

Cryptography Security Policy

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

Introduction and Scope

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.

This policy applies to 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 restricted or secret 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.

Related Policies

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

Policy Review and Assessment

This policy may be amended by Interr at any time in order to take into account changes in legislation and best practice. This policy was last reviewed and agreed by the Board and seeks to be reviewed and updated annually. Any queries arising regarding this policy should be addressed to Mick Tabori.



Mick Tabori - CEO
January 2023