ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-POL-012-Data Transfer Policy

Author:	Paul Ferrier
Date:	28/10/2014

Document Security Level:	**PUBLIC**
Document Version:	1.0
Document Ref:	EA-POL-012-Data Transfer
Document Link:	http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2014/11/EA-POL-012-Data-Transfer.pdf
Review Date:	November 2015

EA-POL-012-Data Transfer Policy

Purpose

The purpose of this policy is to establish and enforce practices for secure data transfer to university systems, thus minimising the risk of information leakage or the compromise of systems. Specifically, this policy deals with the transfer of information between internal systems and servers as well as information that crosses our network border to third party service providers.

Audience

This policy applies to all members and partners of Plymouth University who are directly involved in the creation, delivery, support, maintenance of digital information flows to facilitate a personalised experience used for teaching, learning, research or administration of software or services within 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 systems located within the University and/or its service providers afford day-to-day functionality that the university's business relies on. These services and software on their own provide functionality, but without reliable and accurate data transferred in a secured manner to ensure its confidentiality, integrity and availability the effectiveness of the product will be reduced.

The university makes use of services both within and outside of its network perimeter; however the requirements for transferring data should be designed as though it is traversing the perimeter to ensure consistency. Standardisation with secure methodologies, coupled with the removal of any outdated protocols will reduce the risk of data or service compromise.

Secure protocols will always be used in preference over unsecured protocols for data transmission. If no secured protocol is available then a secured tunnelling (IPSec or SSL VPN) technique must be utilised to prevent information being transmitted in plain sight of network users.

When engaging with third party suppliers of service, data transfer between the relevant parties should be conducted with both a secured tunnel serving secured data wherever possible.

Where it is impossible to implement the secure tunnelling of data (as presented above), transmission of data must still be secured and the target system must be completely isolated, in terms of an appropriate technology (such as VLAN segregation) from connectivity to the main University network. Inbound and outbound traffic will be restricted to either a single IP or an address pool and specific ports must be opened solely for legitimate communications to take place.

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 endeavors."
- 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 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	Paul Ferrier	Enterprise Security Architect	Created the policy	14/08/2014	n/a	n/a	n/a
1.0	Paul Ferrier	Enterprise Security Architect	Updated the policy with TIS doc. Standard	28/10/2014 13:14	Paul Westmore	IT Director	07/11/2014 10:00