# 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. The University of Aberdeen uses encryption to secure information and data while stored, processed and handled, protect user credentials and enable secure communications.

This policy outlines University of Aberdeen's approach to cryptographic controls, management, and provides the requirements and responsibilities to ensure information security and data governance objectives are met.

## 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:

- Reduce information related risk to appropriate and acceptable levels.
- Protect the confidentiality, integrity and availability of University of Aberdeen 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 digital assets.
- Ensure that encryption is managed in a consistent and appropriate manner.
- Provide assurance to IGC, senior management, information owners, individuals and organisations 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 (IGC)** 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 a Digital and Information Services (DIS) group responsible for compliance monitoring and improvements, information security maturity assessment, policy review, assessment of security risk and implementation of risk treatment plans. DIS technical service owners and managers are responsible for the deployment and configuration of digital services and systems.
- **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. Options for encryption of data at rest include:

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

5.2. All University owned devices and storage systems must have full disk encryption enabled and, where possible, monitoring must be in place to ensure this continues to be enabled and effective.

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.

5.4. Protecting data copied to external devices – all data copied to external or removable storage devices must be encrypted.

5.5. Encryption must be implemented using approved methods and technologies. Encryption standards, algorithms, protocols, key length, cipher suites must meet current acceptable standards as defined in the University of Aberdeen Cryptographic standard. Systems, infrastructure, applications and services must be configured to only accept connections that comply with this requirement.

5.6. Unsupported ciphers, protocols and algorithms must be disabled where possible. Superseded or insecure protocols and cipher suites should not be used unless there is an approved exception in place.

5.7. Encryption algorithms and specific implementations of algorithms can contain vulnerabilities. The use of algorithms and encryption software must be monitored and managed through the vulnerability management process.

5.8. Cryptographic keys must be generated, stored and managed in a secure manner that prevents loss, theft, or compromise.

5.9. Access to cryptographic keys must be restricted to authorised individuals.

5.10. Cryptographic keys must be transmitted by reliable and secure methods to maintain confidentiality and integrity. Separate communication 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.

5.11. There must be procedures and controls in place for key or certificate revocation in the event of compromise or expiry.

5.12. It is important to recognise that even with encryption in place there is residual risk to the confidentiality of data. Therefore, secure data handling procedures, as described in section 4.4 of Information Security Supporting Policies, should always be followed for sensitive and confidential information even whilst that information is encrypted.

## 6. Exceptions

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

## 7. Legal & Regulatory Obligations

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

- 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

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. Noncompliance 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.

8.2. 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 policy are met. This right will be exercised across all University owned and operated networks, devices connected to these networks and hosted systems that store University data.

8.3. Audit reports and any non-compliance will be presented to IGC as the body with executive responsibility for information governance and security within the University.

8.4. 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.

8.5. 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.

## 10. Glossary

| Term | Definition |
|---|---|
| **Application encryption** | Encryption of files or fields of data at the application level. |
| **Certificate revocation** | A process in which a certificate is deemed invalid before the end of its lifecycle. |
| **Ciphertext** | Encrypted data transformed from plaintext using an encryption algorithm |
| **Cipher suites** | A set of algorithms that help secure a network connection. |
| **Cryptography** | The science of protecting information by transforming it into a secure format. |
| **Cryptographic keys** | A string of data that is used to lock or unlock encrypted data. |
| **Database encryption** | Encryption of data types, fields or entire dataset at the database level. |
| **Data at rest** | Data that is stored on a hard drive or other media and not actively moving from device to device or over a network. |
| **Data in transit** | Data that is in motion and being transmitted across a network between devices. |
| **Encryption** | The process of converting data to an unrecognisable format, called ciphertext, so that only authorised parties can view it. |
| **Encryption algorithms** | The method used to transform data into ciphertext. An algorithm will use the encryption key to alter the data in a predictable way, so that even though the encrypted data will appear random, it can be turned back into plaintext by using the decryption key |

| | |
|---|---|
| **Full disk encryption** | A cryptographic method that applies encryption to the entire hard drive including data, files, the operating system and software programs. |
| **File encryption** | A method which encrypts individual files. |
| **Plaintext** | Unencrypted data. |

Approval/Review History

| Version | Date | Action |
|---|---|---|
| 1.0 | Director DDIS September 2019 | Approved |
| 2.0 | Information Governance Committee, August 2020 | Approved |
| 2.1 | Information Governance Committee, March 2021 | Approved |
| 2.2 | Information Governance Committee, March 2022 | Approved |
| 2.3 | Information Governance Committee, March 2023 | Approved |
| 2.4 | Information Governance Committee, May 2024 | Approved |

Policy Metadata

| | |
|---|---|
| Title | Cryptographic Policy |
| 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, students, partners, suppliers and contractors who work for or on behalf of the University |
| Related documents | Information Security Policy<br>Data Protection Policy<br>Cryptographic standard |
| 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 |