ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-012 Network Management Policy

Owner:	Nick Sharratt
Author:	Paul Ferrier
Date:	08/03/2018
Document Security Level:	**PUBLIC**
Document Version:	1.10
Document Ref:	EA-ISP-012
Document Link:	
Review Date:	March 2019

EA-ISP-012 Network Management Policy

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.90	Paul Ferrier	Enterprise Security Architect	Created the document	15/02/2014			
0.91	Paul Ferrier	Enterprise Security Architect	Updated using new template	07/02/2015			
0.92	AH	Head of S&A	Agreed working draft	09/02/2015			
0.93	PF	ESA	Altered point 1.5 to reflect requirements	19/03/2015			
0.94	PF, CD	ESA, EA	Addressed a few areas of weakness	24/03/2015			
1.00	PW, GB, PF	IT Director, HoS, ESA	Approved Document	01/04/2015 13:20	Paul Westmore	IT Director	01/04/2015 13:20
1.10	PW, GB, NS, PF	IT Director, HoSM, 2x ESA	Updated document prior to review	06/03/2018 13:05	Paul Westmore	IT Director	06/03/2018 17:20

EA-ISP-012 Network Management Policy

Introduction

The Network Management Policy sets out how networks are designed and systems are connected to them. It includes a requirement for continued risk assessment and appropriate technical and procedural controls to reduce risk and to meet the requirements of the Information Handling Policy (EA-ISP-007[1]) and also the Remote Working Policy (EA-ISP-014), as well as emergency measures to deal with faults and incidents.

Typically, networks should usually be partitioned to reflect different security requirements, with control points preventing unnecessary traffic flows between and within partitions. Particular attention should be paid to protecting these control points from unauthorised access.

1. Network Configuration

1.1 The network must be designed and configured to deliver the following elements: a reliability to meet the needs of the business whilst providing a high degree of access control and a range of privilege restrictions.

1.2 The network must be segregated into separate logical domains with routing and access controls operating between domains. The levels of control must be commensurate with the access policy requirements of the domains being interconnected.

1.3 The network must be designed to provide defence-in-depth to protect all data, with specific segments being subject to additional security measures.

1.4 The network must afford secured communications between servers through appropriate secure tunnelling techniques.

1.5 The network must be accurately documented at all times[2], when changes are made to hardware (other than an exact replacement) it results in a change to the architecture and must be reported to the Information Security team.

2. Controlling Access

2.1 Access control procedures must provide adequate safeguards through robust identification and authentication techniques.

2.2 Remote connection to the organisation's network and resources should only be permitted when authorised users have been authenticated, data is encrypted during transit across the network, and user access privileges are restricted.

3. Management of the Network

3.1 The organisation's network shall be managed by suitably authorised and qualified staff to oversee its day to day running and to preserve its security and integrity in collaboration with nominated system owners. All network management staff shall be given relevant training in information security issues.

3.2 Moves, changes and other reconfigurations of users' network access points will only be carried out by suitably trained and authorised staff and a full record of all changes will be maintained; this must be auditable by appropriate members of the Service Management team as well as the Information Security team.

3.3 The implementation of new or upgraded software or firmware must be carefully planned and managed, to ensure that the information security risks associated with such changes are mitigated using a combination of procedural and technical controls.

3.4 Formal change control procedures, with audit trails, must be used for all changes to critical systems or

[1] EA-ISP-007 - Information Handling Policy

[2] Payment Card Industry Data Security Standards, requirements 1.1.2 and 1.1.3 stipulate an accurate network diagram (that identifies all connections between the card holder data environment and other networks, including any wireless networks) and (card holder) data flows be maintained

network components. All changes, where appropriate, must be properly tested and authorised before moving to the live environment.

3.5 Access to the resources on the network must be strictly controlled to prevent unauthorised access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised.

4. Physical Security and Integrity

4.1 Networks and communication systems, including data in transit must all be configured and safeguarded against physical or logical attack and unauthorised intrusion.