ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-POL-009 - Resilience Policy

Author:	Craig Douglas
Date:	11 July 2014
Document Security Level:	**PUBLIC**
Document Version:	1.0
Document Ref:	EA-POL-009
Document Link:	http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2014/11/EA-POL-009-Resilience-Policy.pdf
Review Date:	October 2015

EA-POL-009 - Resilience Policy

Purpose

The purpose of this policy is to establish and enforce practices for the design and implementation of technology, application and information architecture design going forward, thus minimising the risk of service failure impacting the University and its partners. To achieve adequate continuity of service Plymouth University requires all internal and third party technology service providers to commit to continuity measures; this would ensure that business continuity arrangements for technology meet the needs of the University and its partners in the event of technology failure or incident.

Audience

This policy applies to all members and partners of Plymouth University who are directly involved in the development, creation and maintenance of the enterprise architecture and contributing component architectures.

Scope

This policy applies to all systems that contain technology, application and information components throughout the organisation, including hosted or 3rd party platforms, with particular emphasis on public facing, university wide or business critical systems. Exception may be granted for non-mission critical localised solutions but the steer must deliver resilience in both design and implementation to maintain high availability and productivity through these systems. The table below indicates the classifications of system/service with which new systems must be categorised and the minimum resilience that should be afforded.

Classification	Minimum Resilience Levels
Mission Critical	Resilience must be incorporated across all key components alongside disaster recovery measures being implemented.
University Wide/Public Facing	Resilience should be considered across key components.
Standard/Localised/Point Solutions	Resilience is desirable but not essential for these solutions.

Policy

The design of all solutions shall include the classification of the service or solution being provided and any appropriate resilience factor where applicable, as detailed in the table above. The factors will include (but not limited to), clustered or high availability data sources, load balanced and/or failover capable servers and storage upon which applications or information assets will reside.

Resilience in the communication channels such as network switching, routing and firewall capabilities must also be considered.

Any process facilitating failover between systems must be automated and have no human interaction.

The resilience and failover must be tested at regular intervals to ensure satisfactory operation; these tests must be scheduled and communicated with the business in advance to ensure business continuity.

Enterprise Architecture will not look to retrofit this policy on any live system or service, only when systems, solutions or services are under significant review, or are being introduced to the enterprise shall this policy come into effect.

Failure to comply with this policy will lead to the solution architecture being rejected during Enterprise Architecture review, returned for rework, being placed on hold or managed by a waiver to the Enterprise Architecture.

Exception Management

Exceptions to this policy may be granted using the Enterprise Architecture Waiver Process and will be considered on merit as well as alignment with the overall architecture.

Supporting Documentation

This policy is supported by established Enterprise Architecture documents, namely:

- Enterprise Architecture Principles - Principle 3: Maximise Benefit to the University
  - "Achieving maximum enterprise-wide benefit will require changes in the way we plan and manage information. Technology alone will not bring about this change."
- Enterprise Architecture Principles - Principle 5: Business Continuity
  - "Enterprise operations are maintained regardless of any system interruptions."
- Enterprise Architecture Principles - Principle 7: IT Responsibility
  - "The IT organisation is responsible and accountable for owning and implementing all IT processes and infrastructure that enable solutions to meet business-defined requirements for functionality, service levels, cost, and delivery timing. Decisions should always align back to the requirement of the Business."
- Enterprise Architecture Policy
  - "All Plymouth University information management and technology development, modernisation, enhancement, and acquisitions shall conform to the enterprise architecture and comply with applicable Capital Planning and University budgeting processes. "

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.1	Craig Douglas	Enterprise Architect	Initial Document	11/07/2014			
0.2	Craig Douglas	Enterprise Architect	Updated following peer review	17/07/2014			
0.3	Craig Douglas	Enterprise Architect	Updated Following IT Director Review	07/11/2014			
1.0	Craig Douglas	Enterprise Architect	Approved by IT Director	07/11/2014	Paul Westmore	IT Director	07/11/2014