

---

Technology & Information Services

# **EA-ISP-001 Information Security Policy**

---

Owner: Nick Sharratt  
Author: Paul Ferrier  
Date: 13/03/2015

Document Security Level: **PUBLIC**  
Document Version: 2.5  
Document Ref: EA-ISP-001  
Document Link:  
Review Date: March 2019

## EA-ISP-001 Information Security Policy

### Document Control

Version	Author	Position	Details	Date/Time	Approved by	Position	Date/Time
1.0	Paul Leonard		Initial version	12/03/2012			
2.0	PL, SF, PD, DF, AH		Major updates and amendments	20/07/2012			
2.1	PL, SF, PD, DF, AH, NW		Cloud computing considerations	02/10/2012			
2.2	PL, SF, PD, DF, AH, NW		Document approval	28/11/2012	Academic Board		28/11/2012
2.3	PF	ESA	Updated document in new format and refreshed old elements	19/02/2015			
2.4	PW, AH, GB, CD, PF	IT Director	Approved policy	13/03/2015 14:45	Paul Westmore	IT Director	13/03/2015 11:10
2.41	PF	ESA	Altered document naming for a couple of sub-policies	26/06/2015 15:15			
2.5	PW, GB, NS, PF	IT Director	Reviewed and updated the policy	06/03/2018 15:00	Paul Westmore	IT Director	06/03/2018 17:20

## 1. Introduction

- 1.1 University of Plymouth recognises that information and information systems are valuable assets which play a major role in supporting the University's strategic objectives. Information security is important to the protection of the University's reputation and the success of academic and administrative activities. The management of personal data has important implications for individuals and is subject to legal obligations. The consequences of information security failures can be costly and time-consuming.
- 1.2 The University wishes to support its staff and students in using IT systems safely and securely, and recognises that the ability to protect systems and data is a fundamental enabler for the University's wider Digital Strategy. Promoting an effective security culture will therefore be beneficial to both the institution and the individuals within it.
- 1.3 The Information Security Policy sets out appropriate measures through which the University will facilitate the secure and reliable flow of information, both within the University and in external communications. The approach is based on recommendations contained in ISO 27002 - A Code of Practice for Information Security Management, and relevant legislation including, but not limited to:
  - The Data Protection Act (1998)
  - General Data Protection Regulation (2018)
  - Freedom of Information Act (2000)
  - Copyright, Designs and Patents Act (1988)
  - Computer Misuse Act (1990)
  - Regulation of Investigatory Powers Act (2000)
  - Human Rights Act (2000)

## 2. Aims and Objectives

- 2.1 The principal aim of the Policy is to ensure that all information and information systems within the University are protected to the appropriate level. There are several specific objectives and these are set out below:
  - To ensure all staff, students, contractors and their employees shall have a proper awareness and concern for computer systems security and an adequate appreciation of their responsibility for information security.
  - To provide a framework giving guidance for the establishment of standards, procedures and computer facilities for implementing computer systems security.
  - To support the general objectives of ISO 27002 Code of Practice for Information Security Management.
  - To ensure all staff shall have an awareness of information security related legislation and their responsibilities under it.

## 3. Scope

- 3.1 The Information Security Policy applies to information in all its forms. It may be on paper, stored electronically or other media. It includes text, pictures, audio and video. It covers information transmitted by post, by electronic means and by oral communication, including telephone and voicemail. It applies throughout the lifecycle of the information from creation through storage and utilisation to disposal. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.
- 3.2 For the purposes of this document, information security is defined as the preservation of:
  - **Confidentiality:** protecting information from unauthorised access and disclosure;
  - **Integrity:** safeguarding the accuracy and completeness of information and

# EA-ISP-001 Information Security Policy

- 
- **Availability:** processing methods; and ensuring that information and associated services are available to authorised users when required.
- 3.3 The level of security required in a particular system will depend upon the risks associated with the system, the data held on the system and the working environment of the system.
- 3.4 The policy applies to all staff within the University, contractors and consultants working on behalf of the University and all other individuals and groups who have been granted access to University information systems.
- 3.5 This policy applies wherever information in scope resides, irrespective of where the information is stored or processed.

## 4. Responsibilities and Reporting

- 4.1 All staff, contractors, and students shall be responsible for their role in maintaining information security. Every person shall observe the information security policy and procedures both during and, where appropriate, after leaving the University.
- 4.2 Any observed or suspected security incidents shall be reported immediately where a breach of the University's security policies has occurred. Reports shall be made to the appropriate Head of Department, the owner of the information, or in relation to certain information systems, Technology and Information Services.
- 4.3 Failure to comply with the Information Security Policy will be considered in the context of the University's disciplinary procedures.

## 5. Implementation

- 5.1 All staff shall be aware of the principles, policies and standards that relate to the information handled through their role. Additional training and assistance will be provided if required.

## 6. Relationship with Existing Policies

- 6.1 This Policy has been devised within the context of the following University documents:
- Information Security Classification Policy (EIM-POL-001)
  - Information Handling Policy (EA-ISP-007)
  - Secure Working Policy (EA-ISP-014)
  - Data Protection and Freedom of Information Guidance
- 6.2 The complete Information Security Policy document set comprises of:

Name	ID
Business Continuity Management and Planning Policy	EA-ISP-002
Compliance Policy	EA-ISP-003
Outsourcing and Third Party Access Policy	EA-ISP-004
Personnel IT Policy	EA-ISP-005
Operations Policy	EA-ISP-006
Information Handling Policy	EA-ISP-007
User Management Policy	EA-ISP-008
Use of Computers Policy	EA-ISP-009
System Management Policy	EA-ISP-011
Network Management Policy	EA-ISP-012
Software Management Policy	EA-ISP-013
Secure Working Policy	EA-ISP-014
Encryption Policy	EA-ISP-016

### 7. Review and Amendment

- 7.1 This Policy Statement, and all materials and procedures which emerge as a result of its implementation, will be reviewed at least once a year and, if necessary, amended to maintain its relevance within the University and to ensure continued compliance with relevant legislation.