Outsourcing and Third Party Access Policy

1. Introduction

This policy sets out the conditions that are required to maintain the security of the university's information and IT systems when third parties, other than the university's own staff or students, are involved in their operation. There are 4 possible circumstances when this may occur:

1.1. When 3rd parties (for example contractors/suppliers) are involved in the design, development or operation of university information systems or IT equipment.

1.2. When access is granted from locations outside of the university network and equipment may not be under the control of the university.

1.3. When users who are not members of the University (for Example Research Collaboration) are given access to information systems.

1.4. The use of cloud computing services.

2. Scope

2.1. This document applies to any member of the university who is considering engaging a third party to supply a service where that service may require access to the university's information assets and includes statements on:

- 2.1.1. Informal outsourcing
- 2.1.2. Managing outsourcing and third party access risks.
- 2.1.3. Contractual Issues.
- 2.1.4. Third Party support and maintenance.
- 2.1.5. Facilities Management and Outsourcing.
- 2.1.6. Physical Access by External Parties to Sensitive Area's.
- 2.1.7. Electronic Remote Access by External Parties

3. Informal outsourcing

3.1. Staff and students at the university are able to access and use a range of IT services on the Internet which are provided by third parties with which the university does not have any formal agreement. Any member of staff or student using these facilities is typically required to accept the terms and conditions determined by the supplier.

3.2. Examples of informal outsourcing includes:

- 3.2.1. Using 'Dropbox' to store university business information.
- 3.2.2. Forwarding business sensitive or personal email from a university email account to MSN Hotmail or Google Mail.

3.3. Due to the absence of controls or accountability to the university, a number of security risks are associated with entrusting information to these facilities. Some of the potential risks are listed below:

- 3.3.1. Who has access to the information?
- 3.3.2. How the information is used.
- 3.3.3. Where the information is stored.
- 3.3.4. How securely the information is stored.
- 3.3.5. Will the data be lost in the event of a disaster?
- 3.3.6. Use of these facilities to process data may be in breach of the Data Protection Act 1998

3.4. With the risks highlighted in 3.3 above, wherever possible, university staff should only use services provided by the university for conducting university business. Where a university solution is not provided, however, then staff may use third party systems but must not store or transfer out of the University the following types of information:

3.4.1. **Confidential Information** – business confidential information (which may or may not also be personal information) and which may not be disclosed except to those with the explicit consent of the data owners and where disclosure may constitute an actionable offence.

3.4.2. **Sensitive Personal Information** – information covered by the Data Protection Act 1998 which relates to an individual's ethnicity, political membership or opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, the commission or alleged commission of an offence and any related proceedings.

3.4.3. **Personal Information** – information covered by the Data Protection Act 1998 that allows a living individual to be identified or which relates to an identifiable individual.

3.4.4. For further information on these levels of information see the **Information Handling Policy**

4. Managing Outsourcing and Third Party Access Risks

4.1. The risks involving external party access to the university's information and information processing facilities shall be identified and controls implemented before granting access by the initiator in collaboration with the IT Governance Manager or their nominated deputy.

4.2. Third party access to systems must be restricted to the minimum required system level access.

4.3. Any external access to the university's IT systems must follow established procedures.

5. Contractual Issues

5.1. All third parties given access to the university's IT systems must agree to abide by the university's information security policies prior to being granted access.

5.2. The university will assess the risk to its information and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, the university will require third party suppliers of services to sign a confidentiality agreement to protect its information assets.

5.3. Where relevant, third parties should be asked to provide a copy of their information security policies.

5.4. All contracts with external suppliers for the supply of services to the university must be monitored and reviewed to ensure that information security requirements are being satisfied.

5.5. Contracts must include appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.

6. Third Party Support and Maintenance

6.1. University staff and students must not permit information security safeguards to be bypassed, or allow inappropriate levels of access to the university information or IT facilities to any third parties. For further information see:

6.1.1. User Management Policy

6.1.2. Use of Computers Policy

6.1.3. Information Handling Policy

6.2. Persons responsible for agreeing maintenance and support contracts will ensure that contracts being signed are in accord with the University's information security policies.

7. Facilities Management and Outsourcing

Any facilities management (such as PC maintenance) outsourcing company which the university may enter into a contract with, must be able to demonstrate compliance with De Montfort University's information security policies and enter into binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance.

8. Physical Access by External Parties to Sensitive Areas

A risk assessment must be made by the initiator in collaboration with the IT Governance Manager or their nominated deputy and appropriate controls established before granting third party access to secure areas where confidential information is stored or processed. This also applies to secure areas containing active network equipment.

9. Electronic Remote Access by External Parties

Remote access by External Parties to the DMU network must be limited to the minimum required system level access. Any request for access must first be approved by the Director of ITMS or their nominated deputy.

10. Document Approval

Approved by: Dieter Kraftner Director of ITMS
Approved Date: 24th June 2015
Review Date: 23rd June 2016
Reviewer: IT Governance Manager

11. Document History

11.1. 5th October 2012 – Version 1 Neil Faver
11.2. February 2015 – Version 1.6 Neil Faver