ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-POL-004 - Production, Testing and Development Systems Separation Policy

Author: Craig Douglas

Date: 3 February 2015

Document Security Level: **PUBLIC**
Document Version: 0.2
Document Ref: EA-POL-004
Document Link: <URL>
Review Date: <Optional: dd/mm/yyyy>

EA-POL-004 - Production, Testing and Development Systems Separation Policy

Purpose

The purpose of this policy is to establish, formalise and enforce practices relating to the use of production, test and development environments within the IT organisation at Plymouth University. It will define clear boundaries of what may and may not be done in each environment and identify how transitions between each may be achieved within the lifecycle of any given system or entity.

Audience

This policy applies to all members of Plymouth University, and it's partners who are involved in the various aspects of service provision of the IT infrastructure, its supported applications and data assets.

Scope

This policy applies to all systems present within the architecture of Plymouth University irrespective of physical location, including hosted or 3rd party platforms.

Policy

Plymouth University has for many years operated with a notional idea of the need for development and test environments to exist alongside the live production environment, however, this has never really been formalised and in order to establish a stable, robust and secure production environment for the future this must be addressed.

To ensure the production environment remains stable, robust and secure, a good rule is not do anything which will affect the availability of services contained within it, this will never be possible; security patches, requests for change, software updates and the addition of new services all have an impact on this environment. Therefore, any changes planned for the live systems must first be tested, this clearly must not be done on live systems, and it must be done within a test environment. The test environment must, as far is practical, mirror the live environment. Where investigations for functionality or solution development work is being undertaken, again the production environment must not be used; additionally the integrity of the test environment would be put at risk and may prevent appropriate system testing prior to acceptance into production, therefore a third environment is required, development. These three environments are defined fully and expanded upon below to include usage constraints required.

Development Environment

As the name suggests, this environment is where systems or components are developed. This area of the infrastructure is completely isolated from all other environments so as to prevent any possibility of interference occurring, this must be done using network segregation as a minimum. In order to be compliant with the Data Protection Act, any data used within this environment must not contain any personally identifiable information. Data sets used must be pseudonymised prior to being introduced into the environment, although consideration should be given to the data classification of any live data.

The infrastructure in this area is transient; systems, servers etc may be created and destroyed as requirements dictate, yet it is still subject to formalised change control mechanisms.

The development environment need not contain any testing facilities beyond those required to assess functional operation of systems or components. Once developed to a level where testing is required to

assess interoperability with other systems for example, the solution should be transferred to the test environment to facilitate this. In order to do so a change request must be raised, it is anticipated that this request should be for a minor change.

Test Environment

The test environment is different in terms of it's infrastructure. It must, as far as is practicable, be a mirror image of the production environment. The only exception to this is in terms of resilience, for example, if the production environment calls for multiple servers for any given function to provide resilience, one would suffice in test, however, if it is a clustered or load-balanced system being tested, a minimum of two servers are necessary.

The testing environment is where systems are tested for interaction etcetera prior to being introduced into production, this includes new developments, upgrades and patching. Everything which is to be introduced into production must be tested here first.

Data sets used in this environment must not contain personally identifiable information, and must therefore be pseudonymised before being introduced into the environment, although consideration should be given to the data classification of any live data.

As stated previously, in order for a system to be accepted into this environment a change request must have been raised and approved. Similarly, in order to progress to the live environment a standard change request must be raised, acceptance into service completed and enterprise architecture compliance met.

Production Environment

The production environment is the key to everything, as stated previously, nothing must be done here which will affect the availability of service. Items entering this environment are subject to change control, acceptance into service and enterprise architecture compliance.

Data in this area is not subject to pseudonymisation, but is subject to data protection and classification restrictions.

Pseudonymisation

Pseudonymisation is the process to enable the University to make use of data sets in a legal, safe and secure manner. The aim is to allow the University (and partner organisations where necessary) to use data for secondary purposes such as system development and testing. This will facilitate the University to no longer use personally identifiable information for tasks which are not directly related to core business activities and allow University business processes to continue to be effective in supporting the day-to-day activities of the organisation.

At the time of writing, the University has no published supporting standards, processes or guidlelines in this area, and these will be developed in time. It is expected that these will align with the Information Governance Toolkit published by the Health and Social Care Information Centre. Until these documents are published advice should be sought from the Enterprise Security Architect for all queries relating to pseudonymisation.

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 2: Compliance With Statutory Obligations
  - "The enterprise must be mindful to comply with all laws, regulations, and external policies regarding the collection, retention, and management of data."
- Enterprise Architecture Principles – Principle 3: Maximise Benefit to the Enterprise
  - "This principle embodies ''service above self ''. Decisions made from an enterprise-wide perspective have greater long-term value than decisions made from any particular organisational perspective. Maximum return on investment requires information management decisions to adhere to enterprise-wide drivers and priorities. No Organisation Unit will detract from the benefit of the whole. However, this principle will not preclude any Organisation Unit from getting its job done."
- 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."
- Enterprise Architecture Principles - Principle 8: Data Security
  - "Security must be designed into data elements from the beginning; it cannot be added later. Systems, data, and technologies must be protected from unauthorised access and manipulation. Vice Chancellor's Executive information must be safeguarded against inadvertent or unauthorised alteration, sabotage, disaster, or disclosure."
- Enterprise Architecture Principles - Principle 9: Data is an Asset
  - "Accurate, timely data is critical to accurate, timely decisions. Most corporate assets are carefully managed, and data is no exception. Data is the foundation of our decision-making, so we must also carefully manage data to ensure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it, in doing so data assets can provide additional value to academic and research endeavours."
- Enterprise Architecture Principles - Principle 10: Data is Shared
  - "Data where applicable, will be available externally to the enterprise. This will afford both rich service provision also the ability to perform research collaboratively with partners."
- Enterprise Architecture Principle – Principle 11: Data is Accessible
  - "Wide access to data leads to efficiency and effectiveness in decision-making, and affords timely response to information requests and service delivery. Using information must be considered from an enterprise perspective to allow access by a wide variety of users. Staff time is saved and consistency of data is improved."
- Enterprise Architecture Principles – Principle 15: Requirements-Based Change
  - "This principle will foster an atmosphere where the information environment changes, in a timely and controlled manner, in response to the needs of the business, rather than having the business change in response to IT changes."

- 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	03/02/2015			
0.2	Craig Douglas	Enterprise Architect	Updated following peer review	23/06/2015			