ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

# EA-POL-019 – Service Provisioning Policy

| | |
|---|---|
| Author: | Paul Ferrier |
| Date: | 18/12/2017 |
| Document Security Level: | **PUBLIC** |
| Document Version: | 1.00 |
| Document Ref: | EA-POL-019 |
| Document Link: | |
| Review Date: | 12/2018 |

# EA-POL-019 – Service Provisioning Policy

| Document Control | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Version** | **Author** | **Position** | **Details** | **Date/Time** | **Approved by** | **Position** | **Date/Time** |
| 0.9 | Alex Stubbs, EA, ESA, ESAs | Enterprise Security Assistant | Drafted the policy | 07/04/2017 14:05 | | | |
| 0.91 | PF | Enterprise Security Architect | Updated the policy for use now | 24/08/2017 10:55 | | | |
| 0.92 | PF | ESA | Updated following internal comments | 11/10/2017 11:15 | | | |
| 0.93 | PF | ESA | Departmental approval process complete | 24/11/2017 12:30 | Paul Westmore | IT Director | 24/11/2017 12:00 |
| 1.00 | PF | ESA | Virtual approval by ISG | 18/12/2017 11:45 | Information Security Group | | 08/12/2017 12:00 |

# EA-POL-019 – Service Provisioning Policy

## Purpose

The purpose of this policy is to establish and enforce practices for the addition of IT servers, solutions and infrastructure to any environment owned and operated by Plymouth University. There are established policies in place which govern the correct location for services and how they may be created, this policy sets out the correct approach for choosing how services may be provisioned within our environment.

## Definitions

| | |
|---|---|
| Application Owner | a person or group that is accountable for a specific application within an organisation regardless of where the technology components or professional capabilities reside. |
| Device | is a collective term to describe a hardware component, irrespective of the operating system that is used for transmitting, storing, accessing or manipulating university data, including (but not limited to) servers, laptops and desktop computers, network switches and wireless access points. |
| On Premise | within the physical confines of the organisation. |
| Service Owner | a person or group that is accountable for a specific service within an organisation regardless of where the technology components or professional capabilities reside. |
| Services, systems and servers | in the context of this document these refer to all commissioned and provisioned solutions irrespective of the chosen hosting platform(s), service provider(s) or area(s) of responsibility. |
| Service Technical Contact | is a person or group that is accountable for a specific server within an organisation regardless of where the technology components or professional capabilities reside. |

## Principles

**P1.** Selection of services will follow the cloud first paradigm. This will provide alignment with EA-POL-008 - Provision of Commodity IT Capabilities and EA-POL-014 – Hosting policies. Everything as a Service (XaaS) will therefore be the default.

**P2.** New servers will only have a single function. This will aid sustainability, transparency and compliance. Multi-function servers must be avoided, except where the infrastructure or platform is specifically designed for that purpose.

**P3.** All new services will be implemented and maintained against a secure known controlled baseline. This is to provide assurance that system and servers in our environment are of a known security posture. Maintaining agreed baselines for all systems, servers and other devices must be business as usual.

**P4.** All live services will be fully documented, including configuration, purpose, roles and responsibilities, information classification, data flows and a retirement plan. This will aid with trouble shooting, acceptance into service (AIS), statutory compliance and allow for the true cost of the service to be calculated and reported where required. A central IT service catalogue should be maintained within the architectural repository.

## Goals

**G1.** To facilitate the secure provisioning of services. **(P1, P3, P4)**

**G2.** To clearly associate all systems and services to a business function. **(P2, P4)**

**G3.** To clearly associate all servers with a system or service. **(P2, P4)**

**G4.** All servers will have a single function. **(P2)**
**G5.** All services will be configured in a secure and documented manner. **(P4)**
**G6.** To minimise the operating overheads for maintaining service. **(P3, P4)**
**G7.** Lifecycle costs are understood, transparent and available to inform business decisions. **(P4)**
**G8.** Services will be provisioned to be compliant with statutory obligations. **(P2, P3, P4)**

## Objectives

**O1.** All services will be provisioned in accordance with the following University's policies prior to acceptance into service. (**G1, G2, G5, G8)**
**O2.** For all systems and servers, documentation will be sufficient to capture the initial business, application, technology and security architectures, fulfil the requirements for Acceptance into Service (AIS) process, and support data governance activities regardless of service provider. **(G1, G2, G3, G4, G5, G6, G7, G8)**
**O3.** All servers which contribute to the realisation of a service will have a single function by design where possible. **(G4, G8)**

## Responsibilities

| Role | Responsibility |
|---|---|
| SIRO | is responsible for all information and sets the acceptable level of risk of the University's informational estate. |
| IT Director<br><br>(within Technology & Information Services) | has delegated responsibility for the management and security of the University infrastructure, devices and systems provided internally or by its service providers; additionally, delegated responsibility to impose sanctions on devices for non-compliance with this policy is granted. |
| Faculties and directorates | have delegated responsibility to ensure the security of any non-TIS managed devices and systems that they operate (inclusive of any services supplied by a service provider). |
| Technical Design Authority | has delegated responsibility for aligning IT service provision with University vision whilst ensuring the realisation of benefits to the organisation are delivered through the practice of Enterprise Architecture. |
| Enterprise Security Team | has responsibility for monitoring and reporting compliance against this policy, necessary escalations in terms of sanctions and maintain the secure configuration baseline. |
| University staff acquiring service(s) directly from external parties | have responsibility for ensuring all other roles covered by this policy have been engaged to enable them to meet their responsibilities; and responsible for ensuring that services acquired and related content are managed securely. |

## Requirements under this policy

- All services providers MUST:
    - be made aware of University policies, procedures, guidelines, Enterprise Architecture standards and principles pertaining to service provision as described here and in related documents
    - provide documentation necessary to comply with University policies, procedures, guidelines and standards
- Technical Design Authority MUST:

- ensure alignment with the University vision and goals
- meet Enterprise Architecture policy and standards
- ensure that policies, procedures and relevant guidelines are published and available to all appropriate parties

## Supporting Documentation

**EA-POL-008** – **Provision of Commodity IT Capabilities**
This sets out the practices for introducing new or refreshed IT capabilities that could be classed as commodity IT.

**EA-POL-014** – **Hosting Policy**
This establishes practices relating to the provision of hosted services for electronic assets owned and managed by the University of Plymouth.

## Exception Management

Exceptions to this policy may be granted using the Enterprise Architecture Waiver Policy (EA-POL-002) and process will be considered on merit as well as alignment with the overall architecture, business continuity, regulatory and legislative requirements.