

INFORMATION SECURITY POLICY

January 2026

Document title	
Information Security Policy	
Document author and department	
Ewa Kolaniak, Cyber Governance Risk and Compliance Manager, Information Security Team	
Approving body	
University Executive Board	
Date of approval	
26.01.2026	
Review date	
15 December 2025	
Edition no.	
4	
ID Code	
057	
Date of effect	
26 January 2026	
For a) public access online internet or b) staff only intranet?	b)
<p>External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk</p> <p>If you need this document in an alternative format, please email corporate.communications@port.ac.uk</p> <p>The latest version of this document is always to be found at: https://policies.docstore.port.ac.uk/policy-057.pdf</p>	

Contents

Summary.....	4
What Is This Document About?	4
Who Is This For?.....	4
How Does The University Check This Is Followed?	4
Who Can You Contact If You Have Any Queries About This Document?	4
Executive Summary.....	4
1. Overview	5
2. Purpose	5
3. Scope	5
4. Policy Aims / Objectives	5
5. Principals	6
5.1 Defence in depth	6
5.2 Zero trust	6
5.3 Least Privilege	6
5.4 Need to Know	6
6. ISMS Structure - The Framework of Policies	6
7. Policy Statements.....	7
8. Responsibilities	8
8.1 Information Security Team	8
8.2 UoP Executive Management Responsibilities	9
8.3 UoP Directors / Managers.....	9
8.4 UoP members (staff, students, contractors etc).....	10
9 Application of information security policies	10
9.1 Additional Documentation.....	10
9.2 Exceptions	10
9.3 Reporting violations and Consequences of non-compliance	10
10 Documentation Management.....	10
10.1 Document review.....	10
10.2 Approvals	10
10.3 Document retention	11
10.4 Document distribution.....	11
11. Monitoring, measurement and analysis	11
12. Management review.....	11

Summary

What Is This Document About?

Information is a vital asset to the University of Portsmouth, and it is central to all its activities, including teaching, research, knowledge creation, administration and management. Information is valuable and as such, it must be protected from malice, mistakes and mishandling. At the same time, it must remain readily accessible to those people with a legitimate need to use it.

As a modern, forward-looking business, University of Portsmouth recognises - at the highest levels -the need to ensure that its business operates smoothly and without interruption for the benefit of our students, staff and other stakeholders. To support this, the University of Portsmouth has implemented and maintains an Information Security Management System (ISMS) with the Information Security Policy serving as key component to its success in protecting University from information security risks. It is an overarching document which sets the direction for the information security management and describes a framework of sub-policies; 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 other stakeholders (staff, students, third parties etc.) who may access or process University of Portsmouth 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 systematically reviewed to evaluate its effectiveness, and regular audits will be planned and conducted to assess compliance levels.

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

Any questions or concerns relating to the terms or implementation associated with this Policy should be addressed to the Cyber and Information Security Team at cybersecurity@port.ac.uk

Executive Summary

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

1. Overview

This Policy defines a framework of documents (including other supporting policies) which when taken together lay the foundations for achieving risk-based information security. This ensures that University information assets will be appropriately secured against breaches of confidentiality, failures of integrity, or interruptions to availability of that information. The primary aim is to protect the University's business activities and support 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 Cyber and Information Security Team. Questions can be made by contacting: cybersecurity@port.ac.uk and 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 across the University of Portsmouth. The aim is to reassure all stakeholders that their business information which at times contains personal information is adequately protected and risks to the University's strategic goals are being effectively minimised.

3. Scope

This Policy applies to all systems, people and processes that constitute the University of Portsmouth information systems (including all staff - permanent, fixed term, temporary, all students, suppliers and other third-parties, sub-contractors, agency workers, volunteers, interns and agents engaged by the University in the UK or overseas as well as board members), who have access to the University of Portsmouth data and / or systems.

The scope of this Policy includes the University of Portsmouth infrastructure, services and systems, including those hosted in a cloud environment and those provided by a third party under a managed service agreement that is used for handling UoP data. 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).

4. Policy Aims / Objectives

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

1. Meet contractual, regulatory and legal obligations, as well as relevant requirements of interested parties relating to information security.
2. Develop organisational resilience to cyber-attacks by implementing pragmatic, effective, and measurable security controls and effective management of incidents and threats.
3. Protect information and information related assets through appropriate management of those assets.
4. Develop and implement a strategic approach to managing information security risks.
5. Foster a proactive security culture at all levels in the University.
6. Continually improve information security practices and capabilities
7. Protect the University's global reputation and international commitments.

5. Principals

5.1 Defence in depth

A “Defence in Depth” approach will be adopted to information security whereby multiple layers of controls are used to ensure that the failure of a single component does not compromise the overall security posture.

