Information Security Policy

December 2014

University of Portsmouth

Document title			
Information Security Policy December 2014			
Document author and department			**Responsible person and department**
Robbie Walker, Security Architect, Information Services			Andrew Minter, Director of Information Services
Approving body			**Date of approval**
University Executive Board			8 December 2014, Min 14/255
Review date	**Edition no.**	**ID Code**	**Date of effect**
Annual	2	57	9 December 2014

EITHER **For public access online (internet)?** *Tick as appropriate*	**OR** **For staff access only (intranet)?** *Tick as appropriate*
Yes ✓	**Yes** ☐
For public access on request copy to be mailed *Tick as appropriate*	**Password protected** *Tick as appropriate*
Yes ✓ **No** ☐	**Yes** ☐ **No** ✓

External queries relating to the document to be referred in the first instance to the University Secretary: telephone +44 (0)23 9284 3195 or email university.secretary@port.ac.uk

If you need this document in an alternative format, please contact +44 (0)23 9284 5776.

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

www.port.ac.uk/accesstoinformation/policies/informationservices/filetodownload,140133,en.pdf

Contents

Page no.

Information Security Policy

Summary

What is this Policy about?

Information is an important asset which must be handled safely, securely and lawfully. This Policy provides a framework for the management of information security throughout the University. It sets a direction for the secure management of the University's information assets by defining 'core regulations' which must be followed.

Who is this Policy aimed at?

This Policy applies to **anyone** authorised to use University of Portsmouth IT facilities. Generally referred to as 'users', this includes:

- Students and staff.
- External partners, contractors and agents based on-site and using the University network, or off-site and accessing the University's systems remotely.
- Tenants of the University using the University's computers, servers or network.
- Visitors using the University's WiFi.

All users of University information systems must understand their individual responsibilities for protecting information and the systems that process it.

How does the University monitor compliance with this Policy?

This Policy will be reviewed annually to evaluate its effectiveness.

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

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

1. Introduction

The University of Portsmouth is committed to achieving excellence in the creation and communication of knowledge. The information underpinning that knowledge must be accessible when required and protected from theft, loss or damage. However, all information is not of equal value or importance and the steps necessary for protecting University information must be commensurate with risk and compliant with applicable legislation.

2. Structure

This Information Security Policy sets out the core regulations that must be followed by all users of University of Portsmouth information systems. The Policy is supported by a good practice toolkit of 'IS Advisories', which offer professional guidance and suggest a range of possible solutions to technical issues. Always seek advice from Information Services if help is needed in applying any IS Advisory.

3. Scope

This Policy applies to all members of the University (including staff and students) and any authorised third parties who may process information on behalf of the University. All information, IT systems, IT assets and services that are managed, owned or processed by the University are also within the scope of this Policy.

4. Approval and review

Responsibility for the production, maintenance and communication of this Policy document and all supporting IS Advisories, lies with the University Security Architect. It is the responsibility of the Security Architect to ensure that this Policy remains up to date and appropriate. Heads of department are responsible for ensuring that this Policy is understood and followed within their departments.

5. Core regulations

The core regulations are arranged under five headings and an outline of each is given below. New developments in IT are relentless and security must keep pace with progress. Nonetheless, the core regulations are founded on principles that should remain relatively stable as technology and legislation evolve.

- **Governance**
  Users must comply with all legal, regulatory and policy statements applicable to information security.
- **Identity and Access Control**
  Access to network accounts and University data will be carefully controlled to allow authorised access to appropriate resources.
- **Technology**
  Users must not put the University's IT facilities at risk – for example, by introducing malware, interfering with hardware, loading unauthorised software or circumventing security features.
- **Information**
  All users must safeguard the personal data in their care, and show due regard for intellectual property ownership rights and copyright law.
- **Monitoring**
  The University reserves the right to monitor activities on any University IT system for operational performance and security reasons.

6. Governance

6.1 All users of University information must comply with all relevant legislation and regulations governing data protection, privacy and information security.

6.2 Users of University information will be made aware of their individual responsibility for complying with this Policy and about the IS Advisories on information security, through a programme of security awareness training.

6.3 Contractual agreements with third parties involving usage, modification, processing, transmission or management of the University's information assets or information processing facilities, must cover all relevant security requirements, including compliance with this Policy.

6.4 The risks to the University's information assets arising from new IT systems, or from changes to existing IT systems, or from new IT systems hosted or managed by external parties, must be identified and appropriate security controls implemented.

6.5 All identified security requirements must be adequately addressed before access to University information is granted.

