# Information Security Policy

# Cryptography

This Policy states the Company's intent to use cryptography to protect the confidentiality, integrity and authenticity of sensitive or confidential information and sets out how information should be protected by encryption when it is being accessed, transferred or stored.

**Objectives**

To protect the confidentiality, authenticity or integrity of information by the use of cryptography.

To avoid breaches of the Data Protection Act and other statutory, regulatory or contractual obligations.

**Scope**

This policy applies to Directors and managers with responsibility for the provision of information systems and staff who handle sensitive information through employment. It also applies to third parties who handle sensitive information on behalf of the Company.

Sensitive information comprises information assets that are classified as Confidential or Strictly Confidential under the Information Handling Policy and all instances of Protected Personal Information.

This policy applies to sensitive information held on approved Company systems.

**Policy**

Cryptographic controls shall be applied according to the sensitivity of the data as defined in the Information Handling Policy.

Sensitive information in electronic form shall only be physically taken for use away from the Company in an encrypted form, unless its confidentiality can otherwise be assured.

- Procedures shall be established to ensure that authorised staff may gain access, when needed, to any important business information being held in encrypted form.
- The confidentiality of sensitive information being stored on systems outside the Company, or transferred on portable media or across networks must be protected by use of appropriate encryption techniques.
- Encryption shall be used whenever appropriate on all remote access connections to the Company's network and resources that have the potential to transfer sensitive information (particularly credentials).

- A procedure for the management of electronic keys, to control both the encryption and decryption of sensitive documents or digital signatures, shall be established.
- Important business information being communicated electronically shall be authenticated by the use of digital signatures; information received without a digital signature shall not be relied upon.

5 **Related Policies**

5.1 This policy should be read alongside the Information Handling Policy and other documents within the Company's IT Security Policy.

Signed Dr Adnan Niazi

Date 4/1/2021
Last Reviewed On 05/07/24

Version 1