UNIVERSITY OF PORTSMOUTH

INFORMATION SECURITY POLICY

June 2023

Contents

Document title
Information Security Policy
Document author and department
Rob Walker Information Services
Approving body
UEB
Date of approval
5 June 2023
Review date
5 June 2024
Edition no.
3
ID Code
057
Date of effect
6 June 2023

Document title	
For a) public access online internet or b) staff only intranet?	b)
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://policies.docstore.port.ac.uk/policy-057.pdf

Summary

What Is This Document About?

Information is a vital asset to the University of Portsmouth and it is central to all our activities, including teaching, research, knowledge creation, administration and management. Information is valuable and must be protected from malice, mistakes and mischance - but it must also be readily accessible to those people with a legitimate need to use it.

To achieve these seemingly conflicting goals, we need to think hard about the risks to information and develop acceptable and effective protective measures which match the risks and are adaptable to the demands of a rapidly changing threat environment. This Information Security Policy is key to our success in managing this complex problem. It is an overarching document which sets the direction for the management of information security and describes a framework of supporting policies and standards; ultimately, in support of the University of Portsmouth's strategic objectives.

Who Is This For?

The Information Security Policy applies to all members of the University of Portsmouth and any others who may access or process University information on behalf of the University or as part of a mutual agreement.

How Does The University Check This Is Followed?

This Policy will be reviewed annually to evaluate its effectiveness.

Who Can You Contact If You Have Any Queries About This Document?

Any questions or concerns relating to the terms or implementation details associated with this Policy should be addressed to the Governance Risk and Compliance Group within Information Services.

Executive Summary

This Policy defines a framework of supporting documents (including other policies and standards) which when taken together lay the foundations for achieving risk managed information security. This ensures that University information assets will be appropriately secured against breaches of confidentiality, failures of integrity, or interruptions to the availability of that information. The ultimate aim is to protect the University’s business activities and its strategic goals.

1. Overview

This Policy defines a framework of supporting documents (including other policies and standards) which when taken together lay the foundations for achieving risk managed information security. This ensures that University information assets will be appropriately secured against breaches of confidentiality, failures of integrity, or interruptions to the availability of that information. The ultimate aim is to protect the University's business activities and its strategic goals.

Any questions relating to the interpretation or practical implementation of any terms or actions within this Policy must be addressed to the University Chief Information Officer (CIO) as a matter of urgency. Questions can be made by contacting the Information Services Service Desk (ext 7777 or) using the subject/title: "Policy Question"

2. Purpose

The purpose of this Policy is to provide a statement of intent on how information security will be managed and to reassure all stakeholders involved with the University of Portsmouth that their information is adequately protected and we are minimising the risks to the University's strategic goals.

Compliance with this Information Security and associated framework of policies and supporting standards will be enforced. Failure to take reasonable steps to follow this Policy and its associated policies and standards may result in disciplinary action.

3. Scope

This Policy applies to all members of the University of Portsmouth (meaning all staff - permanent, fixed term, temporary, all students, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged by the University in the UK or overseas).

The scope of this Policy includes the University of Portsmouth IT infrastructure, services and systems, including those hosted in a cloud environment and those provided by a third party under a managed service agreement. In the case of a managed service, responsibility for security will be defined under a service contract. In the "cloud environment" case, responsibility for security will depend on both the service provided and the cloud service model (SaaS, Iaas, PaaS[1]). The table below provides a general overview of how security management responsibilities will be assigned:

[1] SaaS - Software as a Service, IaaS - Infrastructure as a Service, PaaS - Platform as a Service

Service Provided	Cloud Service Model		
	IaaS	Paas	SaaS
Firewalling	Both The UoP and the cloud provider	The cloud provider and possibly the UoP	The cloud provider
Secure configuration	Both the UoP and the cloud provider	Both the UoP and the cloud provider	Both the UoP and the cloud provider
Security update management	Both the UoP and the cloud provider	Both the UoP and the cloud provider	The cloud provider
User access control	The UoP	The UoP	The UoP
Malware protection	Both the UoP and the cloud provider	The cloud provider and possibly the UoP	The cloud provider

4. Policy Aims

Through this Policy, and its supporting documents, the University of Portsmouth aims to:

1. Develop our organisational resilience to cyber attack
2. Protect our digital assets, which if stolen, compromised or damaged would harm our future
3. Develop a constructive and strategic approach to managing information security risks
4. Develop a thoughtful and proactive security culture at all levels in the University
5. Protect our global reputation and international commitments

5. Structure - The Framework Of Policies And Supporting Standards

In addition to this Information Security Policy, the University has created a framework of underpinning policies and standards - which carry equal authority and support this Policy in its practical implementation. All documents within this framework must be considered together as a document set, aimed at ensuring that University information is appropriately secured.

