UNIVERSITY OF ABERDEEN

CRYPTOGRAPHIC POLICY

1. Purpose

Information is an asset and access to it must be managed with care to ensure that confidentiality, integrity and availability are maintained. Encryption of information and devices helps mitigate the risk of unauthorised interception, disclosure and access.

This policy outlines University of Aberdeen's approach to Cryptographic controls and management and provides the guiding principles and responsibilities to ensure University of Aberdeen's information security and governance objectives are met.

2. Scope

This policy applies to:

- All individuals who have access to the University of Aberdeen information 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 whether owned or managed and is applicable to all staff, students and visitors.
- 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 is designed to:

- Protect the confidentiality, integrity and availability of University digital assets, services and data.
- Ensure University of Aberdeen information is appropriately protected from theft or accidental loss of the device on which it is stored.
- Ensure University of Aberdeen information is appropriately protected when it is being transferred from system to system.
- Support secure information sharing and collaboration.
- Observe the key themes of the Cyber Resilience Framework: Identify, Protect, Detect, Respond and Recover.

- Establish minimum standards and responsibilities for the encryption of University digital assets.
- Ensure that the University manages encryption in a consistent and appropriate manner.
- Reduce information related risk to acceptable levels.
- 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

- **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.
- **Heads of Schools and Directors of Professional Services** are accountable for the effective implementation of this policy 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 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

5.1. Protecting data at rest - encrypting data while it is stored provides effective protection against unauthorised access and theft. Encryption must be used to protect University of Aberdeen digital data at rest by default. Any deviation from this policy must be carefully assessed and follow the guidance detailed in section 6 of this policy. Options for encryptions of data at rest include:

- Full disk encryption
- File encryption
- Application encryption
- Database encryption

5.2. All University owned devices, or any personal device used for storing University information, must have full disk encryption enabled by default.

5.3. Protecting data in transit - encrypting data while in transit provides effective protection against unauthorised interception and access. Encryption must be used to protect University of Aberdeen digital data in transit by default. Any deviation from this policy must be carefully assessed and follow the guidance detailed in section 6 of this policy.

5.4. It is important to recognise that even with encryption in place there is residual risk that sophisticated hacking and decryption methods can still be used to access encrypted files and information. Secure data handling procedures should always be followed for sensitive and confidential information even whilst that information is encrypted.

5.5. Encryption must be implemented using approved methods and technologies. Superseded or insecure protocols and cipher suites should not be used unless there is an approved exception in place. Systems, infrastructure, applications and services must be configured to only accept connections that comply with this requirement.

5.6. Encryption algorithms and specific implementations of algorithms can contain vulnerabilities. The use of algorithms and encryption software must be monitored and managed.

5.7. Cryptographic keys must be generated, stored and managed in a secure manner that prevents loss, theft, or compromise. Keys need to be communicated by reliable and secure methods and kept confidential. Separate channels should be used for key and data transfer. Under no circumstances should the key and encrypted data be transferred together via the same medium. There must be procedures and controls in place for certificate revocation in the event of compromise or expiry.

6. Exceptions

Any exceptions to the requirements defined in this policy must be justified, documented and approved following a risk assessment by the Information Security Manager.

7. Legal & Regulatory Obligations

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

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

7.2. 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.

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 ISMS 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 and Development

This policy is reviewed on at least an annual basis 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
1.0	Director DDIS September 2019	Approved
2.0	Information Governance Committee, August 2020	Approved

Policy Metadata

Title	Cryptographic Policy
Author / Creator	Gary Fisher, Information Security Manager
Owner	Information Security Manager
Date published / approved	12th August 2020
Version	V 2.0
Reviewed	August 2020
Date of next review	August 2021
Audience	All staff, students, partners, suppliers and contractors who work for or on behalf of the University
Related documents	Information Security Policy Data Protection Policy
Subject / Description	Cryptographic requirements
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, cryptography, encryption