UNIVERSITY OF PORTSMOUTH

PHYSICAL SECURITY ADVISORY

March 2015

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

What is this document about?

This advisory aims to ensure that University information systems and data is kept physically secure - to prevent unauthorised access, damage and/or interference.

Who is this for?

This advisory is aimed at all staff, students, visitors and contractors who are permitted to access University premises. **It is important to take reasonable steps to protect IT equipment and data from theft or unauthorised physical access – particularly if the equipment is small and portable.**

How does the University check this is followed?

Annual review of this 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

1.0 Secure Areas

1.1 Areas and offices where restricted information is processed shall be protected with appropriate physical access controls. These areas should be secured when not occupied.

1.2 Account holders must protect their user account with a password screen-lock. The screen-lock should be set to activate after no more than 15 minutes of inactivity.

1.3 Paper documents containing restricted information must be kept out of sight when not in use and stored in a locked draw or cabinet.

1.4 Small items of IT equipment - including external hard drives, USB sticks, magnetic tape cassettes, disk drives and optical media must be kept out of sight when not in use and stored in a locked draw or cabinet.

1.5 Secure areas of the University (e.g. staff offices, University House, data centres) will be protected by a swipe-card access control system at the point of entry. Only authorised staff will be allowed to access these areas.

1.6 The University data centres at James Watson and Anglesea Buildings - and all network wiring closets around the University campus are strictly controlled areas. **These areas will only be accessible to named staff on an access list held by the Estates Dept.**

2.0 Physical and Environmental Security

2.1 The risk of natural or man-made disasters such as fires or floods should be considered before deciding where to site IT systems and critical data.

2.2 Business critical IT systems and systems requiring high availability should be housed in dedicated secure rooms which provide a controlled environment with air conditioning and an uninterruptable power supply.

2.3 All cables providing infrastructure support (including power and data) should be adequately protected from tampering and/or accidental damage.

3.0 Portable digital equipment.

3.1 Portable devices - like laptops, tablet computers and tablet devices (including USB sticks and external hard drives) must be adequately secured at all times.

3.2 Ideally, a portable device should be secured by a cable to a safe anchor point. This is not always possible because many portable digital devices do not provide any means to make them physically secure in this way. If this is the case, then the device must not be left unattended unless locked away out of sight. Always ensure that the device hard drive is encrypted and access to the device is protected by a strong password.

3.3 All data stored on portable devices should be encrypted and the device must be kept out of sight when not in use.

4.0 Secure data deletion and equipment disposal

4.1 All University unwed computers and digital devices must be returned to Information Services for asset deletion and secure disposal when no longer required or at their end-of-lease period. Secure disposal procedures ensure that all data and licensed software have been removed before an item of computer and storage equipment is re-sold, re-deployed or scrapped.

Contact the IS Service Desk (ext 7777) or the Estates Service Desk (ext 6677) for further information. (see also: IS Advisory - Secure Disposal)

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