5.2 Zero trust

A “zero trust” approach will be applied wherever possible – in strategy, design and system implementation. The main concept of zero trust is never trust, “always verify”. Users and devices will not be trusted by default, even when connected to controlled networks such as the corporate LAN.

Summary of the principles:

- ✓ Know your architecture, including users, devices, services and data
- ✓ Know your User, Service and Device identities
- ✓ Use policies to authorise requests for data or service
- ✓ Authenticate and authorise everywhere
- ✓ Focus your monitoring on users, devices and services
- ✓ Do not trust any network, including your own
- ✓ Choose services designed for Zero Trust

5.3 Least Privilege

The default approach taken must be to assume that access is not required, rather than to assume that it is. Everything shall be forbidden unless expressly permitted.

5.4 Need to Know

Access to information systems shall only be granted for individuals to fulfil their job role.

6. ISMS Structure – The Framework of Policies

In addition to this Information Security Policy, the University has created a framework of underpinning policies - which carry equal authority and support meeting this Policy Objectives.

Each policy within our information security framework is defined by subject matter experts with proven competence in the relevant area. Once formally approved, these policies are communicated to the appropriate audience. The table below outlines the individual policies included in the documentation set, summarising their purpose and identifying the target audience for each. Where applicable, the implementation of each policy may be supported by a procedure - usually written by process owners- which provides detailed guidance on how to achieve the identified objectives.

POLICY TITLE	PURPOSE	TARGET AUDIENCE
Information Security Acceptable Use Policy	To ensure information and other associated assets are appropriately protected, used and managed.	Applies to all
Information Security Identity Access Management Policy	To ensure only authorized access and to prevent unauthorized access to information and other associated assets.	Applies to all
Information Security Secure System Policy	To ensure information security is designed and implemented within the secure development life cycle of software and systems and when in use software is managed securely.	Employees responsible for software development and management
Information Security Vulnerability Management Policy	To prevent exploitation of technical vulnerabilities.	Employees responsible for protecting the organization's infrastructure from malware

7. 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 shall be protected in line with relevant UoP policies 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. Information assets will be identified and protected in accordance with their sensitivity, value and importance to the University.
2. Senior management shall provide sufficient 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 shall be created to manage information security risks and control the implementation and operation of information security controls within the University. The process of information security management shall be subject to ongoing improvement.
4. All members of the University, including staff, students, contractors and third parties shall understand their responsibilities in relation to information security.
5. Access to information and information processing facilities shall be facilitated on a need-to-know basis to prevent unauthorised access and users shall safeguard their authentication information (e.g. username, password).
6. Cryptography and cryptographic technology shall be used to protect the confidentiality, authenticity and/or integrity of information as appropriate.
7. Unauthorised physical access to the University's information and information processing facilities

shall 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.

8. Information and technology assets shall have owners and be inventoried and handled in line with ISMS direction.
9. Security vulnerability assessments shall be conducted on a regular basis and identified vulnerabilities managed appropriately.
10. Information systems shall be kept up to date with patches and security updates.
11. Information and information processing systems shall be protected against malware.
12. Information shall be backed up to protect against its potential loss, corruption or malicious encryption.
13. Reasonable logging and monitoring of activities shall be employed to detect anomalies and respond quickly and appropriately to potential threats.
14. Information security shall be an integral requirement of information systems throughout their lifecycle (from concept and development through to maintenance and final disposal)
15. Real (live) data shall not be used for testing purposes without written approval from the Risk Owner.
16. University information assets and systems that are accessible to suppliers shall be adequately secured and acceptable levels of information security built into supplier agreements.
17. Third party risk assessments shall be conducted for vendors that will access UoP data.
18. An effective approach to the management of security incidents, including training exercises shall be implemented.
19. Information security shall be included within the University's business continuity management arrangements.
20. Security awareness training shall be provided to all members of the University, including staff, contractors and third parties; guidance on security policies, procedures, and best practices will also be available.
21. Information security shall be implemented, operated and maintained in accordance with this Policy and other supporting policies and standards.

8. Responsibilities

8.1 Information Security Team

UoP Senior Management recognizes the importance and criticality of maintaining an agile information security, compliance, and governance. To support and facilitate this, UoP Management has established an Information Security Team, led by the Head of Cyber and Information Security. This team is responsible for driving strategic initiatives, implementing effective controls, and ensuring the University's information assets are protected against evolving threats.

The responsibilities of UoP Information Security are to:

- ✓ Review the status of UoP's information security
- ✓ Design and maintain an information security management system
- ✓ Develop specific methodologies and processes for information security,
- ✓ Define roles and responsibilities for the management of information security
- ✓ Ensure integration of information security with other UoP processes and projects
- ✓ Promote the visibility and awareness of information security within UoP,
- ✓ Coordinate the implementation of specific information security measures,
- ✓ Review, monitor and manage information security incidents (SOC team)
- ✓ Monitor compliance with applicable policies and standards,
- ✓ Conduct risk assessments and provide advice appropriate to support the corporate mission,
- ✓ Perform other essential information security management activities.

