ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-013-Software Management Policy

Owner:	Adrian Hollister
Author:	Paul Ferrier
Date:	10/03/2015
Document Security Level:	**PUBLIC**
Document Version:	1.00
Document Ref:	EA-ISP-013
Document Link:	http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2015/03/EA-ISP-013-Software-Management-Policy.pdf
Review Date:	March 2016

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

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.

Please refer to the appendix for further explanation of the points below.

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.

Appendix

1. Security Management

Explanatory Notes

All business applications require ongoing management and the managers will be responsible for overseeing their day to day running. The management of business applications necessarily involves a significant amount of security related work.

All organisations will, from time to time, consider replacing or upgrading the applications that support their business processes. The procedures required to carry out the implementation or upgrade need to be properly managed if security is not to be compromised.

An analysis of security requirements must be carried out at the requirements analysis stage of each development project and appropriate security controls must be designed into both the application systems and the operational procedures being supported.

2. Change Control

Explanatory Notes

All software needs to be updated periodically and, whether it is a minor change or major upgrade, the information security issues need to be actively addressed with safeguards to protect the live operations of the organisation. Change control ensures that all changes are analysed, authorised, fully tested and documented before being made available for live or operational use. Procedures should include rules for managing all information assets including program source, operational libraries, old versions and test environments.

When an operating system is upgraded, the supported applications should be reviewed to ensure that there is no adverse impact on security.

3. Packaged Software / Systems

Explanatory Notes

Modifications to vendor supplied software can lead to unforeseen security issues and ongoing information security maintenance overheads when future versions are implemented. Interfacing of such systems with other business applications, by transferring information between them, is usually required. Such processes can put data at significant risk.