ENTERPRISE
ARCHITECTURE
WITH
PLYMOUTH
UNIVERSITY

Technology & Information Services

EA-ISP-011-System Management Policy

Owner:	Adrian Hollister
Author:	Paul Ferrier
Date:	17/03/2015
Document Security Level:	**PUBLIC**
Document Version:	1.00
Document Ref:	EA-ISP-011
Document Link:	http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2015/03/EA-ISP-011-System-Management-Policy.pdf
Review Date:	March 2016

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

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.

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 the increased information security risks associated with such changes are 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 environment.

2. Access Control

2.1 Access to all information services shall use a secure logon process and access to high risk systems shall, where appropriate, also be limited by time of day or by the location of the initiating terminal or both.

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 shut down 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.

Appendix

1. System Management

Explanatory Notes

All systems require ongoing management and system managers will be responsible for overseeing their day to day running. Systems management necessarily involves a significant amount of security related work.

It is common for all software and most firmware to require periodic updates and, whether it is a major change or a minor upgrade, changes to active systems need to be handled with care.

Change control is essential: a major upgrade to any system or any change to high risk system should have appropriate levels of management authorisation and provide an audit path to aid subsequent enquiries and investigation.

2. Access Control

Explanatory Notes

Access control standards are the rule which an organisation applies to control access to its information assets. Such standards should always be appropriate to the organisation's business and security needs. The dangers of using inadequate access control standards range from inconvenience to critical loss or corruption of data.

Most computer systems are accessed by a combination of user ID and password. The selection of passwords, their use and management as a primary means to control access to systems and it is necessary to adhere strictly to best practice guidelines. For example, passwords shall not be shared with any other person for any reason.

3. Monitoring System Activity

Explanatory Notes

Measurement of current demands may allow systems to be tuned to make better use of available resources. Projections of future capacity requirements should be made to avoid failures or performance degradation resulting from inadequate processing power, disk channel throughput, network capacity or information storage space. These projections should take account or proposed new facilities as well as current and projected trends in the use of IT.

System access must be monitored regularly to thwart attempts at unauthorised access and to confirm that access control standards are effective. For high risk systems, or where intrusion would have serious consequences, intrusion detection systems should be used.

Records of failed attempts to gain access to privileged facilities and similar security events can give an early indication of unauthorised attempts at intrusion. Audit logs contain details of the changes made to files and to the operational environment, and require close monitoring. Error logs are the reports produced by your system relating to errors or inconsistencies that have arisen during processing and are important sources of information for ensuring proper use of the system. All log files must be protected against modification to ensure that the information they contain is reliable.

The operating system controls a computer's operations; preloaded with it are commands and utilities which set up and maintain the computer's environment. Systems should be hardened to remove access to all unnecessary development tools and utilities prior to delivery to end users.

4. Importing Files

Explanatory Notes

There are significant information security risks when receiving any files (including graphics files of any format), programs, or scripts, etc. from the Internet. It is vital that the information you receive is complete and correct. Take care with electronically supplied data, such as email attachments, in case of possibility of forgery.

5. System Clocks

Explanatory Notes

The need to ensure that where time related information is held within your systems, it is set to Universal Coordinated Time (UTC) with the correct time zone and daylight saving settings and, where possible this should be by automatic reference to a reliable time-server system. Most computer clocks tend to vary in their accuracy, but this should not be significant.

However, if these differences become material, then this may have security implications for the organisation, especially where transaction timing is crucial.