In order to maintain knowledge of existing and emerging trends within the information security community, as well as cultivating relationships with industry and law enforcement professionals, UoP Information Security is required to maintain membership in relevant industry groups e.g. JISC.

8.2 UoP Executive Management Responsibilities

University of Portsmouth Senior Management / Executive Management is committed to the following responsibilities:

- ✓ Support Information Security operational goals that are with organizational requirements and strategy
- ✓ Provide clear direction and visible management support for UoP Information Security initiatives,
- ✓ Allocate the necessary resources for successful implementation of UoP Information Security measures,
- ✓ Approve assignment of specific roles and responsibilities for UoP Information Security across the organization,
- ✓ Ensure coordinated implementation of Information Security controls throughout the University,
- ✓ Establish a formal, regular management review to address information security matters.
- ✓ Designated UoP representatives shall participate in the management review meetings, including but not limited to: UoP Executive Management, UoP Information Security, Human Resources, Legal and IT.

8.3 UoP Directors / Managers

- ✓ Overall responsibility for ensuring data that is handled within relevant directorate, area of responsibility / accountability is managed in line with Information Security policy.
- ✓ Promote and manage implementation of approved policies within their Directorates and / or respective areas of accountability / responsibility.
- ✓ Report any violations of information security policies without undue delay to Information Security Team.

8.4 UoP members (staff, students, contractors etc)

- ✓ Responsible for making informed decisions to protect the information that they process and / or own and the information services and systems they work with.
- ✓ Familiarise themselves with the relevant policies governing the information and systems they access and apply guidance provided.
- ✓ Seek advice from Information Security, if required

9 Application of information security policies

The policy statements made in this document, along with the supporting set of policies have been formally reviewed and approved by the University of Portsmouth Senior Management. Compliance with these policies is mandatory.

9.1 Additional Documentation

In order to define more specific information security requirements, it is necessary to create additional, lower-level documentation such as procedures. All such documentation must at a minimum meet the requirements outlined in this Policy and shall not contradict or otherwise void these requirements.

9.2 Exceptions

Exceptions to any part of these documents must be requested via raising a Hornbill ticket to UoP Information Security Team. An exception may be granted for a limited time, only if the benefits of the exception outweigh the increased risks and Information Security will provide relevant advice to the Risk Owner.

9.3 Reporting violations and Consequences of non-compliance

All suspected violations of Policy and all suspected security breaches must be reported without delay to the appropriate UoP entity (Line Manager, UoP Information Security Team) and may result in short-term or permanent loss of access to UoP computing systems. Any attempt to interfere with, prevent, obstruct, or dissuade a worker or to retaliate against a worker in their efforts to report a suspected information security problem or violation is strictly prohibited and may be a cause for disciplinary action. Failure by an employee to comply with these policies may result in escalation process being triggered and disciplinary action being taken in accordance with the organisation's Employee Disciplinary Process. Serious violations may be referred to the Law Enforcement and may result in civil or criminal prosecution.

10 Documentation Management

10.1 Document review

ISMS Policies and other supporting documentation must be reviewed for necessary changes and updated accordingly on a regular basis. Additionally, any time the environment that this document governs changes, change related documentation must be reviewed, approved and documented. Environment changes may include business line changes, additional business capability, and mergers and acquisitions.

10.2 Approvals

UoP INFOSEC Policies are written and implemented under the authority of the Head of Cyber and Information Security, once approved by the UoP Executive Board.

10.3 Document retention

All Information Security Policies must be retained for a minimum of six years. Only Major and Intermediate document versions which have been Approved and Published must be retained. Minor versions and those Major and Intermediate versions which have not been Approved and Published are not subject to retention requirements.

10.4 Document distribution

This Policy, as well as all relevant policies, standards, and procedures, shall be made available to all relevant Users, including vendors, contractors and business partner. Communication process will be in place to facilitate sharing information with interested parties.

11. Monitoring, measurement and analysis

Compliance monitoring activities to ensure all existing ISMS policies listed in this document are implemented correctly, will be performed on a regular basis. When violations are identified, escalation process will be triggered and further decisions taken to eliminate risk.

The methods for monitoring, measurement, analysis and evaluation will be selected to produce comparable and reproducible results to be considered valid.

12. Management review

Management (this includes all University Managers & governance bodies that have an objective or role in information security matters) will be informed about ISMS advancements, risks and changes in needs and expectations of interested parties that are relevant to the ISMS on a regular basis.

University of Portsmouth
Floor 1, Mercantile House
Hampshire Terrace
Portsmouth PO1 2EG
United Kingdom

T: +44 (0)23 9284 3195
E: corporate-governance@port.ac.uk
W: www.port.ac.uk