ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-002 Business Continuity Management and Planning Policy

Owner:	Nick Sharratt
Author:	Paul Ferrier
Date:	06/03/2018
Document Security Level:	**PUBLIC**
Document Version:	1.15
Document Ref:	EA-ISP-002
Document Link:	
Review Date:	March 2019

EA-ISP-002 Business Continuity Management and Planning Policy

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.9	PF	ESA	Initial version drafted	08/02/2014			
0.91	SF, PD	Head of School of Computing, Associate Professor	Added in changes recommended	05/03/2014			
0.92	PF	ESA	Finished the appendix (explanatory notes)	19/03/2014			
0.93	PF	ESA	Moved to new document template	10/03/2015			
1.00	PW, AH, GB, CD, PF	IT Director, TIS HoS & EA	Approved document	13/03/2015	Paul Westmore	Interim IT Director	13/03/2015 11:15
1.10	PF, CD	ESA & EA	Revised document to use new University risk register rating	06/03/2017			
1.15	PW, GB, NS, PF	IT Director, HoSM, 2 x ESA	Updated the document ahead of formal review	06/03/2018 14:15	Paul Westmore	IT Director	06/03/2018 17:15

EA-ISP-002 Business Continuity Management and Planning Policy

Introduction

The Business Continuity Management and Planning Policy sets out the process for assessing and addressing risks to business continuity and defines the responsibilities for preparing and implementing business continuity plans (BCP).

This policy is however, specifically focussed around business that necessitates the use of technology to continue business-as-usual (BAU), it should complement the University's Disaster Recovery & Business Continuity Plan[1], which is held and maintained by Finance and Sustainability.

Usually there will be a number of systems, each with different continuity requirements depending on the level of criticality to the organisation. The risk assessment process to classify systems should be aligned with the organisations risk register that uses the categories very low, low, medium and high, this allows appropriate business continuity plans for each system or classification can then be produced.

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

1. Definitions

Low Criticality Systems	Medium Criticality Systems	High Criticality Systems
Business can continue using manual processes for up to the RTO timescale.		
A replacement for the failed system must be in place within the RPO value.		
Relevant departmental plans accommodate a failure up to the RTO timescale.		
Purchasing strategies/plans incorporate their role in information systems continuity.	Estates, purchasing and insurance strategies/plans incorporate their role in information systems continuity.	
Recovery Time Objective (RTO) The target time to recover your systems and business activities after a disaster has struck.		
Four weeks	Five days	Two days
Recovery Point Objective (RPO) The amount of data loss that is tolerable for the affected systems.		
One week	One day	Four hours
Example System		
Inter Library Loans System	Staff Records System	Digital Learning Environment (DLE)

Changing Criticality	Certain systems may become more critical at certain times of the year than others, for example, the University telephony

[1] University Emergency Business Continuity Plan

	service may be deemed to be of a medium criticality, but during Clearing its criticality may be raised to ensure business as usual will be restored quicker than if left as originally defined.
Defining Criticality	When a system is designed or significantly upgraded (such as a service pack or major release version change) the criticality will be defined for the system and stored for ease of reference at a later date.

2. Initiating the BCP Project

2.1 The Technology and Information Services management team are required to initiate a business continuity plan.

3. Processing the BCP Security Risk

3.1 The Technology and Information Services management team are required to undertake a formal risk assessment in order to determine the requirements that should inform the business continuity plan.

Low Criticality Systems	Medium Criticality Systems	High Criticality Systems
A small sample of systems have been assessed against the most likely risks to occur.	A large sample of systems have been assessed against known risks.	All systems have been assessed against known risks.
Simple steps have been taken to mitigate against obvious risks.	Steps to mitigate against the most likely risks have been identified and implemented where appropriate.	All feasible steps to mitigate against risks have been implemented.

4. Developing the BCP

4.1 The Technology and Information Services management team are required to develop a business continuity plan which covers all essential Information Technology business activities.

Low Criticality Systems	Medium Criticality Systems	High Criticality Systems
There is a documented recovery procedure.	Continuity plan covers: • Recovery procedures for most likely scenarios • Any temporary arrangements	Continuity plan covers: • Recovery procedures for most likely scenarios • Any temporary arrangements • Disaster recovery contracts • Replacement equipment arrangements • Relocations arrangements

5. Testing the BCP

5.1 The business continuity plan is to be periodically tested to ensure that the management and staff understand how it is to be executed.

Low Criticality Systems	Medium Criticality Systems	High Criticality Systems
Continuity plans are tested on a small sample set of systems after any major system change.	Continuity plans are tested on a sample set of systems after any major system change.	Continuity plans are tested on a sample set of systems every six months and after any major system change.

6. Training and Staff Awareness on BCP

6.1 All appropriate staff must be made aware of the business continuity plan and their own respective roles.

7. Maintaining and Updating the BCP

7.1 The business continuity plan is to be kept up to date and retested periodically.

Low Criticality Systems	Medium Criticality Systems	High Criticality Systems
Continuity plans are reviewed periodically, for example, when any major service change occurs.	Continuity plans are reviewed annually.	Continuity plans are reviewed six monthly.