CRYPTOGRAPHIC CONTROLS POLICY

Policy Statement

This Policy defines the ways in which the confidentiality, integrity and availability of AzteQ Group Ltd's information are protected by applying an appropriate level of cryptographic control.

Scope

The scope of this Policy applies to all AzteQ Group Ltd's employees. All such employees are obliged to adhere to this and any other Information Security Policy. Failure to comply with this Policy may be regarded as a disciplinary matter and will be dealt with in line with the Organisation's disciplinary policy with possible sanctions up to and including summary dismissal (or termination of contract for temporary workers).

The Policy applies to all electronic data which is either:

1. Owned by AzteQ Group Ltd
2. Temporarily in the possession of AzteQ Group Ltd, e.g. clients and which can be regarded as critical or sensitive, where:
3. Critical is defined as relating to information which is of commercial, strategic or significant monetary value to AzteQ Group Ltd
4. Sensitive is defined as relating to information which would either contravene the Data Protection Act, or cause measurable damage to AzteQ Group Ltd's reputation or that of its clients, or other stakeholders if it were to fall into the public domain.

Objectives

To ensure AzteQ Group Ltd's permanent and temporary employees are aware of their responsibilities in:

1. The protection of electronic data within the scope defined above
2. The protection of AzteQ Group Ltd reputation.

To provide high-level guidance on the appropriate use of cryptographic controls.

Principles

1. This Policy exists to set out the principles and requirements for the use of cryptographic controls.
2. AzteQ Group Ltd's information system resources are important business assets that are vulnerable to access by unauthorised individuals or unauthorised remote electronic processes. Sufficient precautions are required to prevent unwanted access by applying a level of encryption to critical and sensitive data which is proportionate to the business risk.

General

1. All critical or sensitive data transferred outside AzteQ Group Ltd is encrypted.
2. All removable media, including memory sticks, is encrypted.
3. Laptop hard drives are whole-disk encrypted utilising a 2048-bit encryption key for any laptops which leave AzteQ Group Ltd premises.
4. All remote access is to take place via an encrypted VPN or an equally secure alternative.
5. WPA2 encryption is mandatory for all wireless networks carrying AzteQ Group Ltd data (including domestic networks where remote working is undertaken).
6. E-mails must be encrypted by using FIPS 140-2 encryption mechanism or similar whenever sensitive or critical data is included or attached.

Client access to web-based applications is encrypted using at least a 128-bit SSL certificate.

Encryption according to classification

1. All information marked 'Client Confidential' or 'AzteQ Group Ltd Confidential' is to be regarded as sensitive or critical within the context of this Policy.
2. Information not marked 'Client Confidential' or 'AzteQ Group Ltd Confidential' should still be considered for encryption if it falls within the definitions of sensitive or critical data outlined within the Scope of this Policy.

Encryption of data in transit

1. Sensitive or critical data in transit must always be encrypted.
2. Data which is already in the public domain (or would be of no adverse significance if it were to be so) may be sent unencrypted.

Key Management

At the discretion of the CEO, a key management system will be implemented if the volume of encryption keys reaches such a level as to require this.

Roles and Responsibilities

All individuals are responsible for ensuring that sensitive or critical data is encrypted before leaving AzteQ Group Ltd premises.

Encryption for data exported outside the UK

Regulatory controls for any country to which data is exported outside the UK are checked to ensure that cryptographic legislation will not be contravened.

Avoiding adverse impacts from encryption

1. Where necessary, encryption keys are securely managed in a central location such that all information encrypted by AzteQ Group Ltd can be decrypted if required.
2. Should a client request that sensitive or critical information be sent unencrypted, an indemnity opt-out letter (or e-mail) must be sent to the client before the transfer of data is made.

User awareness

This Policy will be drawn to the attention of all AzteQ Group Ltd's staff.

Compliance

ISO 27002: Clause 10.1.1 (Policy on the Use of Cryptographic Controls)

Responsibility for implementation

ISMS Manager

Revision

This Policy will be reviewed and revised in **(date of review)** or at such earlier time as operational requirements demand.

Policy Sign-off

Date of Issue:	27/10/2020
Date of Next Review:	15/09/2021
Name:	Tim Barber
Signed:	

Amendment History

Version	Modified On	Modified By	Comments
1.0	15/09/2020	Jo Holloway	
2.0	27/10/2020	Jo Holloway	Updating dates