ENTERPRISE
ARCHITECTURE
WITH
PLYMOUTH
UNIVERSITY

Technology &
Information Services

EA-POL-010-Remote Access Policy

Author:	Paul Ferrier
Date:	12/08/2014
Document Security Level:	**PUBLIC**
Document Version:	1.0
Document Ref:	EA-POL-010-Remote Access Policy
Document Link:	http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2014/11/EA-POL-010-Remote-Access-Policy.pdf
Review Date:	October 2015

EA-POL-010-Remote Access Policy

Purpose

The purpose of this policy is to establish and enforce practices for secure connection to university systems and underlying information, thus minimising the risk of information leakage or the compromise of systems. Specifically, this policy deals with remote connections to both core university systems (inclusive of network infrastructure) and disparate ones such as desktop computers, for the purpose of routine maintenance and/or general remote operations.

Audience

This policy applies to all members and partners of Plymouth University who are directly involved in the creation, development, maintenance and retirement of systems within the enterprise architecture and contributing component architectures, as well as all members of the University accessing any system or systems from remote locations not bounded by the university firewalls.

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 provider locations need to be accessed for various reasons, such as routine maintenance or troubleshooting purposes. Although there are several methods for achieving this, the only approaches for achieving this goal are to either use an IPSec (site-to-site) VPN or a secure (SSL) VPN connection in conjunction with a suitably authorised discretionary user account.

The transmission of non-public classified data across the University's network boundary must be secured at all times. Many service providers and solutions look to use lightweight directory access protocol (LDAP) or Secure LDAP to interact with systems on client premises. At the present time, and for the foreseeable future Plymouth University will not support this type of access, all requests to do so will be refused, therefore alternatives should be sought.

The security of data transmission 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 4: Information Management is Everybody’s Business
    - “To operate as a team, every stakeholder, or customer, will need to accept responsibility for developing the information environment.”
- 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.”
- 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	Initial Document	12/08/2014	n/a	n/a	n/a
1.0	Paul Ferrier	Enterprise Security Architect	Updated the document with new template	07/11/2014	Paul Westmore	IT Director	07/11/2014 10:00