ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-POL-021 - Network Access Protection Policy

Owner:	Adrian Hollister
Author:	Craig Douglas
Date:	20 December 16
Document Security Level:	**PUBLIC**
Document Version:	0.2
Document Ref:	
Document Link:	
Review Date:	

EA-POL-021 - Network Access Protection Policy

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.1	Craig Douglas	Enterprise Architect	Initial Document	20/12/2016			
0.2	Craig Douglas	Enterprise Architect	Updated following peer review	09/01/2017			

EA-POL-021 - Network Access Protection Policy

Purpose

The purpose of this policy is to establish and enforce ownership and practices surrounding the control of devices accessing the University of Plymouth network infrastructure, with the intent of protecting all University systems against unauthorised access and cyber-attack.

Audience

This policy applies to all users of the University's network resources including, but not limited to students, staff, contractors, partners and the general public.

Scope

The intention is to provide a secure computing environment for all members of the University and its partners, as such, the scope of this policy covers all points of access to our network infrastructure; at the border and internally via wired or wireless connections.

Policy

The University of Plymouth invests heavily in its Information Technology estate and processes a great deal of valuable and sensitive data upon it, as such we must look to protect this data from unauthorised access, theft and misuse. Network access protection is one method of achieving the level of protection required. In this context, network access protection is a multi-faceted beast, many different technologies will be brought together to achieve the desired result of being able to protect University resources against cyber-incident whether intentional or not.

Protecting and Guarding Our Borders

University security defences must incorporate the following elements:

- Stateful packet inspection capabilities;
- Data loss prevention measures where appropriate; and
- Analytics for traffic egress and ingress to tailor rules to block threats where required.

Internal Network Connections

All devices connected to the University's network will be subject to a health check before access may be granted to University systems. This will be achieved through a combination of Enterprise Mobility Management (device health check) and Role Based Access controls (end user health check).

Operation

The service owner for all network access protection components is the Enterprise Security team within Technology and Information Services; it is this team that will carry out analytics, define rules and associated policy. Daily operation of the technologies is carried out by Technology and Information Services experts on behalf of the security team. All alterations are subject to change control.

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, business continuity, regulatory and legislative requirements.