6.6 Where acceptable confidentiality provisions do not form part of a contract, an acceptable non-disclosure agreement (NDA) must be put in place to protect University information and intellectual property.

6.7 Before establishing any new or substantially modified program or activity involving the processing of personal information a proper assessment of the risks must be made and a Privacy Impact Assessment (PIA) must be carried out.

6.8 Vital records must be protected from loss, destruction or falsification, in accordance with statutory, regulatory, contractual, and University Records Management Policy requirements.

6.9 Disaster recovery arrangements must be created and maintained for corporate systems.

6.10 This Information Security Policy must be subject to annual review. It may also be appropriate to review this Policy whenever a major risk is discovered, or when very significant changes occur to the University's information assets or infrastructure.

7. Identity and access control

7.1 Only properly authorised users must be allowed access to University IT systems.

7.2 Account passwords and usernames should not be shared without authorisation from Information Services.

7.3 Users should protect their identity by using a strong password and keeping it secret.

8.0 Technology

8.1 The University's IT systems and infrastructure must be secured in a manner commensurate with the identified risks.

8.2 All users must take reasonable steps to reduce the risks to University IT systems and infrastructure.

8.3 All changes to information processing facilities and systems must be subject to change control.

8.4 Operating procedures for IT systems must be documented and maintained.

8.5 Security awareness training must be made available to all users.

8.6 All digital equipment and media must be disposed of securely and safely when no longer required.

8.7 Digital equipment and media containing information must be secured against theft, loss or unauthorised access when outside the University's physical boundaries.

8.8 Information transferred in electronic or digital format must be appropriately secured.

8.9 Access controlled doors or staffed reception desks must be used to protect work areas that contain or are likely to process restricted information.

8.10 Restricted information processed on portable devices and media must be encrypted. The password to an encrypted device must not be stored with the device.

8.11 The University's IT infrastructure, information systems and data must be protected against unauthorised access and disclosure from the internet, using appropriate technology (e.g. firewalls, internet gateways, access control lists (ACLs) or similar security network devices).

8.12 The operating systems and application software running on University servers and network devices must be configured to provide only the services required to fulfil their role.

8.13 The operating systems and application software running on University computers and network devices must be kept up to date and in good order (including software updates and security patches). These patches must be applied in a timely manner sufficient to reduce the risks to an acceptable level.

8.14 Appropriate measures will be put in place to guard against infection from malicious software.

8.15 User accounts, particularly those with special access privileges (e.g. administrative accounts), must only be given to authorised individuals and configured to provide the minimum necessary level of access to applications, computers and networks.

8.16 Mobile digital devices, if used for University business, whether personally owned or supplied by the University must provide adequate security to protect University information and access to University IT systems.

8.17 System owners (i.e. business managers of corporate systems or managers of IT systems owned by faculties, departments or schools) must produce a risk assessment and adequate security management arrangements for the IT system under their control.

9.0 Information

9.1 If restricted documents have to be sent by fax, the sender should ensure they use the correct number and that the recipient is near to the machine at the other end ready to collect the information immediately it is printed. If restricted documents are sent by external post, they must be sent by Special Delivery. The sender must ensure that the envelope is properly secured. If restricted information is to be transmitted by email, then the sender must ensure that the information is encrypted for transit.

9.2 The number of copies made of restricted information, whether on portable devices or media or in hard copy, should be the minimum required. Paper copies must be physically secured in a locked cupboard, drawer or filing cabinet when not in use. When no longer needed, the e-copies should be deleted and any paper copies securely destroyed.

9.3 Copyright controls, terms of use agreements and licence provisions for software or other materials must be adhered to by users.

9.4 Explicit permission from line management must be obtained before removing restricted information from University premises.

9.5 Restricted information must be properly disposed of when no longer required. Digital equipment known to have contained restricted data (or suspected of containing restricted data) must be returned to Information Services for secure disposal at its end of life.

10. Monitoring

Information Services will monitor the University IT network, collecting data on the performance and use of University IT systems. This monitoring is essential for network performance management, incident response and the detection and prevention of malicious activity. Any data collected through monitoring will be kept for an appropriate period depending upon the nature of the data and its intended use.

11. Infringement

Breaches of this Policy may result in disciplinary action.

University of Portsmouth
Information Services
St Andrew's Court
St Michael's Road
Portsmouth PO1 2PR
United Kingdom

T: +44 (0)23 9284 3348
F: +44 (0)23 9284 3700
E: university.secretary@port.ac.uk
W: www.port.ac.uk

MD9914 0215