Encryption Policy

Document Filename
Version
Information Classification
Status
Date
Policy owner
Policy contact

Encryption Policy.docx
1.0
Open
Approved
18 December 2015
Graham McKay
g.mckay@dundee.ac.uk.
Document Approval

<table>
<thead>
<tr>
<th>Title/Role</th>
<th>Name of Approver(s)</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Management Committee</td>
<td>Jim McGeorge, Paul Saunders, Ian Leith, Richard Parsons, Wesley Rennison, Andrew Hewitt, Tim Hustler.</td>
<td>18/12/2015</td>
</tr>
</tbody>
</table>

Version Control

<table>
<thead>
<tr>
<th>Revision</th>
<th>Status</th>
<th>Author(s)</th>
<th>Reviewed By</th>
<th>Approved By</th>
<th>Issue Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Draft</td>
<td>Graham McKay</td>
<td>Richard Parsons</td>
<td>Alan Bell</td>
<td>19/10/2015</td>
</tr>
<tr>
<td>1.0</td>
<td>Approved</td>
<td>Graham McKay</td>
<td>Richard Parsons</td>
<td>Alan Bell</td>
<td>18/12/2015</td>
</tr>
</tbody>
</table>
Contents

1 Document overview .................................................................................................................. 1
  1.1 Purpose ............................................................................................................................. 1
  1.2 Scope .................................................................................................................................. 1
  1.3 Definitions .......................................................................................................................... 1
  1.4 References .......................................................................................................................... 1

2 Policy ........................................................................................................................................ 2
  2.1 Storage ................................................................................................................................ 2
  2.2 Communications .................................................................................................................. 2

3 Review ....................................................................................................................................... 3

4 Breaches of policy ..................................................................................................................... 3

5 Further information .................................................................................................................. 3

6 Further guidance ....................................................................................................................... 4
  6.1 Using a USB storage device ................................................................................................. 4
  6.2 Using a laptop, smartphone or tablet ................................................................................... 4
  6.3 Using cloud storage ............................................................................................................. 4
  6.4 Using a personal device ........................................................................................................ 4
1 Document overview

1.1 Purpose

1.1.1 The purpose of this policy is to safeguard the confidentiality and integrity of the University’s information assets particularly when being sent or used outside of the University’s network.

1.2 Scope

1.2.1 This policy is applicable to all staff, students and visitors accessing University data classified as Private or Confidential.

1.3 Definitions

1.3.1 University – The University of Dundee is a Scottish Registered Charity, No. SC01509 with its registered office at Tower Building, Nethergate, Dundee DD1 4HN.

1.3.2 Staff - Staff are salaried members of the University or contracted individually by the University to provide a service.

1.3.3 Student - a person pursuing any course of study in the University.

1.3.4 Visitors - A visitor is anyone, not a member of staff or student, requiring access to University premises or services.

1.3.5 Plain text - Refers to any type of data in its original, readable, unencrypted form.

1.3.6 Key - A random piece of data used with encryption and decryption. Encryption and decryption algorithms require a key and plain text or cipher text to produce cipher text or plain text, respectively. The key is usually shared only with those parties that should be allowed to encrypt and decrypt messages.

1.3.7 Encryption - The process of taking plain text and using a key to convert it into cipher text. Ciphers, algorithms, or schemes are used to encrypt data. All encryption algorithms require the use of a key, and must be able, with the proper key, to be reversed, converting the cipher text back into the original plain text.

1.3.8 Decryption - Taking cipher text and using a key to convert it into plain text. In most cases, the algorithm or key used to encrypt the data is not the same as the one used to decrypt the data. Decrypting cipher text should not be computationally feasible without the proper key.

1.3.9 Portable devices – A portable device is any device that can be easily carried and has the capacity to store data digitally. Examples include laptops, tablets, smart phones, USB devices, games consoles.

1.4 References

1.4.1 Information Classification Scheme.

1.4.2 Information Commissioners Office – Advice on the use of encryption

---

1 https://ico.org.uk/for-organisations/encryption/
2 Policy

2.1 Storage

2.1.1 It is the University's policy to encrypt all data classified as private or confidential when it is stored on portable devices and devices outside the University’s network.

2.2 Communications

2.2.1 It is the University’s policy to encrypt all data classified as private or confidential when it is transmitted outside the University's network.
3 Review

3.1.1 The Information Security Steering Group is responsible for keeping this policy current. This policy will be reviewed annually or more frequently as required.

4 Breaches of policy

4.1.1 Failure to comply with this policy may result in disciplinary action being taken against you under University of Dundee disciplinary procedures, which may include summary dismissal. If there is anything in this policy that you do not understand, please discuss it with your line manager.

5 Further information

5.1.1 If you have any questions regarding this policy, please contact the Chief Information Security Officer at g.mckay@dundee.ac.uk.
Further guidance

6.1 Using a USB storage device

6.1.1 Where an external USB device is used to store data, this must be encrypted and not be a primary storage device.

6.1.2 Do not use unencrypted USB keys to hold private or confidential data.

6.2 Using a laptop, smartphone or tablet

6.2.1 University issued laptops, smartphones and tablets will be setup with encryption enabled. Ensure you set a strong passcode on your smartphone or tablet.

6.3 Using cloud storage

6.3.1 If you use cloud storage, you must ensure that it is securely encrypted by checking with your service provider.

6.3.2 The University’s cloud storage provider is Box and all data stored on this platform is encrypted by default both in transit and at rest.

6.4 Using a personal device

6.4.1 If you use your personal laptop or home PC to access University data, either encrypt your device, or ensure you do not hold data that is private or confidential on it.