The Information Security Policy Document Set Is Outlined In The Table Below:

Information Security Policy *The overarching Policy that provides the framework for the below policies and supporting standards.*			
Acceptable Use Policy *Describes the activities that are considered to be acceptable or unacceptable use of our IT systems.*	**Secure Systems Policy** *Describes a collection of technical documents defining how IT systems should be securely designed, developed, configured, used and maintained.* *The collection is structured under the categories: People, Process and Technology*	***"Supporting Standards"*** *- Backup Standard* *- Remote Access Standard* *- Monitoring & Logging Standard* *- Change Management Standard* *- Incident Response Standard* *- Data Breach Standard* *- Encryption and Key Management Standard*	**Identity And Access Management Policy** *Defines the provision of appropriate access to systems and information, and prevents unauthorised access.*

6. Policy Statements

All University staff, students and all third parties with access to University information systems and/or data must comply with the following Information Security Policy statements:

1. The information assets managed by the University shall be adequately secured to defend against breaches of confidentiality, failures of integrity or interruptions to the availability of that information; and to ensure we meet all legal, regulatory and contractual compliance requirements.

2. Senior management will provide sufficient management direction and support for information security; aligned to the University's strategic objectives and relevant laws and regulations.

3. To reduce the risk of cyber attack and/or data breaches, a risk management framework will be created to manage information security risks and control the implementation and operation of information security controls within the University.

4. The process of information security management will be subject to ongoing improvement.

5. All members of the University, including staff, students, contractors and 3rd parties must understand their responsibilities in relation to information security. These responsibilities are defined in the University Cyber Security Awareness training programme.

6. Effective security controls will be applied to mitigate the risks associated with the University's collaborative engagements, funding sources and partnerships.

7. Information assets will be identified and protected in accordance with their sensitivity, value and importance to the University. A register of information assets will be created and an asset owner identified for each identified asset. The asset owner will be responsible for defining the appropriate

uses for the asset and ensuring that appropriate security measures are in place to protect it from unauthorised disclosure, modification, removal, or destruction.

8. Access to information and information processing facilities will be facilitated on a need basis to prevent unauthorised access. All information assets will only be made available solely to those who have a legitimate need for access and who are authorised to do so.

9. All members of the University, including staff, students, contractors and 3rd parties must safeguard their authentication information (e.g. usernames, passwords).

10. Cryptography and cryptographic technology will be used to protect the confidentiality, authenticity and/or integrity of information as appropriate.

11. Unauthorised physical access to the University's information and information processing facilities will be prevented with adequate access control systems, to minimise the risks of loss, damage, theft or compromise of IT assets and interruptions to the University's operations.

12. Information systems must be kept up to date with patches and security updates.

13. Information and information processing systems must be protected against malware

14. Information must be backed-up to protect against its potential loss, corruption or malicious encryption.

15. Reasonable logging and monitoring of activities will be employed to detect anomalies and respond quickly and appropriately to potential threats.

16. Internal and external security vulnerability assessments will be conducted on a regular basis.

17. The security of information transferred to and from external agents will be protected with adequately strong cryptographic techniques (e.g. encryption).

18. Information security must be an integral requirement of information systems throughout their lifecycle (from concept and development though to maintenance and final disposal) regardless of how they are delivered and managed.

19. Real (live) data must not be used for testing purposes without the written approval of the CIO.

20. University information assets and systems that are accessible to suppliers must be adequately secured and acceptable levels of information security built into supplier agreements.

21. An effective approach to the management of security incidents, including training exercises will be developed.

22. Information security will be included within the University's business continuity management arrangements.

23. The University will comply with legal, regulatory or contractual obligations related to information security.

24. Security awareness training will be provided to all members of the University, including staff, contractors and 3rd parties; guidance on security policies, procedures, and best practices will also

be available.

25. Information security will be implemented and operated and maintained in accordance with this Policy and other supporting policies and standards.

7. Responsibilities

The following individuals and groups have specific information security responsibilities:

Responsibility for the production, maintenance and communication of the Information Security Policy and all other documents within the security documentation set, resides with the University’s CIO. This Information Security Policy has been approved by the University Executive Board and will be reviewed by the CIO annually. Formal approval of all supporting standards is delegated to the CIO who will consult with other stakeholder groups as appropriate.

The CIO has operational authority for the information security within the University and is responsible for developing policies that underpin the necessary controls. In practice, this is normally exercised by delegation to the Governance, Risk and Compliance Manager.

An Information Security Working Group will be created to oversee the day to day operation of information security, including the planning, implementation, audit and remediation of security controls and risk management.

Information Asset Owners are senior/responsible individuals involved in managing the relevant business area. Their responsibility is to understand what information is held and how that information is processed (i.e. what is added and what is removed, how information is moved, and who has access and why).

Their contextual knowledge is a vital contribution to inform effective risk management in accordance with this Policy.

Users are responsible for making informed decisions to protect the information that they process and the information services and systems they work with. Users must familiarise themselves with the relevant policies governing the information and systems they access and seek advice from Information Services if required.

University of Portsmouth
University House
Winston Churchill Avenue
Portsmouth PO1 2UP
United Kingdom

T: +44 (0)23 9284 3199

E: corporate-governance@port.ac.uk
W: www.port.ac.uk