UNIVERSITY OF PORTSMOUTH

SECURE REMOTE ACCESS

Jan 2020

Contents

Document title		
Normal text		
Document author and department		
Normal text		
Approving body		
Normal text		
Date of approval		
Normal text		
Review date		
Normal text		
Edition no.		
Normal text		
ID Code		
Normal text		
Date of effect		
Normal text		
EITHER For public access online (internet)? Tick as appropriate		**YES**
For public access on request copy to be mailed Tick as appropriate	**NO**	**YES**
OR For staff access only (intranet)? Tick as appropriate		**YES**
Password protected Tick as appropriate	**NO**	**YES**
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk		

If you need this document in an alternative format, please email corporate.communications@port.ac.uk

The latest version of this document is always to be found at:

https://erecords.port.ac.uk/documents/qA43279

Summary

This advisory sets out the technical and procedural safeguards required for remote access to the University IT network. Remote access is necessary for home working.

Who is this for?

This IS advisory is aimed at staff, students and third party contractors who have or are responsible for a account on the University network or its associated systems. These safeguards must be applied, even when using a privately owned computer.

How does the University check this is followed?

Annual review of this IS advisory will be performed to evaluate its effectiveness.

Who can you contact if you have any queries about this document?

Any questions about this advisory should be directed to servicedesk@port.ac.uk

It is essential that all 'remote workers familiarise themselves with their responsibilities under the University's Data Protection Policy (available in the Document Warehouse)

1.0 Remote Risk

Remote access to the University network by members of staff must be carefully managed to minimise the security risks. These risks arise because remote computers are beyond the control of the University and it is almost impossible to guarantee their security. To address this problem, the University offers a secure remote connection called a a Virtual Private Network (VPN).

1.1 VPN (Virtual Private Network)

A VPN uses special technology to create a private channel between two computers. The internet is not safe from eavesdroppers, so if you need to connect remotely from say, a home computer to the University network, you must do so over a secure VPN.

2.0 Minimum security requirements for remote access computers

The VPN provides a secure, 2-way communications channel but the remote computer must also meet certain security requirements. Computer equipment provided under the University's managed service agreement is configured to meet all security requirements, however, a personally owned computer may need individual attention to meet the standard. Seek advice from IS Service Delivery (ext 7777) if you want to connect a private computer to the University network over a VPN. The basic requirements are set out below:

- The computer must be protected with up to date anti-virus software
- The computer must be supported i.e. the vendor will provide new software releases and security patches as soon as they become available.
- The computer must be protected with a personal firewall
- The device must only use the Virtual Private Network to create a secure connection to the University network. Instructions on how to set up a VPN can be found on the IT Help Pages.

3.0 Procedural requirements

The following are good practice procedural requirements for protecting data processed on a remote computer.

3.1 Corporate data and personal data relating to staff and/or students of the University must not be downloaded *or* stored on an unencrypted device such as a private computer or smart device.

3.2 Corporate data and personal data relating to staff and/or students of the University must not be stored on an unencrypted storage device (e.g. USB stick, external hard drive, CD/DVD).

3.3 Corporate data and personal data relating to staff and/or students of the University must not be copied or transferred to internet storage (aka ‘cloud ’storage), either whole or in part.

3.4 Reasonable precautions must be taken to protect remote computers from theft. This might include: hiding the device when not in use, locking the device in a secure room or container, securing the device with a steel cable and lock (Kensington Lock).

3.5 When used in public/non-private area, data displayed on the computer screen must be concealed from the furtive glances of unauthorised persons.

3.6 Residual (‘cached’) data that may have been inadvertently collected during the connection must be deleted from the computer.

3.7 Personally owned computers that have been used to remotely access University data must be erased by Information Services **before** they receive maintenance or repair from a commercial supplier.

3.8 In addition to the security that must be applied to personal data, some financial and research information may also be sensitive and may be subject to a non-disclosure agreement. This data must be protected in the same way.

University of Portsmouth
Department of Human Resources
University House
Winston Churchill Avenue
Portsmouth PO1 2UP
United Kingdom

T: +44 (0)23 9284 3141
F: +44 (0)23 9284 3122
E: university.secretary@port.ac.uk
W: www.port.ac.uk