ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-013 Software Management Policy

Owner:	Nick Sharratt
Author:	Paul Ferrier
Date:	06/03/2018
Document Security Level:	**PUBLIC**
Document Version:	1.1
Document Ref:	EA-ISP-013
Document Link:	
Review Date:	March 2019

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.9	PF	ESA	Initial version drafted	24/03/2014			
0.91	PF	ESA	Migrated to new document template	10/03/2015			
1.00	PW, AH, GB, CD, PF	IT Director, HoS, EA	Approved Policy	13/03/2015	Paul Westmore	IT Director	13/03/2015 11:55
1.1	PW, GB, NS, PF	IT Director, HoSM, 2x ESA	Updated the policy prior to review	06/03/2018 13:20	Paul Westmore	IT Director	06/03/2018

EA-ISP-013 Software Management 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.

This Software Management Policy sets out how the software which runs on the organisation's information systems is managed. The policy includes controls on installation and use of software, the features provided and the granting of access to software packages. In addition, it covers the maintenance of software, with appropriate procedures for upgrades, to minimise the risk to information and information systems. The policy should be familiar to all staff involved in the specification, installation and maintenance of software.

1. Security Management

1.1 The University's business applications are to be managed by suitably trained and qualified staff to oversee their day-to-day running and to preserve security and integrity in collaboration with nominated individual applications owners. All business application staff shall be given relevant training in information security issues.

1.2 The procurement or implementation of new, or upgraded, software must be carefully planned and managed and any development for or by the organisation must always follow a formalised development process. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls.

1.3 Business requirements for new software or enhancement of existing software shall specify the requirements for information security controls.

2. Change Control

2.1 Formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to business software. All changes must be properly authorised and all software, including that which interacts with the amended software, must be tested before changes are moved to the live environment.

3. Package Software / Systems

3.1 Modifications to vendor supplied software shall be discouraged, only strictly controlled essential changes shall be permitted and the development of interfacing software shall only be undertaken in a planned and controlled manner.

3.2 The University should provide services to deliver operating systems and/or applications where possible, removing the need for manual installations which increase and diversify the application landscape and resources required to manage these environments.

4. Malicious and Mobile Code

4.1 The implementation, use or modification of all software on the University's business systems shall be controlled. All software shall be checked before implementation to protect against malicious code.

4.2 Where the use of mobile code is necessary, appropriate defensive coding practices and peer review prior to launch shall be undertaken.