ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-012-Network Management Policy

Owner:	Adrian Hollister
Author:	Paul Ferrier
Date:	01/04/2015
Document Security Level:	**PUBLIC**
Document Version:	1.00
Document Ref:	EA-ISP-012
Document Link:	http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2015/04/EA-ISP-012-Network-Management.pdf
Review Date:	April 2016

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

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.

Please refer to the appendix for further explanation of the points below.

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 Enterprise Architecture team. The ability to provide effective assessment of security vulnerabilities necessitates accurate information, covering but not limited to:

1.5.1 Software and firmware versions of network hardware

1.5.2 Logical changes to the routing of the network

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 Enterprise

[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

Architecture 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 network components. All changes 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.

4.2 Regular penetration testing must be carried out quarterly and any exposed weaknesses addressed within a maximum of ten working days from notification or discovery.

Appendix

1. Network Configuration

Explanatory Controls

The configuration of the network impacts directly on its performance and affects the stability and information security. For all but the simplest networks, management can be assisted by defining logical domains with firewalls or access controls in routers, as appropriate, operating between the domains.

As the network is the bedrock of all digital communications, it must be accurately represented to inform service or system changes through the Enterprise Architecture system planning lifecycle.

There are certain systems that stipulate an up-to-date an accurate network diagram for regulatory compliance purposes (for example, PCI DSS showing card holder data flows and any connected systems), failure to meet the requirements could result in the organisation being prevented from undertaking credit or debit card based payments.

To prevent standard or restricted data being available to any party who may break the outer layer of defences, encrypted tunnelling for data transmission between servers will ensure that no plain text data can be seen within relevant segments of the network.

2. Controlling Access

Explanatory Controls

In the interests of information security, it might be necessary to restrict access to the network to be only by authorised individuals from well-defined locations. Before allowing use of the network without first authenticating, such as providing an open cybercafé facility, the risks should be fully assessed. The use of a user ID and password as the sole means of access may provide adequate security to enable access to some of the organisation's systems – especially where remote access is permitted.

Remote or mobile users, outside of the organisations perimeter, may need to communicate directly with systems to receive/send data and updates. Such users are physically remote and often connecting through public (insecure) networks. This increases the threat of unauthorised access. Remote access was traditionally provided by means of dial-up or leased phone lines. Today however, Virtual Private Networks (VPNs) provide access across public networks, e.g. the internet.

3. Management of the Network

Explanatory Controls

All but the smallest networks, where changes are relatively infrequent, require ongoing management and a nominated network manager will be responsible for overseeing its day to day running.

It is common for all software and most firmware to require periodic updates and, whether it is a major change or a minor upgrade, changes to active systems must be handled with care.

Change control is essential: a major upgrade to any system or any change to a high risk system (including firmware, software and configuration changes to its critical network components) should have appropriate levels of management authorisation and provide an audit path to aid subsequent enquiries or investigation.

Connections to the network (including remote equipment using VPNs or users' log ons) have to be properly managed to ensure that only authorised devices/persons are connected and, whilst in many

cases this might be primarily an issue for systems design, this can be greatly assisted by appropriate planning and configurations of the network.

4. Physical Security and Integrity

Explanatory Controls

Measures need to be taken to defend the organisations' infrastructure and information stores, including computer hardware against physical damage and unauthorised usage.

Frequent penetration testing can reveal areas of weakness in the network perimeter, these vulnerable areas must be remediated at the earliest available opportunity to prevent informational assets leaking outside of the environment.