Encryption Policy

Template

This is an example policy. Please ensure you update this policy template so that it’s suitable for your organisation.

## Definition

Encryption is the process of encoding (or scrambling) information. This is so it can only

be converted back to its original form (decrypted) by someone who has the correct decoding key or device.

## When to use encryption

Data will be encrypted when it’s being:

* stored
* used
* transmitted

Encryption must always be used to protect strictly confidential information

transmitted over data networks. This is to protect against the risks of interception. This includes when:

1. Accessing network services which require authentication – for example, usernames and passwords.
2. Sending or accessing strictly confidential information – for example, in emails.

Where confidential data is stored on or accessed from mobile devices the

devices themselves must be encrypted (using ‘full disk’ encryption), irrespective of

Ownership. These devices include:

* laptops
* tablets
* smartphones
* external hard drives
* USB sticks
* digital recorders

Where strictly confidential data is stored in public, cloud-based storage facilities the

data must be encrypted prior to storing. This is to ensure that it’s not possible for the cloud service provider to decrypt the data.

Where data is subject to an agreement with an external organisation, the data should

be handled (stored, transmitted or processed) in accordance with the organisation’s

specified encryption requirements.

## Key management

In most cases, encryption keys will be in the form of a password or passphrase.

Losing or forgetting the encryption key will leave encrypted information unusable. Therefore, it's critical that encryption keys are effectively managed. It’s advisable to make secure backups of your keys and to consider storing copies with trusted third parties.

## Encryption standards

Originally adopted by the US government, Advanced Encryption Standard (AES) encryption has become the industry standard for data security. This policy recommends AES 256-bit strength encryption implementations.

## UK law

Export regulations relating to cryptography (encryption) are complex, but so long as

the encryption software used to encrypt a device or file is considered to be a "mass

market" product it is unlikely that you will encounter any problems leaving or re-

entering the UK. That said, you may be required to decrypt any devices or files by

UK authorities on leaving, entering or re-entering the country. If you are requested to

decrypt your files or devices you are advised to do so.

## Travelling abroad

In addition to what has been written above about export regulations, you should also

be aware that government agencies in any country may require you to decrypt your

devices or files on entry or exit from the country. If you are travelling abroad with

encrypted confidential data this means that there is a risk that the data may have to

be disclosed and you should consider the consequences of this. Wherever possible,

do not take confidential data with you when you travel.

Particular attention should be paid to the possible export of data under the data protection act for countries outside of the European Economic Area (EEA) when travelling. This includes the other countries deemed to have adequate levels of protection.

## Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the <role> and <organisation>.

Policy exceptions must describe:

* the nature of the exception
* a reasonable explanation for why the policy exception is required
* any risks created by the policy exception
* evidence of approval by all appropriate parties

Review of this document: annually by <role>.

Next review date: <date month year>.