ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-003 Compliance Policy

Owner:	Nick Sharratt
Author:	Paul Ferrier
Date:	28/03/2018 07:35:00
Document Security Level:	**PUBLIC**
Document Version:	1.03
Document Ref:	EA-ISP-003
Document Link:	
Review Date:	March 2019

EA-ISP-003 Compliance Policy

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.90	Paul Ferrier	Enterprise Security Architect	Created the document	10/02/2014			
0.91	Steve Furnell and Paul Dowland	Head of School of Computing / Senior Professor	Academic Review	February 2014			
0.92	PF, SW, CD, KW	Technical Architecture Group	Conversation around policy and amendments	07/03/2014			
0.93	PF	Enterprise Security Architect	Inclusion of appendix for reference notes				
0.94	AH	Head of S&A	Agreed working draft	09/02/2015			
1.00	PW, AH, GB, CD, PF	Interim IT Director, Head of Strategy & Architecture	Approved document	17/02/2015 16:25	Paul Westmore	Interim IT Director	17/02/2015 13:25
1.01	PF	ESA	Inclusion of IP Policy and Data Retention information	06/03/2015 09:55			
1.02	PF	ESA	Reviewed and updated for 2018	08/12/2017			
1.10	PW, GB, NS, PF	IT Director, HoSM, 2 x ESA	Slight tweak before formal review	06/03/2018 14:35	Paul Westmore	IT Director	06/03/2018 17:20

EA-ISP-003 Compliance Policy

Introduction

This policy forms part of the University's Information Security Policy Set and should be read in conjunction with the Information Security Policy (EA-ISP-001) and other supporting documentation, such as the Information Security Classification Policy.

The Compliance Policy aims to ensure both compliance with legal obligations and compliance with the organisations own information security standards. The policy document sets out the processes for identifying any legal obligations which may bind the organisation; defines measures to avoid any breaches of those obligations; and describes the controls necessary to ensure that the standards in the organisation security policy are met.

1. Awareness of Legal Obligations

1.1 Each core primary data source, for example (but not limited to) the student records or staff records system, an Information Asset Owner and Information Asset Stewards must be identified and documented. These roles will act as local guardians for the specific information assets, they should be business users with expert knowledge of business processes and how the data is used.

1.2 Any concerns that are raised by the introduction or modification of systems, services or processes will be added to either a central Information Security Risk Register of specific project risk registers.

2. Ensuring Compliance with Legal Obligations

2.1 The organisation will comply fully with the requirements of data protection legislation.

2.2 It is the responsibility of all authors who make or publish materials to be aware of the Intellectual Property and Copyright restrictions outlined by the Research and Innovation directorate[1].

2.3 The information created or stored within the organisation's information systems must be retained for no longer than the maximum periods (as denoted in the data retention policy[2]) to meet both legal and business requirements; all staff must adhere to these requirements.

2.4 Any concerns that are raised by the introduction or modification of systems, services or processes will be added to either a central Information Security Risk Register of specific project risk registers. These registers will be maintained and updated with mitigations or acceptance by the relevant areas of the organisation.

2.5 The archiving of documents must take place with due consideration for legal, regulatory or business issues and must be transparent to the users responsible for the archiving process.

2.6 Information regarding the organisation's applicants, students, suppliers and other people dealing with the organisation is to be kept confidential and must be protected and safeguarded from unauthorised access and disclosure.

2.7 The organisation via Human Resources are to ensure that all employees are fully aware of their legal and corporate duties and responsibilities concerning the inappropriate sharing and releasing of information, both internally within the organisation and external parties.

2.8 The Information Security team (or a delegated nominees) are responsible for preparing guidelines to ensure that all staff and students are aware of the key aspects of computer misuse legislation (or its equivalent), in so far as these requirements impact on their duties.

3. Evidence

3.1 Where it is necessary to gather evidence to support an investigation, surrounding a person or organisation, it shall be collected and presented to conform to the relevant rules of evidence. Expert guidance will normally be sought.

---

[1] Research and Innovation - IP Policy

[2] EIM-POL-004 Record Retention Schedule

4. Ensuring Compliance with Organisational Security Policy

4.1 All staff and students are required to comply fully with the organisation's information security policies. The monitoring of such compliance is the responsibility of management at all levels.

4.2 The organisation's systems must be operated and administered using documented procedures in a manner which is both efficient but also effective in protecting the organisation's information security.