ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-POL-014 - Hosting Policy

Author: Craig Douglas

Date: 05 September 2014

Document Security Level: **PUBLIC**
Document Version: 2.0
Document Ref: EA-POL-014
Document Link: http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2015/01/EA-POL-014-Hosting-Policy.pdf
Review Date: January 2016

EA-POL-014 - Hosting Policy

Purpose

The purpose of this policy is to establish and enforce practices relating to the provision of hosted services for electronic assets owned and managed by Plymouth University; consideration will be made to minimise the number of hosting entities whilst realising value in terms of offering flexibility in supplier choice based on information security constraints.

Audience

This policy applies to all members and partners of Plymouth University who are directly involved in the creation, delivery, support, maintenance, procurement and supply of systems and services into 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.

Policy

It is recognised that there are many facets to the work carried out at Plymouth University. Each area of the university has requirements which Technology and Information Services will endeavour to meet, either directly or indirectly, examples of these may include, the provision of a web server, some shared storage, the provision of a blogging or document repository to name but a few. A request for resource to facilitate such items can be fulfilled in essence in one of two ways, either on premise or by purchasing the resource externally. Each request must be investigated on its merits and the appropriate location sourced to meet the requirements of the requestor. Certain circumstances mean that (at the time of writing) the only possible solution would be to host the solution internally, these circumstances would generally be because the nature of the data to be stored is of a sensitive nature which may not be appropriate for storage on the internet, or because we are legally or contractually obliged to keep the data within our borders. Another reason could be performance related where latency on the Internet connections may severely impact on the effectiveness of a system. Under all other circumstances, we will look to host the solution externally, as set out in "**EA-POL-008 - Enterprise Architecture Policy – Provision of Commodity IT Capabilities**" and based on sound business judgement decisions.

This policy mandates that when examining a location to host such information, the following are taken into consideration:

- Suppliers must conform to the Government Security Classifications Policy 2014[1], which uses the terms "Official", "Secret" and "Top Secret", these terms can be mapped across to Plymouth University data classifications and should be used as indicated in the table below:

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

PU Classification	Government Classification	Former Government Impact Level (Rough Guide)	Type of Service	Use Case
Public	Official	IL0 (minimum), IL2 (Preferred)	Unassured Cloud Service/Assured Public Cloud	Non-sensitive information suitable for the public domain
Standard	Official	IL2 (minimum)	Assured Public Cloud	Information that is standard in nature and suitable for internal consumption or collaboration with partners.
Restricted	Secret/Top Secret	IL3 or Higher	Formally Accredited Public Cloud, Private Cloud or on premise	Information which must be controlled throughout it's lifecycle and accessed by named individuals only

- Each solution being introduced shall be assessed individually to ensure proposed suppliers meet the minimum security standards
- In recognition that each contract with a supplier must be managed, we will seek to make sound business judgements and in doing so endeavour to keep the number of suppliers to a manageable level, wherever possible, as described in the "**Technology and Information Services Supplier Management Policy**", ideally these suppliers will be able to offer a range of security options relating to the table above.
- Each agreement with a supplier must be negotiated in order to achieve the best value for the University.
- Hosting solutions, must, wherever possible include the option for additional services, such as server maintenance and patching if appropriate to do so.
- 3rd party provided solutions must include resilience, where needed, to prevent downtime or other loss of service, as described in "**EA-POL-009 – Enterprise Architecture Policy – Resilience**".
- Systems must be capable of Single-Sign-On if required.
- The security of data transmission and penetration to detect possible leakage 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.

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 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 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. "
- EA-POL-008 – Enterprise Architecture Policy – Provision of Commodity IT Capabilities
  - "When implementation phases for any piece of work are being considered, it is essential that not only that 3rd party managed services or the "clouding" of software, data and technology (with a managed services wrapper) be considered, it is to be the default option for all IT component provision going forward, when it is sensible to do so."
- EA-POL-009 – Enterprise Architecture Policy – Resilience
  - "The design of all solutions shall include a resilience factor in all relevant areas, such as (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."
- Plymouth University, Technology and Information Services Supplier Management Policy
  - Aims and objectives – "… To minimise the number of suppliers."

EA-POL-014 - Hosting Policy

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.1	Craig Douglas	Enterprise Architect	Initial Document	05/09/2014			
0.2	Craig Douglas	Enterprise Architect	Update Following EAP	16/09/2014			
0.3	Craig Douglas	Enterprise Architect	Addition of IL requirement	15/11/2014			
1.0	Craig Douglas	Enterprise Architect	IT Director Approval	07/11/2014	Paul Westmore	IT Director	07/11/2014
1.1	Craig Douglas	Enterprise Architect	Updated & included classification levels	21/01/2015			
2.0	Craig Douglas	Enterprise Architect	IT Director Approval	21/01/2015	Paul Westmore	IT Director	21/01/2015