SECURITY WITH PLYMOUTH UNIVERSITY

Technology & Information Services

SEC-POL-001 - Patching Policy

Author:	Paul Ferrier
Date:	02/02/2018
Document Security Level:	**PUBLIC**
Document Version:	1.65
Document Ref:	SEC-POL-001
Document Link:	
Review Date:	February 2019

SEC-POL-001 - Patching Policy

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
1.0	Paul Ferrier	Enterprise Security Architect	Prepared the document for publication	30/10/2014	Paul Westmore	IT Director	07/11/2014 10:00
1.1 - 1.6	PF	ESA	Overhaul following comments from Head of School of Computing	08/01/2015 - 22/03/2017	n/a	n/a	n/a
1.61-1.64	PF, CD	ESA, EA	Added responsibilities, definitions and standardised language and cloud hosting requirements	24/03/2017 – 20/06/2017			
1.65	PF	ESA	Added compliance programme goal, objective and amended O2 and O3	02/02/2018 10:00	Paul Westmore	IT Director	13/02/2018 12:00

Table of Contents

SEC-POL-001 - Patching Policy

Purpose

Plymouth University has a vast informational estate; all information has a value to the organisation and there are legal requirements associated with keeping this secured. Therefore, it is of paramount importance that the devices storing, transmitting or processing alongside the applications that interact with this information are secured against known vulnerabilities within an appropriate timescale.

The protection of information is only as secure as its weakest element, this could be at a physical level, an operating system level or an application level, all three levels must be considered in conjunction to ensure adequate security is applied where required.

Definitions

Cloud hosting/hosted	refers to a service that is not bound by the physical constraints of the University network; it is hosted by a service provider with greater resources than traditional IT can offer, meaning that services can easily scale up or down and be geographically resilient if required with little impact to users of the service.
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.
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].
Environments	
Developer Sandbox / Staging Environment	is an environment that is specifically used to develop new or adjusted features of a service that does not directly affect live service.
Pre-production Environment	also known as a test environment, is a replica of the live system, aimed at testing code changes before release into the production environment.
Production Environment	also known as a live environment; is a system that provides the business as usual capability to an organisation.
Vulnerability remediation	
Critical rated 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.

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

High rated 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 rated 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 rated patch	impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component.
Information rated 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.

Principles

P1. The protection of our devices and the data they contain, process or transmit is enhanced by being patched up to date. We are patching devices to protect our estate, data and people. Failure to undertake this work may increase the risk of system or service compromise, therefore work is required to maintain this position. Correctly configured devices protect the integrity and confidentiality of the data that they hold.

P2. The patching process will minimise the period that systems and services are at risk. All devices and systems that have vulnerabilities are exploitable. The longer these vulnerabilities are left in situ the likelihood increases that they may be used as a vector for ingress or onward access other systems.

P3. The patching process will maximise the availability of service. Correctly configured and patched devices will reduce the risk of downtime due to compromise. All devices and systems will be subject to downtime to allow any patches to be installed or configuration changed accordingly.

P4. The patching of cloud hosted solutions will be covered as part of the contract of service provision. Irrespective of where the service is hosted it is still important that it is secured to protect the information that it holds. Service contracts must include patching windows that are appropriate in timeframe and duration to maintain security while not excessively impacting service users.

Goals

G1. To secure University devices against threats posed by inherent vulnerabilities.

G2. To achieve and maintain patching compliance requirements for target services and systems in terms of cyber security certification.

Objectives

O1. All University devices that are in scope of any certification programme will be protected within their proscribed patch management timescales. **(P1, P2, P3, P4)**

O2. Regardless of **O1**, all University devices will be patched against critical and high rated vulnerabilities within one month of disclosure. **(P1, P2, P3, P4)**

O3. Regardless of **O1**, all University devices will be patched against medium and low rated vulnerabilities within three months of disclosure. **(P1, P2, P3, P4)**

O4. Ensure or maintain the patching of cloud hosted solutions commensurate with the timescales laid out in this policy where possible. **(P1, P2, P3, P4)**

O5. To assess and remediate zero day exploits/vulnerabilities within two working days of patch identification. **(P1, P2)**

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, devices and systems provided internally or by its service providers; additionally, delegated responsibility to impose sanctions on devices for non-compliance with this policy is granted.
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	has 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 for ensuring hosting services and related content are managed securely. They also have a duty of care to ensure that contracts include windows of downtime and/or are resilient in order that while patching is undertaken the service is always available.
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, 4 & 5, responsible parties within this policy must ensure the following in order to protect the University's data:

- All devices under their jurisdiction are patched;
- 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 as described in ***SEC-POL-009 – Vulnerability and Penetration Testing Policy***;
- Operational and governance processes will be developed and maintained to facilitate the consistent delivery of the objectives.

Supporting documentation

SEC-POL-009 – Vulnerability and Penetration Testing Policy (Internal staff only)
This sets out the governance around vulnerability and penetration testing.

EA-PRC-010 – Vulnerability Assessment and Remediation Procedure (Internal staff only)
This is a security governance view on how the procedure is operationalised.

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.

EIM-POL-001 – Information Security Classification Policy
This sets out the governance around how different classifications of data should be protected to preserve its confidentiality, integrity and availability.

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 leading 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.