Mobile Computing and Remote Access Policy

Document Filename | Mobile Computing and Remote Access Policy.docx
Version | 1.0
Information Classification | Open
Status | Approved
Date | 18 December 2015
Policy owner | 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 Alan Bell</td>
<td></td>
<td>27/08/2015</td>
</tr>
<tr>
<td>1.0</td>
<td>Approved</td>
<td>Graham McKay</td>
<td>Richard Parsons Alan Bell</td>
<td>Information Management Committee</td>
<td>18/12/2015</td>
</tr>
</tbody>
</table>
# Mobile Computing and Remote Access Policy

## Contents

1. **Document overview** .............................................................. 1
   1.1 **Purpose** ................................................................. 1
   1.2 **Scope** ........................................................................ 1
   1.3 **Definitions** .............................................................. 1
   1.4 **References** ............................................................... 1
2. **Policy** .................................................................................. 2
3. **Review** .................................................................................. 3
4. **Breaches of policy** .............................................................. 3
5. **Further information** ............................................................. 3
6. **Further guidance** ................................................................ 4
   6.1 **Physical security** .......................................................... 4
   6.2 **Secure access** ............................................................. 4
   6.3 **Policy awareness** ........................................................... 4
Document overview

1.1 Purpose

1.1.1 The purpose of this policy is to ensure that people accessing University data by mobile devices or remote connections:

• do not expose the University to increased legal or governance risk;

• understand the risks and responsibilities associated with working remotely or using mobile devices; and

• restricts the distribution of private and confidential information.

1.2 Scope

1.2.1 This policy is applicable to all staff, students and visitors accessing University data.

1.3 Definitions

1.3.1 Remote working – where a person works from out with the primary geographical work place.

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

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

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

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

1.3.6 Two factor authentication - It is an authentication process where two of three recognised factors are used to identify a user:

1.3.6.1 Something you know - typically a password, passcode, passphrase or PIN.

1.3.6.2 Something you have – a time based authentication code, smartcard or token.

1.3.6.3 Something you are - fingerprints, iris patterns, or voice prints.

1.4 References

1.4.1 Acceptable use of computing devices policy.
2 Policy

2.1.1 The University of Dundee provides people with the facilities and opportunities to work remotely and utilise mobile devices as appropriate whilst ensuring remote workers are aware of the acceptable use of computing devices policy.

2.1.2 Any remote or mobile computing devices used for remote working require to be encrypted and protected by means of a password or PIN.

2.1.3 Remote administrative access to systems should require two factor authentication.
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.
6 Further guidance

6.1 Physical security

6.1.1 Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location. Computing devices should not be left unattended where it would attract the interests of the opportunist thief.

6.1.2 At home, remote computing devices should also be located out of sight of the casual visitor and must be secured whenever it is not in use.

6.1.3 Users must ensure that authentication tokens and passwords are kept in a separate location to the computing devices at all times.

6.1.4 No paper documents falling into the University classification of confidential (See University Information Classification Scheme) should be taken off site unless approved in advance. Guidance can be provided by Records Management Services\(^1\).

6.1.5 Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use.

6.1.6 Documents should be collected from printers as soon as they are produced and not left where they can be casually read. Waste paper containing data classified as Private or Confidential must be shredded when no longer required.

6.2 Secure access

6.2.1 Computing devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

6.2.2 All data on computing devices must be encrypted.

6.2.3 The use of VPN or two factor authentication should be considered as a further means of security.

6.3 Policy awareness

6.3.1 All users must comply with appropriate information security policies for the use of IT equipment.

\(^1\) http://www.dundee.ac.uk/recordsmanagement/