UNIVERSITY OF PORTSMOUTH

NETWORK VULNERABILITY ASSESSMENT

March 2016

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:

http://webaddresshere

Summary

What is this document about?

In the same way that a homeowner might check the security of doors and windows before leaving the house, it is important to check the security of the University network from the outside - looking in. Vulnerability assessment allows the University to look for security weak spots and take remedial action before they are exploited by a real cyber-threat.

Who is this for?

This IS Advisory is aimed at all staff of the University of Portsmouth, partners and third-party contractors.

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 should be directed to servicedesk@port.ac.uk

1. What must be protected?

1.1 The outward facing systems and services of the University of Portsmouth IT network must be adequately secure to protect these systems and data from compromise.

2. What are the risks?

2.1 Loss or theft of data
The University might be exposed to the theft or loss of data if forced access to the network is successful.

2.2 Damage or destruction
Important data held by the University might be exposed to damage or destruction if forced access to the network is successful.

2.3 Open doors for malware onto the network
Network perimeter vulnerabilities can also provide pathways for a wide range of malicious threats, including virus infection, spam launch-pads or bots.

3. Annual vulnerability assessment

3.1 Annual 3rd party vulnerability assessment of the University network will take place.

3.2 The vulnerability assessment will be carried out by adequately qualified staff and will be subject to a contract. IS-NSS staff will arbitrate on the adequacy of the qualifications offered and their decision will be final.

3.3 Vulnerability assessment results will be shared with relevant server owners and associated technical staff. These staff must plan and implement the recommended actions to address any problems found.

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