SECURITY
WITH
PLYMOUTH
UNIVERSITY

Technology & Information Services

SEC-POL-009 – Vulnerability and Penetration Testing Policy

Author:	Paul Ferrier
Date:	11/07/2017
Document Security Level:	**PUBLIC**
Document Version:	1.00
Document Ref:	SEC-POL-009
Document Link:	
Review Date:	July 2018

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.1	AS	Enterprise Security Assistant	Initial Document	28/11/2016			
0.2	AS, CJD, NS, PF, RB	Enterprise Security Team	Document Review	06/12/2016			
0.3 – 0.53	AS, PF, RB	Enterprise Security Team	Various document revisions	05/01/2017 – 04/05/2017			
1.00	PF	ESA	Approved by Information Security Group	11/07/2017 11:00			

Table of Contents

SEC-POL-009 – Vulnerability and Penetration Testing Policy

Purpose

Plymouth University have an obligation to make sure all services provided by the University and third parties in provision of underlying application portfolio are patched against known vulnerabilities and subject to vulnerability and penetration testing. The purpose of this policy is to outline the discovery and remediation of these vulnerabilities. Any end-point devices not owned by the University are subject to the conditions outlined in "EA-POL-021 – Network Access Control Policy".

Definitions

Device	a hardware component, irrespective of operating system that is used for transmitting, storing, accessing or manipulating university data, including (but not limited to) servers, laptops and desktop computers, network switches and wireless access points.
Patch	a remediation that addresses a vulnerability and prevents it from being exploited, patches (or software updates, fixes or new secured configuration) can be provided by the manufacturer of the product, or can be an alteration in configuration to mitigate the vulnerability, whether it is an operating system, application or piece of infrastructure that transmits or stores data.
Penetration testing	is the practice of testing whether a vulnerability can be exploited on a given device.
System	a piece of equipment which consists of one or more devices.
Service	a collection of systems or devices which together provide a level of business functionality.
Vulnerability	is a weakness which allows an attacker to reduce a system's information assurance. A vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. Vulnerabilities are scored against The Forum of Incident Response and Security Teams (FIRST) Common Vulnerability Scoring System (CVSS)[1].
Vulnerability remediation	
Critical patch	to fix a vulnerability whose exploitation could allow code execution without user interaction. These scenarios include self-propagating malware (e.g. network worms), or unavoidable common use scenarios where code execution occurs *without* warnings or prompts.
High patch	to fix a vulnerability whose exploitation could result in the compromise of the confidentiality, integrity, or availability of corporate or user data, or of the integrity or availability of processing resources.
Medium patch	impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations.
Low patch	impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component.
Informational patch	While not of the utmost importance, informational patches should not be ignored. In combination with other vulnerabilities they can widen a route for exploit or can highlight a concern around the state of a device.
Zero-Day Vulnerability	is a flaw in software, hardware or firmware that is exploitable as soon as or before it becomes generally known to the public.

[1] https://www.first.org/cvss

SEC-POL-009 – Vulnerability and Penetration Testing Policy

Principles

P1. Network discovery and subsequent vulnerability scans will be performed periodically on University owned services, systems and servers. The resultant information will direct any corrective remedial actions. Reducing the vulnerabilities that services, systems and servers are susceptible to will reduce both the likelihood and impact of any exploitation activities being undertaken.

P2. Services, systems and servers hosted by third parties will be subject to compliance reporting and spot checks. These parties will have their own vulnerability scanning processes in place and would not likely expose their infrastructure for third party scanning to take place. Reporting on this compliance should be written into contracts and spot checks performed to ensure that University data hosted by third parties are being protected as would be expected within our own environment.

P3. Systems will undergo vulnerability assessments prior to being transitioned into the production (or live) environment. Any system that is present within the production environment should not pose an unacceptable level of risk to the organisations data protection requirements. Any remedial activities that are identified as part of the assessment must be conducted in order to reduce the risk posed by the system to all other University systems.

P4. Services, systems and servers that are affected by an unacceptable level of vulnerabilities may be subject to penetration testing and/or deeper analysis. The level of acceptable risk will be defined and reviewed by the University's Senior Information Risk Owner and may differ for each level of data classification. Not all information requires the same level of protection, for example, publically classified information must be protected against unauthorised changes being made yet must be accessible to all and be available as much as possible.

P5. Results of the vulnerability scans will be provided to appropriate stakeholders throughout the organisation. Information security is a University-wide concern, protection of all assets must be considered and responsible parties identified, empowered and assisted to carry out their stewardship duties. The implementation of an information assurance framework will promulgate the appropriate culture to protect the University's information throughout its lifecycle.

Goals

G1. All University information will be protected based on its classification to provide an acceptable level of risk. **(P1, P2, P3, P4)**

G2. All University services, systems and servers will undergo vulnerability scans periodically. **(P1, P2, P3, P4)**

G3. Any University service, system or server posing an unacceptable level of risk may be removed from production environment until an appropriate level is obtained and confirmed. **(P4)**

G4. Any information asset owner, steward or server administrator can request an individual assessment of their service, system or server for assurance purposes. **(P5)**

Objectives

O1. Obtain and sustain an acceptable level of information risk based on the vulnerability landscape for the organisation. **(P1, P2, P3, P4)**

O2. Third party providers of service will report on their compliance to assure their protection of University information. **(P2)**

O3. Information protection will be understood, accepted and embedded into service, system and server management by all associated parties. **(P5)**

Responsibilities

Role	Responsibility
SIRO	is responsible for all information and sets the acceptable level of risk of the University's informational estate.
IT Director (within Technology & Information Services)	has delegated responsibility for the management and security of the University infrastructure provided internally or by its service providers.
Faculties and directorates	have delegated responsibility to ensure the security of any non-TIS managed devices and systems that they operate (inclusive of any services supplied by a service provider).
Enterprise Security Team	have responsibility for monitoring and reporting compliance against this policy and necessary escalations in terms of sanctions.
University staff acquiring service(s) directly from external parties	have responsibility including (but not limited to) hosting services for University related content are responsible for the management and security of that environment.
Everyone	has a role to play in information security including the identifying and reporting of vulnerabilities within the University.

Requirements under this policy

In accordance with Objectives 1, 2 & 3 above, responsible parties within this policy must ensure the following in order to protect the University's data:

- All devices under their jurisdiction are maintained at or below the threshold of acceptable risk for the service, system or server;
- All responsible parties must report to the Enterprise Security Team, any inability to comply with the policy for exception management purposes or to request assistance with doing so;
- The Enterprise Security Team will prepare and distribute compliance reports to governing bodies on a regular basis;
- Operational and governance processes will be developed and maintained to facilitate the consistent delivery of the objectives.

Supporting documentation

SEC-POL-001 – **Patching Policy**
This sets out the governance around the required timescales to mitigate published vulnerabilities.

EA-PRC-010 – **Vulnerability Assessment and Remediation Process**
This is a security governance view on how the procedure is operationalised.

EA-POL-021 – **Network Access Control Policy**
This sets out the governance surrounding the logical or physical barriers to prevent authorised access, theft or misuse of University information.

EA-ISP-009 – **Use of Computers Policy**
This is a security governance view on the acceptable use of devices that are connected to the University network.

Sanctions

Failure to comply with this policy may result in either the device being placed into quarantine on the University network or being disconnected in its entirety and potentially lead to disciplinary action for the responsible party.

Policy Exclusions

Personal devices are not covered by this policy, except where they are providing a service to or is integral to the delivery of a service to the University. In addition, any device connecting to the University network is subject to the ***EA-ISP-009 – Use of Computers Policy***.

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.