Information Services and Systems

Policy on Remote Access - Access to DMU systems from off site

1. Introduction

1.1 The purpose of this policy is to ensure that users understand their role and responsibilities when taking University data, and equipment off site and accessing DMU networks and systems from remote locations. It is designed to minimize the potential exposure to the University from damage that may result from unauthorised use of University resources.

1.2 This policy supplements and does not replace any existing policies or regulations. These are published on the University Internet site. It applies to all University staff and students, contractors, vendors and other agents

1.3 Many learning and administrative support systems are now available via the Internet using Web technology and secure data systems. There are other access systems that designed to support particular users and applications. Access to Web based applications is provided to registered users.

1.4 University IT facilities are provided to meet the aims of the organisation.

1.5 The University regulations contain information relating to non-institutional use of facilities.

1.6 The University IT regulations apply to the use of equipment away from University premises. The need to ensure that data is kept safe from destruction or theft and that equipment and passwords are held safely.

2. Authorisation for the removal of equipment from the University

2.1 Before any equipment is removed from University premises a record of the loan must be made and signed by an authorised person. Consult your supervisor who will arrange for a "RECORD OF LOAN EQUIPMENT " form PC257 to be completed and authorised. A copy of the authorised form should be available from the person borrowing the equipment for inspection as required.

3. Using University IT off premises

The following guidelines must be observed for computer systems taken off site;

3.1 All personal computers taken off site from the University must have virus protection active which must be used according to University guidance on Virus protection.

3.2 No computer media should be used on any system connected or to be connected to University systems unless it has first been scanned for viruses and cleaned if required.

3.3 When travelling equipment and media should not be left unattended. Portable computers and media should be carried as hand luggage when travelling.

3.4 Systems taken off site from the University should have password protection activated and if material is sensitive encryption should be considered for relevant data files

3.5 Manufacturers instructions regarding transportation, protection against hazards and operation should be observed at all times

3.6 Any loss, damage or potential breach of security should be notified to the University information security manager and line manager as soon as possible.

4. Using University software off-site

4.1 Users should ensure that they are authorised to use operating systems software and applications when they are removed from University premises, particularly if the equipment is taken to another organisation for demonstration purposes. Generally software that may be used off campus can only be used by University personnel and in relation to the business of the University.

4.2 Users should never copy or, allow to be copied, software from University systems to another person or onto another system. Details on the availability of major software packages for off campus use is updated regularly.

5. Using University data off-site

5.1 Where University data are to be taken outside the University users must register that need with the Information Custodian for that data. The extent and period of approved removal will be governed by need and authorised as appropriate by the Custodian of the data.

5.2 Removal without prior authorisation or for purposes beyond the scope of the authorisation of use may constitute a serious disciplinary offence.

6. Remote access

6.1 The University provides facilities for students and staff to access IT systems off campus. The main mode of access for students is through the world wide web using Uniform Resource Allocators (URL's) notified to users.

6.2 It is the responsibility of Remote Users to ensure that all possible measures have been taken to secure the remote machine. This includes the use of physical or software firewalls and anti-virus software.

6.3 If a domestic wireless solution is used at the users premises, it must be made secure to ensure no unauthorized users can access the domestic wireless network.

7. Secure remote access

7.1 Secure remote access is provided to staff. Secure remote access must be strictly controlled. Access to DMU Secure remote access is by user ID and Password.

7.2 All remote users working with sensitive or restricted data must use the DMU SRA service.

7.3 At no time will a remote user provide another person, including family members with their remote user password.

7.4 Remote users must ensure that when their University owned or personal computer or workstation is connected to the DMU University network it is not connected to any other network at the same time, other than a private network under the users control.

7.5 Remote users must ensure that computers connected to the DMU SRA service must use up to date anti virus and anti trojan software and that the system they are using has the most recent operating system and application patches loaded.

7.6 If requested, users must accept that DMU will check the users appliance for up to date AV and operating system patches.