SYSTEMS DEVELOPMENT AND MAINTENANCE

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

As systems are developed and maintained, security vulnerabilities can creep in if the developers and maintainers do not pay close attention to security matters.

This IS Advisory offers guidance on security in development and maintenance. In summary, how to design an application securely, how to implement it securely and finally, how to operate it securely. Security thinking must be all encompassing or it won't work. Obviously there is no point having highly secure infrastructure if your applications are not secure and if the infrastructure team is almost totally unaware that security is important.

The purpose of this IS Advisory is to present basic good practice for systems development and maintenance - it won't answer every question but it will make the reader better able to answer many questions for themselves.

Who is this for?

This IS Advisory is aimed at all personnel who have or are responsible for systems development or maintenance on any system that is owned by the University of Portsmouth.

How does the University check this is followed?

Annual review of the systems development process 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. Security requirements of systems

Security Requirements of Information Systems

Information Security requirements analysis and specification

Securing application services on public networks

Protecting application services transactions

Security in Development and Support Processes

Secure development policy

System change control procedures

Technical review of applications after operating platform changes

Restrictions on changes to software packages

Secure system engineering principles

Secure development environment

Outsourced Development

System Security Testing

System Acceptance Testing

System acceptance testing should include testing of information security requirements and adherence to secure system development practices. The testing should also be conducted on received components and integrated systems. Automated tools, such as code analysis tools or vulnerability scanners, and should be used to verify the remediation of security-related defects. Testing should be performed in a realistic test environment to ensure that the system will not introduce vulnerabilities to the organization's environment and that the tests are reliable.

Security of Test Data

The use of operational 'live 'data containing personally identifiable information or any other confidential information for testing purposes should be avoided. If this is not practical, then all sensitive details and content should be removed or obfuscated.

a) the access control procedures, which apply to operational application systems, should also apply to test application systems;

b) there should be separate authorization each time operational information is copied to a test environment;

c) operational information should be erased from a test environment immediately after the testing is complete;

d) the copying and use of operational information should be logged to provide an audit trail.

2. Security in application systems

2.1 Appropriate security controls, audit trails and/or activity logs should be designed into all application systems.

2.2 Security controls should include the validation of input data, internal processing, and output data.

3. Cryptographic controls

3.1 Cryptographic systems and techniques should be used for the protection of information that is considered at risk and for which other controls do not provide adequate protection.

3.2 Passwords must be encrypted before transmission.

4. Security of system files

4.1 To ensure that IT projects and support activities are conducted in a secure manner, access to system files should be restricted to those IS staff responsible for managing and supporting the various IT systems, services and servers.

5. Security in the development and support processes

5.1 Changes to the University's business systems must be authorised by the Change Management Board, who will ensure that security is maintained.

6. Security of the development and support environment

6.1 Project and support environments should be strictly controlled. Project managers are responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

----

1. Security requirements of systems

1.1 A project team should be established for each major new systems development. This includes infrastructure, business applications, and user-developed applications.

1.2 Security requirements should be identified and agreed prior to the development of information systems.

1.3 The project team is responsible for designing security into the system.

2. Security in application systems

2.1 Appropriate security controls, audit trails and/or activity logs should be designed into all application systems.

2.2 Security controls should include the validation of input data, internal processing, and output data.

3. Cryptographic controls

3.1 Cryptographic systems and techniques should be used for the protection of information that is considered at risk and for which other controls do not provide adequate protection.

3.2 Passwords must be encrypted before transmission.

4. Security of system files

4.1 To ensure that IT projects and support activities are conducted in a secure manner, access to system files should be restricted to those IS staff responsible for managing and supporting the various IT systems, services and servers.

5. Security in the development and support processes

5.1 Changes to the University's business systems must be authorised by the Change Management Board, who will ensure that security is maintained.

6. Security of the development and support environment

6.1 Project and support environments should be strictly controlled. Project managers are responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

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