Cryptographic & Key Management Policy

Contents

1. Introduction

Information is a valuable 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 disclosure and tampering. It also ensures that access to Company assets is only granted to those with authorisation.

The General Data Protection Regulations (GDPR) and The Data Protection Act 2018 requires the Company to implement appropriate technical and organisational measures to ensure that personal data is processed securely. Article 32 of the GDPR includes encryption as an example of an appropriate technical measure. Encryption is a widely available measure with relatively low costs of implementation and helps to ensure that appropriate controls are used. The Information Commissioner's Office (ICO) has considered encryption to be an 'appropriate technical measure' for a number of years. In cases where data has been lost or unlawfully accessed and encryption has not been used, the ICO will consider taking appropriate regulatory action.

This policy sets out the principles and rules relating to when and how Company assets should be encrypted.

2. Scope

The policy covers the application of encryption to all Company assets, including but not limited to:

- All laptop and desktop devices used for Company purposes.
- All removable and mobile devices (i.e., USB drives, Mobile Phones, Tablets, etc.).
- Data and information classified as sensitive/PII.
- Services used to access and those included within the Company Network (Network Traffic/Infrastructure, Data Centres, VPN, Wi-Fi, etc.).
- Network and web-based services including email.

3. Objectives

The purpose of this policy is to establish specific minimum standards and responsibilities for the encryption of Company and personal assets that access or process Company Information. This policy is designed to ensure that the Company manages encryption in a consistent manner and to appropriately safeguard access to all Company assets.

4. Responsibilities

It is the responsibility of asset owners and users to ensure that relevant devices, data, and information is encrypted using approved Company methods.

5. Policy Statements

Encryption must be used to protect data at rest and in transit by default. Although exemptions may be granted, they must be carefully assessed against the risk, any compensating controls and must be properly authorised as described in Policy Compliance.

6. Data at rest:

a) All Company owned devices must have full disk encryption (Bitlocker) enabled. This shall be part of the MS Intune policy.
b) Any personal devices such as smartphones that are used to access company data (including company emails) must have encryption and password access enabled.

7. Data in Transit:

a) When Company information is transmitted outside secure Company systems, it shall be encrypted in transit. Encryption in transit may include sharing a file/folder using SharePoint, encrypting a file sent via email, encrypting a portable hard disk being used to transfer data or through the use of encrypted transmission protocols such as TLS. Please refer to Information Security Policy for more information on procedures.

8. Implementation of Encryption:

a) Encryption must be implemented using approved methods and technologies.
b) Encryption employed on desktop and laptop computers must allow for a random cryptographic key to be generated and for the relevant key to be stored in Active Directory (AD). During the build process for desktops and laptops, processes must be in place to check the make and model of computers to verify they have a Trusted Platform Module (TPM) chip on board. If the TPM chip is available, the build process should enable the TPM function and start the encryption process. All desktop and laptop computers must be updated with the latest security and OS patches as these updates may include security patches to flaws or vulnerabilities discovered in the encryption software.
c) Mobile Devices - All Company provided mobile phones must be configured to force the use of a pin code lock which includes a minimum of six characters. While the use of a PIN alone to secure a mobile phone does not constitute encryption, it does play a vital role in supporting mobile device encryption. Company data should not be held on a mobile phone or any other mobile device.
d) Portable Storage Media – The use of PSM is discouraged and permission must be granted by either the IT Director or DPO. Where required, the Company provides encrypted USB data sticks. These storage devices are for the temporary storage of data only. The Company would only allow the use of USB data sticks (and similar storage devices) under the following conditions: Users must set a password for accessing the

device. See IS Policy. The password for encrypted, portable devices must be in accordance with the Company password policy.

e) The Company shall use MS Intune as part of the implementation and on-going management of this Policy.
f) Sensitivity Labels in MS Office shall be adopted and the corresponding encryption enforced. Staff & Participant Confidential labels shall be applied for files containing PII (see Classification Policy).
g) To meet the necessary encryption levels Participant Confidential documents that are required to be transferred to a 3rd party shall be transferred via a clients SFTP or the use of the company SharePoint (SHARING-DIRECTORY). In addition, it is best practice to apply a secure password (see Password Policy) to documents of a Staff or Participant level of sensitivity as part of the transfer process.
h) The company encourages documents with a sensitivity of staff confidential to also be shared with a 3rd party using SFTP or the Company SharePoint.
i) In addition, it is best practice to apply a secure password (see Password Policy) to documents of a Staff or Participant level of sensitivity as part of the transfer process.
j) Business Confidential information can be shared securely by email although the Company encourages the user of the Company SharePoint directory.

9. Cryptographic Keys

Cryptographic keys are required to access data and systems which utilise encryption. The Company takes the following approach in the management of these keys:

a) Cryptographic keys will be stored with MS Azure Active Directory (AD).
b) Access to cryptographic keys in Active Directory must be restricted to authorised staff with administration rights only (and the Company's IT support company).
c) Procedures must be in place to ensure that requests for cryptographic keys can be appropriately authorised, provided in a timely manner and appropriately recorded.
d) If a cryptographic key is provided for recovering access to a computer, the existing key must be revoked, and a new key must be generated to prevent data leakage and use of such keys is recorded.
e) Cryptographic keys must be securely managed and protected though their whole lifecycle. This includes protection against modification, loss, unauthorised access/use, or disclosure.
f) Cryptographic algorithms, key lengths and use must be in accordance with all relevant Company policies, procedures and in accordance with professional best practices.
g) Equipment used to generate, store and archive keys must be physically protected using appropriate, secure access controls.
h) Awareness of encryption/decryption passwords for devices, media or systems must be limited to authorised personnel only.
i) In the event of a cryptographic key being compromised, the existing key must be revoked, and a new key (or key pair) must be generated.

N.B. The loss of a decryption key could cause data to become inaccessible. Depending on the circumstances, loss of a decryption key could constitute 'accidental loss, destruction or damage'

to personal data and would therefore be a contravention of the GDPR's security principle. Additionally, if data cannot be restored, this may also constitute a personal data breach due to a lack of availability. QRS has minimised this risk by the use of MS Azure AD but the risk can never be completely removed.

10. Policy Compliance

Compliance with this policy will be continually verified through on-going monitoring and internal and external audits.

Exemptions to this policy may be applied where there is a clear business/technical need, where risks are appropriately managed and when the exemption is approved by a relevant and authorised party.

Regulatory compliance will adhere to the UK/EU territory.

11. Policy Implementation

The implementation of this policy will be supported by ongoing training and dedicated systems and controls.

The Company will ensure that this policy is appropriately implemented through the continuous monitoring, internal & external audits and through the continued management of asset registers.

With the help of the IT Director and DPO, the department managers are responsible for ensuring their staff adhere to this policy as appropriate to their roles.

Any questions or concerns about the interpretation or operation of this policy should be taken up with the IT Director.

These policies supplement your terms of employment but are not of contractual effect not withstanding the potential implications of your employment in relation to UK Laws. Their purpose is to explain the Company's current policies and procedures, but they may be subject to change without notice if changes are considered appropriate by the Company or if there are changes in relevant legislation.