ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-006-Operations Policy

Owner:	Adrian Hollister
Author:	Paul Ferrier
Date:	17/03/2015
Document Security Level:	**PUBLIC**
Document Version:	1.00
Document Ref:	EA-ISP-006
Document Link:	http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2015/03/EA-ISP-006-Operations-Policy.pdf
Review Date:	March 2016

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.9	Paul Ferrier	Enterprise Security Architect	Initial version drafted	08/02/2014			
0.91	AH	Head of S&A	Agreed working draft	09/02/2015			
0.92	PF, RJ, LF	ESA, Change Manager, AIS Manager	Updated document following SM conversations	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 11:20

EA-ISP-006-Operations Policy

Introduction

This Operations Policy sets out how information processing systems are used and managed to protect information security. It includes standard procedures for operations of key systems (including operation by end user departments) and responsibilities of operations in normal conditions as well as fault and incident reporting and review. Processes for assignment of duties to staff, who operate or use sensitive systems, should include consideration of whether segregation of duties is necessary. The policy also includes rules for migration of facilities from development to operational status.

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

1. Physical Security

1.1 Areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security and access control. Staff with authorisation to enter such areas are to be provided with information on the potential security risks and the measures used to control them.

Low Criticality Systems	Medium Criticality Systems	High Criticality Systems
Normal building access and control procedures are adopted.	Facilities are in defined locked rooms with access controlled by key or code. Delivery personnel and visitors are to be supervised.	Facilities are in specially designated areas, with walls and doors of solid construction, security alarms, and access controlled and recorded by an electronic system. Deliveries and enquiries are to separate areas and visitors are accompanied at all times.

2. Procedures and Responsibilities

2.1 The procedures for the operation and administration of the organisation's business systems and activities must be documented with those procedures and documents being reviewed (at least yearly, but must be performed after significant departmental change) and maintained.

2.2 Segregation of duties and areas of responsibility will be imposed to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to the organisation.

3. Security Incidents and Faults

3.1 All security incidents and suspected security weaknesses in the organisations' business operations and information processing systems must be reported based on the categorisation below.

Low Criticality Systems or **Very Small Scale Problem**	**Medium Criticality Systems** or **a Problem affecting more than thirty identified users**	**High Criticality Systems** or **a Problem that has the capability of spreading and affecting a large number of users**
Normal fault reporting to the University Service Desk should be followed.	Incidents or suspected weaknesses to be reported to the Enterprise Security Architect or a member of the Strategy and Architecture team.	Incidents or suspected weaknesses to be reported to the Head of Strategy and Architecture, or the Enterprise Security Architect or a member

		of the Strategy and Architecture team. Central communications disseminated to the Senior Management Team within the University as appropriate by the Senior Information Risk Owner (SIRO) or nominated deputy.
Standard Service Level Agreement applied for investigation.	Prompt response for investigation required.	Immediate response is required and investigation to ensure there is no repetition.

3.2 The reporting of software malfunctions, data inaccuracies and faults in the organisation's information processing systems shall be conducted through the Service Desk. All faults or errors shall subsequently be monitored and timely corrective action taken.

3.3 Mechanisms shall be in place to monitor and learn from those incidents.

4. Changes and Acceptance

4.1 Development and testing facilities shall be separated from operational facilities and the migration of software form development to operational status shall be subject to formal change control procedures.

4.2 Technology and Information Services operate a Change Team that co-ordinate and oversee the change process itself. Changes are assigned one of four classifications detailed below:

Normal			Emergency
Minor	**Significant**	**Major**	
Changes that are not defined as a problem or an incident and are likely to exhibit a known repeatable outcome.	Change are technically complex, have implications for our technical strategy, requires effort and input from a number of people, and/or could seriously impact University operations if goes wrong.	Changes are high risk, large scale, complex, and require significant resource to complete. Changes in this category will be assigned by the Operations – Change Team. Major Changes must be recorded into the Forward Schedule of Change.	Changes that need to be undertaken within a short timescale, often when something critical is not working or non-action could lead to larger problems.

The Change Authorisation Board (CAB) convenes once per week to discuss normal changes and convene when required for emergency changes.
Further details about the change management process are available through the Change Management Collaboration site[1].

4.3 Technology and Information Services operate an Acceptance Into Service process that ensures before entry in the live environment any new or significantly upgraded system is documented in terms of its design, testing and support.
Further details about the Acceptance Into Service (AIS) process are available through the AIS

[1] Change Management Documentation

Collaborate site[2].

4.4 Technology and Information Services operate a Testing process to ensure elasticity, endurance and stresses of systems are undertaken prior to transition to a production state.
Further details about the Testing processes are available through the Test Collaborate site[3].

Test involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place.

5. Project Control

5.1 The security risks to the information assets of all system development projects shall be assessed and access to those assets shall be controlled.

