Encryption policy

1. Introduction

1.1. It is the policy of De Montfort University (DMU) that appropriate measures are taken to ensure that all confidential, personal or sensitive personal electronic data is stored and transmitted in a secure manner relevant to the type of data and the system it is held on. This policy outlines the standards which must be adhered to for the storage of such data on systems or devices not already on university secure storage and the transmission of data between systems or devices.

2. Scope

2.1. This policy applies to all users of DMU information systems who process confidential, personal and sensitive personal electronic data outside of the DMU Campus Network.

2.2. It covers the use of systems or devices such as (but not limited to):

- Laptops
- Tablets
- Desktop PC's
- Smartphones
- USB memory stick
- External hard drives
- CD, DVD, floppy disk, tape etc.
- Solid state or other storage device (e.g. CompactFlash, SD, other new digital storage)
- Cloud based storage systems not managed by the university

2.3. It covers any device used for storing or processing confidential, personal and sensitive personal electronic data, including personal devices, university devices and devices owned by third parties.

2.4. It covers communication methods used for transmitting confidential, personal and sensitive personal electronic data outside of the university through email, SMS or other similar methods.

3. Definitions

3.1. **Processing** – means any operation on data, including organisation, storage, adaptation and alteration, consultation or use; disclosure, transmission, dissemination and otherwise making available.

3.2. **Classes of information** – definitions of the different levels of information (confidential, personal, sensitive personal and unclassified) can be found in the Information Handling Policy.

3.3. **Encryption** – the process of converting information so that it cannot be read by unauthorised people.

4. Policy statement

4.1. No electronic data owned by the university that is classified as confidential, personal or sensitive personal data according to the Information Handling Policy will be stored in an unencrypted format anywhere other than on university secure storage
4.2. Procedures shall be established to ensure that authorised staff may gain access, when needed, to any important business information being held in encrypted form.
4.3. Transmission of any data that is confidential, personal or sensitive personal outside of the university data network must be protected by use of appropriate encryption techniques.
4.4. Encryption shall be used whenever remote access to confidential, sensitive or personal sensitive information is required.
4.5. Access to encrypted data will be available from any device owned by the university or approved personal devices.

5. Implementation of Encryption Policies

5.1. Establishing a continuous "Plan-Do-Check-Act" cycle of activities which ensure that suitable practices are documented, reinforced and improved with time. (Documentary evidence of the processes and procedures involved may be required to demonstrate implementation of this policy to external parties.)
5.2. Ensuring that the university has access to suitable encryption technologies to enable secure and effective storage and processing of confidential, personal or sensitive personal data.
5.3. Ensuring that all users who process information, or otherwise handle information, understand this policy and any consequences for non-compliance.
5.4. Using various lawful forms of monitoring activities, data and network traffic to detect policy infringements.
5.5. Take into account relevant information security policy requirements when planning and undertaking activities involving IT-based information systems.
5.6. Formal or informal risk assessment, to identify the probability and impact that various hazards could have on information systems.
5.7. Monitoring effectiveness of its information security policy implementation. This may involve review independent from those charged with its implementation

6. Management of encryption keys

6.1. A procedure for the management of electronic keys, to control both the encryption and decryption of data, must be established to ensure the adoption of best practice guidelines and compliance with both legal and contractual requirements.
6.2. To ensure compliance with the Data Protection Act and business continuity, all electronic keys will be centrally stored and managed by trained and authorised personnel nominated by the Director of ITMS.

7. Consequences of non-compliance

Failure to comply with this policy could expose the university, its staff and students to risks including fraud, identity theft and reputational and financial damage to the university. The Information Commissioner can also impose a fine of up to £500,000 on the university for breaches of the Data Protection Act.

8. Document approval

Approved by: Dieter Kraftner Director of ITMS
Approved Date:
Review Date:
Reviewer: IT Governance Manager

9. Document history

9.1. 19th May 2014 – Draft 1 Neil Faver
9.2. 28th May 2014 – Draft 1.1 Neil Faver
9.3. 18th June 2014 – Draft 1.2 Jonathan Hill
9.4. 27th August 2014 – Version 1.0 Neil Faver