UNIVERSITY OF PORTSMOUTH

SECURE OPERATIONS

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 how information systems are operationally managed to support information security. It covers standard procedures for operation of information systems under normal conditions.

Who is this for?

This IS advisory is aimed at all University staff who manage information systems and is of particular relevance to Information Services staff.

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

1.0 Documentation

1.1 All standard operating procedures (SOPs) should be reviewed annually and updated whenever changes to operating procedures are made.

1.2 Changes to SOPs must have management approval and steps should be implemented to ensure that any changes to documentation happen in a controlled and authorised manner.

1.3 Activity logs are collected, the aim being to collect sufficient data to be able to identify the source of a problem, without generating excessive data or compromising the privacy of individuals.

2. Segregation of Duties

2.1 Operational duties and areas of responsibility should be appropriately segregated to reduce the risk and consequential impact of information security incidents.

3. Incident Management

3.1 Security incidents, suspected security weaknesses, malfunctions and faults in information systems must be reported and dealt with in accordance with incident and problem management procedures.

3.2 Mechanisms should be in place to monitor and learn from those incidents and problems.

4. Development and System Implementation

Procedures shall be used to control the development and implementation of all information systems. These procedures shall include assessment of the security risks to information.

4.1 Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place.

4.2 Personal data used in a test or development environment must be protected from accidental loss or exposure. No personal data should be carelessly left on an intermediate server or test system after testing or migration is complete.

4.3 Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to migration to operational status.

4.5 Development and testing facilities for business critical systems should be adequately separated from operational facilities.

5. Backups

Backups of data are intended to maintain the integrity and availability of information. It is the responsibility of IS-EPS staff to ensure that information stored in an approved manner on University systems is backed up appropriately and processes for restoring data are regularly tested to ensure successful system recovery.

5.1 Backup Storage

Backup copies should be stored at a location separate from the original data and system.

5.2 System Recovery

Appropriate disaster recovery procedures should be implemented and tested for IT systems, on the basis of risk and business criticality, so that these systems can be adequately restored within a reasonable period, following a data centre outage.

6. Monitoring and Logging

6.1 The IS department must be able to trace and isolate the source of any disruptive network traffic or abusive, malicious activity. Activity logs are collected, the aim being to collect sufficient data to be able to identify the source of a problem, without generating excessive data or compromising the privacy of individuals.

6.2 Logs will be periodically scrutinised for the purpose of threat detection.

7. Account and System Privileges

7.1 University System Administrator privileges should be set the minimum privileges necessary to perform in that specific role and should be assigned to authorised personnel only.

Software and applications should only run with the minimal privileges necessary for the task and should not, for example, be run as 'root '(i.e. with unnecessary privileges). If such a highly privileged application was compromised then the attacker could use these privileges to cause extensive damage to the system.

8. Malicious Code

8.1 Up to date protection against malicious software should be activated which is appropriate to protect the University networks and systems.

8.2 If you notice any suspicious activity, software or files on your computer (e.g. an increase in advertising pop-ups, sudden low performance, unexpected email replies) then report it to the IT Service Desk on x7777.

9. Training

9.1 Information security training should be included as part of staff induction. Staff who manage IT systems should be trained as appropriate to their role.

9.2 Anyone employed (either internally or externally) to write software must be adequately trained and fully aware of any potential security issues. Software that allows user input or data upload any kind should be properly reviewed and security validated.

9.3 If system owners/administrators are not members of the IS department, then they must still be aware of their responsibilities towards information security and should adhere to the University of Portsmouth Information Security Policy, Acceptable Use Policy and all relevant IS advisories.

10. System update

10.1 A very common cause of security incidents is out-of-date software. To reduce the risk of a security incident it is vital that the operating systems and all third party software are up-to-date in terms of patching and release version.

11. Remote access to services

11.1 Remote access services (SSH, Remote Desktop etc.) should be limited as far as possible. Virtual private networking (VPN) is the recommended method for remote access.

12. Configuration errors and testing

12.1 All changes to system configurations will be subject to change control and should be tested before release to ensure that there are no unexpected consequences. Special consideration should be given to configuration changes that increase the likelihood of security incidents.

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