5.2 Security within the Change Management process must be captured as an Impact Assessment provided by the Enterprise Architecture team or nominated delegate.

Security within projects should be assessed throughout the lifecycle of the project and is the responsibility of all parties concerned.

[2] Acceptance Into Service Documentation
[3] Testing (Validation and Verification) Documentation

Appendix

1. Physical Security

Explanatory Notes
Security perimeters should be defined to protect areas that contain information processing facilities, each with appropriate entry controls. The definition of secure areas should extend to offices and work areas as well as those containing IT equipment. Personnel who work in, or have access to, secure areas may inadvertently jeopardise security or be put under pressure to perform unauthorised tasks, such as copying confidential information. The organisation should provide adequate information regarding, and safeguards to prevent, such eventualities.

2. Procedures and Responsibilities

Explanatory Notes
The operational procedures in all departments handling sensitive or critical data should be documented and subject to regular review. For example, it may be appropriate to prohibit unaccompanied access to areas where these types of data are used, or to control the use of recording devices in these areas. Procedures need to ensure the correct and secure operation of information processing facilities and that best practice guidelines are being followed.

There is no way to completely prevent fraud in an organisation. However, segregation of duties is a primary internal control that prevents, or reduces the risk of, errors, irregularities, or unauthorised modification of information. Likewise, dual control is a simple means of ensuring that colleagues perform critical activities as a team and is particularly relevant where the validation of a financial entry is critical. The segregation of duties is also desirable in information system development projects to ensure, for example, that change is properly managed.

3. Security Incidents and Faults

Explanatory Notes
Security incidents and suspected security weaknesses or threats, whether in day to day operations or in IT based systems, must be reported to appropriate management as quickly as possible. The organisation should establish and maintain a formal reporting procedure and an incident response procedure, setting out the action to be taken on receipt of an incident report. All employees and contractors should be made aware of the procedure for reporting security incidents. Resources, procedures and authorities needed to respond promptly and effectively to security incidents must be made available.

The organisation must ensure that it is notified and takes prompt and appropriate action when security weaknesses in software and systems are discovered by external parties. Software vendors frequently publish patches or workarounds for newly discovered vulnerabilities in their software. The organisation may also be informed directly of problems with bespoke software or systems developed internally. A process for responding to these notifications may require prior testing of the patch or workaround on a non-production system. If it is necessary, for this reason or otherwise, to continue to run a production system that is known to be vulnerable to attack then additional measures to protect that system should be considered, for example reducing the service provided or increasing monitoring to detect misuse.

Users of information systems must be encouraged to note and report, usually to a central point, such as an Information Systems' Help Desk, any software or system that appears not to be functioning

correctly, i.e. not as expected or according to specification.

4. Changes and Acceptance

Explanatory Notes
Any changes to operational procedures involving sensitive or business critical information, whether they result from an information system change or process changes within a unit such as Human Resources or Finance, must be analysed and the risks assessed to ensure that the needs of information security have been addressed. Management responsibility for information security should be assigned, changes must have management approval at the relevant level and procedures should be implemented to ensure satisfactory control of the changes.

If systems are not separate, development staff may obtain unauthorised access to sensitive or confidential information and the operational system might suffer as development and testing activities can cause unintended changes to software and data sharing the same environment.

Inadequate control of changes to IT facilities and systems is a common cause of security failures. (Technology and Information Services, Change Management processes refer to this requirement).

Formal management responsibility should be defined and procedures implemented to ensure satisfactory control of all changes to equipment, software or operational procedures.

The criteria for accepting new or upgraded software into operational status should be fully understood prior to commencing the migration. It is essential that systems are fully tested, documented and accepted by the information owner before they are made available for live or operational use. (Technology Information Services, Acceptance Into Service processes refer to this requirement).

Testing should initially only use realistic test data, expressly created for the purpose. However, it may become desirable to use a copy of current data files to compare and validate results against the existing systems, in which case it is imperative that the information security risks are understood and appropriate controls put in place. (Technology and Information Services, Testing processes refer to this requirement).

5. Project Control

Explanatory Notes
If IT projects and support activities are to be conducted in a secure manner, the implementation of all systems that might be used operationally must be properly managed and controlled.

Unless carefully managed, that which begins as a minor database or small set of web pages can migrate into informal systems development effort, but with none of the necessary controls and safeguards to protect the live operations of the organisation.

If bespoke software is written for the organisation, rights and access to the source code and other products must be agreed as part of the development or the organisation risks being unable to use or update its information processing facilities in future.

In any system development project, there is a considerable amount of information that needs to be protected from unauthorised access. Clearly, strict control must be maintained over program source libraries, with amendment only possible by authorised staff, in order to prevent deliberate or

accidental introduction of unauthorised changes. System documentation must also be protected from unauthorised access and test data must be protected and controlled, otherwise test results might be invalid. Access controls are particularly relevant if test data contains personal information.