ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-011 System Management Policy

Owner:	Nick Sharratt
Author:	Paul Ferrier
Date:	08/03/2018
Document Security Level:	**PUBLIC**
Document Version:	1.10
Document Ref:	EA-ISP-011
Document Link:	
Review Date:	March 2016

EA-ISP-011 System Management Policy

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.9	PF	Enterprise Security Architect	Initial draft created	27/02/2014			
0.91	PF	ESA	Updated to new document format	19/02/2015			
1.00	PW, AH, GB, CD, PF	IT Director, HoS, EA	Approved policy	13/03/2015	Paul Westmore	IT Director	13/03/2015 11:40
1.10	PW, GB, NS, PF	IT Director, HoSM, 2x ESA	Updated policy prior to review	06/03/2018 12:50	Paul Westmore	IT Director	06/03/2018 17:20

EA-ISP-011 System 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 System Management Policy sets out the responsibilities and required behaviour of those managing computer systems, including requirements on the maintenance and management of information systems and the software and service they run. Policies are required to cover all systems in the organisation, whatever the management regime. Some elements of the policy applying to non-critical systems might not need to be as strict as those applying to a high risk system; a risk assessment needs to be made. Policies also need to set out the requirements for system configuration and the implementation of security systems (e.g. antivirus), as well as appropriate logging and monitoring of system activity, and managing capacity.

Reference should also be made to the Software Management Policy (EA-ISP-013) as the policies it defines must also be applied to operating system software.

Definitions

Mobile code	is any program, application, or content (such as a Java Applet) that is transmitted across a network and executed on a remote device.

1. System Management

1.1 The organisation's systems 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 system owners. All systems management staff shall be given relevant training in information security issues.

1.2 The implementation of new or upgraded software must be carefully planned and managed, to ensure that to ensure that any existing or new information security risks are documented, assessed and where required mitigated using a combination of procedural and technical controls.

1.3 Formal change control procedures, with audit trails, must be used for all changes to systems. All changes must be properly tested and authorised before moving to the live managed environment.

2. Access Control

2.1 Access to all systems containing **standard**, **confidential** or **restricted** information shall use a secure logon process to authenticate valid users.

2.2 Access controls shall be maintained at appropriate levels for all systems by ongoing proactive management and any changes of access permissions must be authorised by the manager of the system or application. A record of access permissions granted must be maintained.

2.3 Inactive terminals in high risk locations or serving high risk systems shall log unattended sessions off after a defined period of inactivity to prevent access by unauthorised persons.

2.4 Password management procedures shall be put into place to ensure the implementation of the requirement of the Information Security Policy and to assist users in complying with best practice guidelines.

3. Monitoring System Activity

3.1 Capacity demands of systems supporting existing business processes shall be monitored and projections of future use are made to enable adequate processing power, storage and network capability are provisioned in accordance with business requirements.

3.2 All access to IT services is to be logged and monitored to identify potential misuse of systems or information.

3.3 Security event logs, operational audit logs and error logs must be properly reviewed and managed by qualified staff.

3.4 Access to operating system commands is to be restricted to those persons who are authorised to perform systems administration or management functions. Where appropriate, use of such commands should be logged and monitored.

4. Importing Files

4.1 Files downloaded from the internet, including mobile code and files attached to electronic mail, must be treated with the utmost care to safeguard against both malicious code or inappropriate material. Such files, or any others not known to come from a trusted source, must be scanned for possible malicious code before being executed.

5. System Clocks

5.1 System clocks must be regularly synchronised between the University's various processing platforms.