiality can otherwise be assured.

iii. Encryption will be used whenever appropriate on all remote access connections to the University's network and resources.

Title	Information Security Supporting Policies
Author / Creator	Garry Wardrope, IT Security Manager
Owner	IT Security Manager
Date approved	Court - 25 March 2014
Date published	April 2019
Action	Extracted from version 2 of Information Security Policy
Version	Version 1.0
Date for Next Review	April 2020
Audience	All staff, partners, suppliers and contractors who work for or on behalf of the University.
Related	Data Protection Policy Records Management Policy Information Security 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.
Equality Impact Assessment	N/A
Theme	Information Management

Keywords	Information security, corporate, governance, data, information, risk, breach, security, employment, controls, compliance, access

Policy Zone Template - Metadata fields with explanatory notes

Title	Information Security Supporting Policies
Author / Creator	Garry Wardrope, IT Security Manager
Owner	IT Security Manager
Date approved	Court - 25 March 2014
Date published	April 2019
Action	Extracted from version 2 of Information Security Policy
Version	Version 1.0
Date for Next Review	April 2020
Audience	All staff, partners, suppliers and contractors who work for or on behalf of the University.
Related	Data Protection Policy Records Management Policy Information Security 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.
Equality Impact Assessment	N/A
Theme	Information Management
Keywords	Information security, corporate, governance, data, information, risk, breach, security, employment, controls, compliance, access