University of Bristol
Information Security Policy - Encryption

Title	Encryption
Reference	ISP-16
Status	Approved
Version	2.0
Date	March 2014
Review	October 2021
Classification	Public

Contents

1. 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.

2. Scope

This policy applies to all systems (including but not limited to personal computing devices, cloud systems, servers and networks) containing University owned information classified as confidential or above, and anyone processing University information classified as confidential or above.

2.1. Definitions

Encryption is a mathematical function using a secret value - the key - which encodes (scrambles) data so that only users with access to that key can read the information. In many cases encryption can provide an appropriate safeguard against the unauthorised or unlawful processing of data.

3. Policy

3.1. When to use encryption

Encryption is a critical method of safeguarding data in a number of data storage and transfer activities. This includes, but is not limited to, the short term or long-term storage of data (for example data locally stored on a device, portable drives, cloud backups, databases and file servers) and the transfer of data between systems (for example through email, USB drives, file sharing solutions and instant messaging).

When handling data classified as confidential or above, either during storage or transfer, encryption must always be used to prevent unwanted access to the data.

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 encrypting files, individuals are responsible for the management and secure storage of encryption keys.

It is important to note the means of decrypting files (encryption keys, including passwords) should never be stored or transmitted alongside the encrypted files themselves.

3.2. Encryption of data at rest

Data can be considered at rest when it is held physically in computer storage (on cloud storage, file hosting services, databases, spreadsheets and as files stored on computing devices). When at rest, data classified as confidential or above must always be encrypted to prevent unwanted access.

All end-user devices (laptops, mobile phones and portable drives) containing or accessing University owned data of any classification must be encrypted.

University owned devices will be encrypted as part of the deployment process with encryption keys managed by IT Services. In cases where data classified as confidential or above is handled on a non-University owned device or system (including USB drives or third-party cloud storage solutions), the owner of the device, or user of the system, must take responsibility for ensuring the encryption of the data. This includes the secure storage of passwords and keys for accessing and decrypting the data.

3.3. Encryption of data during processing and in transit

When transferring data classified as confidential or above from one device or system to another (such as across the internet or over wired or wireless connections), data must be encrypted.

Encryption during transfer must either be through the conversion of data into an encrypted format (for example through file encryption) or through the use of a secure communication method which is able to provide assurance that the content cannot be understood if intercepted (such as using Transport Layer Security or TLS).

For information classified below confidential (Public and Open), encryption is still recommended and is best practice for maintaining data integrity.

For additional guidance on encryption standards and when to use encryption, contact IT Services.

3.4. UK law and travelling abroad

Upon leaving or entering the UK, you may be required by UK authorities to decrypt any devices, or files you have stored on devices in your possession. 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.

Similarly, government agencies operating outside of the UK may require you to decrypt your devices or files upon entry to or exit from their territories. If you travel abroad with encrypted data classified as confidential or above, there is a risk that the data may require decryption and therefore a risk of disclosure. It is advised that you consider the

consequences of such disclosure and wherever possible information classified as confidential or above should not be taken with you while travelling.

For access to information classified as confidential or above abroad, it is recommended the data remains stored on University systems, with access to the data provided by means of a secure and encrypted remote connection.

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

4. 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