ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-006 Operations Policy

Owner:	Nick Sharratt
Author:	Paul Ferrier
Date:	28/03/2018 07:35:00
Document Security Level:	**PUBLIC**
Document Version:	1.01
Document Ref:	EA-ISP-006
Document Link:	
Review Date:	March 2019

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, HoSA, EA	Approved policy	13/03/2015	Paul Westmore	Interim IT Director	13/03/2015 11:20
1.10	PW, GB, NS, PF	IT Director, HoSM, 2 x EA	Reviewed policy	06/03/2018 15:45	Paul Westmore	IT Director	06/03/2018 17:20

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 through the development lifecycle.

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.	Facilities are in specially designated areas, with walls and doors of solid construction, security alarms, and access controlled and recorded by an electronic system.
	Delivery personnel and visitors are to be supervised.	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 team.	Incidents or suspected weaknesses to be reported to the Head of Service Management, or the Enterprise Security 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 from 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.	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.
		Major Changes must be recorded in the Forward Schedule of Change.	

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 Service Management 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 is available through the Service Management team 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.

[1] Change Management Documentation

[2] Acceptance Into Service Documentation

Further details about the Testing processes are available through the Service Management team 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 Information Security Team or nominated delegate.

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

[3] Testing (Validation and Verification) Documentation