[Company]

CRYPTOGRAPHIC CONTROL AND ENCRYPTION POLICY

Management and use of encryption

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Cryptographic Control Policy

3.1 Purpose

The purpose of this policy is to ensure the proper and effective use of encryption to protect the confidentiality and integrity of confidential information.

3.2 Scope

Confidential and personal information processed, stored, or transmitted on or in company owned, managed, and controlled systems and applications deemed in scope by the ISO 27001 scope statement.

All employees and third-party users.

3.3 Principle

Information is protected by controls based on classification as set out in the Information Classification and Handling Policy and based on risk assessment.

Only company approved encryption technology and processes are used.

The export of encryption technologies or encrypted data may be restricted by regulation. Personnel will seek guidance from the legal department should export of cryptographic technologies or encrypted data be required.

3.4 Encryption Algorithm Requirement's

Symmetric encryption: AES-256bit

Asymmetric encryption: RSA (2048 bit recommended, at least 1200 bits required).

Hash functions: SHA2 (four sizes, 256 bits is recommended).

Digital signatures: RSA (2048 bit recommended, at least 1200 bits is required).

3.5 Mobile, Laptop and Removable Media Encryption

Mobile devices, laptops and removable media are having disk encryption implemented at either the hardware and / or operating system level propriety to the manufacturer.

Device encryption must never be disabled.

Access to encrypted storage on mobile devices must be protected by a password, passphrase, PIN, or other authentication mechanism.

Where generic passwords are used to access encrypted storage, a secondary unique login, must be in place to access the device itself.

Only company owned and provided removable media encrypted devices may be used to store confidential data.

3.6 Email Encryption

Email is / is not encrypted by default using x, y, z implementation.

Email should not be used to transfer confidential or personal data in an unencrypted format in line with the Information Transfer Policy.

Where required, an encrypted file should be attached with a key length that meets the Encryption Algorithm Requirements.

3.7 Web / Cloud Services Encryption

Web and cloud services that require the exchange of confidential, personal, or sensitive data must implement TLS 1.2 at a minimum to protect the data in transit over the internet.

All servers must have a valid certificate issued by a recognised Certificate Authority. It is the System Owner's responsibility to renew the certificate and ensure that the systems are updated.

3.8 Wireless Encryption

WEP must not be used as a security control for wireless networks.

WPA or WPA2 Enterprise mode with 802.1X authentication and AES encryption is implemented for WLAN networks.

Centralized management systems that can control and configure distributed wireless networks are implemented.

If required, it is recommended that WPA2 Personal mode be used with a minimum 13-character random passphrase and AES encryption.

3.9 Card Holder Data Encryption

Store secret and private keys always used to encrypt/decrypt cardholder data in one (or more) of the following forms:

- Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key
- Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device)
- As at least two full-length key components or key shares, in accordance with an industry-accepted method

Note: It is not required that public keys be stored in one of these forms.

3.10 Backup Encryption

Backups are encrypted using the manufacture propriety back up technology.

3.11 Database Encryption

Database containing confidential information or personal data are encrypted at rest at either the Database Application Layer or the Disk Layer.

3.12 Data in Motion Encryption

The Data Handling Procedures require the transfer of confidential and personal information through a secure channel. A secure channel is an encrypted network connection.

Various methods of encryption are available and generally built-into the application. The user should be aware of the data connection being used to transmit sensitive data and if encryption is enabled for that connection.

Encryption is required for

- The transport of sensitive files (SSL or SCP usage to encrypt sensitive data for network file access of unencrypted files).
- All network traffic for remote access to the virtual desktop environment
- Transport of sensitive data that is part of a database query or web service call (examples SQL query to retrieve or send data from database or a web service call to retrieve or send data from a cloud application).
- Privileged access to network or server equipment for system management purposes, i.e., SSH

3.13 Bluetooth Encryption

Bluetooth is not approved as a communication method for unencrypted confidential, personal, or otherwise sensitive data.

See the Information Transfer Policy for the use of Bluetooth.

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.