Ulster University Standard Cover Sheet

Document Title	REMOTE ACCESS STANDARD 2.6
Custodian	Deputy Director of Finance and Information Services (Information Services Directorate)
Approving Committee	Information Services Directorate (ISD)
Policy approved date	2017-03-09
Policy effective from date	2017-03-09
Policy review date	2018-03-09

Changes to previous version
Page 1 – “in order to” changed “to”
Page 2 – “line manager” changed to “line manager or Dean”
Page 2 – Added “RDweb for browsers”
Page 3 – “in order to” changed to “to”
Page 4 – “for the purpose of providing” changed to “to provide”
Page 4 – “actually running” changed to “running”

INTRODUCTION AND BACKGROUND

It is appreciated that access to University networks, systems and services may be required when staff and 3rd parties are working remotely in order to support business needs. However, the mechanism by which this is provided must be securely managed with full auditing to meet IT Security standards to protect information.

Two main categories of remote access are covered in this document. “Attended Remote Access” refers to a situation in which a user within the University temporarily passes the control of their workstation screen, mouse and keyboard to an external third-party while they are in continuous attendance throughout.

“Unattended Remote Access” refers to connections made to University networks as if the user were inside the University, independently from users inside. This primarily used for staff who are remote working, or third-party suppliers who require administrative access to internal University systems, servers and services.

Further information on ISD policies, standards and guidelines is available at:

http://www.ulster.ac.uk/isd/policies

RELEVANT LEGISLATION

The University will comply with all legislation and statutory requirements relevant to information and information systems, including:

- Computer Misuse Act 1990;
- Data Protection Act 1998;
- Communications Act 2003;
- Copyright, Designs and Patents Act 1988;
- Freedom of Information Act 2000;
- Human Rights Act 2000;
- Regulation of Investigatory Powers Act 2000;
- Police and Justice Act 2006;
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (‘the Lawful Business Regulations’)

STANDARD

Unattended Remote Access

1 General

1.1 Remote access is only permitted when the user is authorised to do so.

1.2 Final Approval to be granted unattended remote access rights will be on recommendation of a line manager or Dean with authority to approve expenditure from budget to cover costs (if any) incurred in the provision of the service.

Delivery of service will be on approval by Deputy Director of Finance and Information Services (Information Services Directorate) or their delegate.

1.3 Authorisation for unattended remote access shall be based on business need.

1.4 Unattended remote access is only permitted when conducted using the University's remote access service; Information Systems and/or Services which are permitted to be exceptions to this standard are approved by the Deputy Director of Finance and Information Services (Information Services Directorate) or their delegate and classified in the Information Systems Services Catalogue as such, for example self-service applications for students.

1.5 Grant of unattended remote access requires two factor authentication;

1.6 Standards for authentication defined by the University's Authentication Standard shall apply to unattended remote access.

1.7 Third parties (Contractors and other non-University employees) who are authorised for unattended remote access shall have time limits placed on their authorisation, which shall not exceed 12 months. Third parties being authorised for Remote access are required to conform to controls, such as Confidentiality, Non-disclosure and Information Assurance, on third parties specified by University policies.

1.8 Unattended remote access shall be supported by the following services:

1. RAVPN;
2. RDA for Microsoft Windows clients;
3. Remote File Share access for Microsoft Windows Clients;
4. Remote Virtualized Applications for Microsoft Windows Clients;
5. RDweb for browsers;

1.9 Use of the RAVPN service shall only be conducted from University owned or authorised third party devices. Mobile devices used in this respect must have their data storage encrypted.

1.10 Where possible, devices using the Remote Access Service will be checked to ensure appropriate anti-malware services are in effect.

1.11 Users of Remote access shall be trained and otherwise be made aware of their responsibilities for handling data, information & documents which are subject to a) the Data Protection Act and b) Information Handling standards of the University's Electronic Information Assurance Policy.

Attended Remote Access

2 General

2.1 The internal University User in attendance must be supervising the remote activity throughout the attended remote access session.

2.2 Where possible, attended remote access enabling software should be removed or disabled between sessions. Configuration should disallow remote initiation of sessions

PURPOSE AND SCOPE OF THE POLICY

The purpose of this document is to define University standards for remote access to minimize the potential exposure of the University to risk of damage which may result from unauthorised access to internal information systems and services. Damages include:

1. The loss of:
    a. Personal data covered under the Data Protection Act,
    b. Confidential and/or commercially sensitive information,
    c. Intellectual property,
2. Public image
3. Loss of service
4. Reduction in quality of service

This standard applies to all remote access and to all persons.

DEFINITIONS

“Internal Information System or Service” is used to refer to any Information System or Service hosted on the University’s telecommunications infrastructure, which is not specifically designed and implemented for public access, irrespective of ownership.

“Remote Access Service” is used to refer to the service implemented and maintained by the Information Services Directorate to provide a secure, centrally managed and audited remote access for staff who are authorised to use it.

“Remote Access Virtual Private Network (RAVPN)” is a technology which is used to achieve a secure network connection between a remote user and the University’s private network, over the public Internet. The remote user may use any mechanism to connect to the Internet in order to initiate the RAVPN to the University, such as a) a home broadband connection via a) an Internet Service Provider, b) a public or private WiFi connection which has access to the Internet, or c) a mobile broadband service from a mobile telephony operator.

“Remote Desktop Access (RDA)” is where total control of a workstation hosted on the University’s private network, is provided to another client computer located on a remote network. Total control means that the remote user is presented with a view of the remote computers desktop and can manipulate the University hosted computer as if they were physically using the University hosted computer on campus.

“Remote Virtualized Applications (RVA)” is used to refer to a client computer accessing a pre-defined list of University Applications via a Web based portal. The application is presented in a “window” on the client device, with the application running on a University hosted server.

“Two factor authentication” – An authentication factor is a piece of information and process used to authenticate or verify the identity of a person, such as a password or PIN. Two-factor authentication is a system wherein two different factors are used in conjunction to authenticate a user. Using two factors as opposed to one factor generally delivers a higher level of authentication assurance. Two-factor authentication typically is a signing-on process where a person proves his or her identity with two methods: "something you know" (e.g., password or PIN) and “something you have" (e.g. a smartcard or token). A third factor type which can be used is “something you are” (e.g. a fingerprint or iris scan).