University of Bristol
Information Security Policy

Title:	**Encryption**
Reference:	**ISP-16**
Status:	**Approved**
Version:	**1.1**
Date:	**March 2014**
Reviewed:	**April 2019**
Classification:	**Public**

Contents

Introduction

This Encryption Policy is a sub-policy of the Information Security Policy (ISP-01) and sets out the principles and expectations of how and when information should be encrypted.

Definition

Encryption is the process of encoding (or scrambling) information so that it can only be converted back to its original form (decrypted) by someone who (or something which) possesses the correct decoding key.

When to use encryption

Encryption must always be used to protect strictly confidential information transmitted over data networks to protect against risks of interception. This includes when accessing network services which require authentication (for example, usernames and passwords) or when otherwise sending or accessing strictly confidential information (for example, in emails).

Where confidential data is stored on or accessed from mobile devices (for example, laptops, tablets, smartphones, external hard drives, USB sticks, digital recorders) the devices themselves must be encrypted (using "full disk" encryption), irrespective of ownership.

Where strictly confidential data is stored in public, cloud based storage facilities the data must be encrypted prior to storing to ensure that it is 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 render encrypted information unusable so it is critical that encryption keys are effectively managed. When devices are encrypted by IT Services, IT services will take responsibility for the secure management of the keys. In all other cases, it will be the individual member's responsibility to manage the keys. It is advisable to make secure backups of your keys and to consider storing copies with trusted third parties.

Encryption standards

There are many different encryption standards available. Only those which have been subject to substantial public review and which have proven to be effective should be used. Specific guidance is available from IT Services and the University's Information Security website.

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.

Section 49 of the Regulation of Investigatory Powers Act (RIPA) includes a provision whereby certain "public authorities" (including, but not limited to law enforcement agencies) can require the decryption of devices or files. Failure to comply with such a lawful request is a criminal offence in the UK.

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 (keep the data at the University and access it using the University's secure, remote access facilities).

Particular attention should be paid to the possible inadvertent export of data subject to the Data Protection Act to countries outside of the EEA (or the few other countries deemed to have adequate levels of protection) when travelling

Further guidance

Encryption advice (InfoSec website):

http://www.bris.ac.uk/infosec/uobdata/encrypt/

Mobile and Remote Working Policy:

http://www.bris.ac.uk/infosec/policies/docs/isp-14.pdf

Information Handling Policy:

http://www.bris.ac.uk/infosec/policies/docs/isp-07.pdf

The University's Export Control website (which includes a link to the University's Export Control Policy):

http://www.bristol.ac.uk/secretary/legal/export-control/