SECURITY WITH PLYMOUTH UNIVERSITY

Technology & Information Services

SEC-POL-011 – Anti-Malware Software Policy

Author: Alex Stubbs

Date: 10/08/2017

Document Security Level: **PUBLIC**
Document Version: 1.00
Document Ref: SEC-POL-011
Document Link:
Review Date: August 2018

SEC-POL-011 – Anti-Malware Software Policy

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.1	Alex Stubbs	Enterprise Security Assistant	Initial Document	26/09/2016 14:54			
0.9	PF, AS, RB, CD	ESA Team	Various updates	19/05/2017 – 10/08/2017			
1.00	PF	ESA	Addition of infection quarantine timescales	17/08/2017 09:15	Paul Westmore	IT Director	17/08/2017 09:15

Table of Contents

SEC-POL-011 – Anti-Malware Software Policy

Purpose

The University has an obligation to protect its services, systems and infrastructure against malicious software. Protection must be provided to prevent contaminated devices spreading infection which may lead to disruption across the organisation. Anti-malware is the last line of defence on a device connected to the organisations network, therefore it is an important element in order to try and stop a threat that has not been halted by another defensive mechanisms.

Definitions

Anti-malware	is a collective term used to protect an end-point device against malicious software
On access scanning	is the real-time scanning of files that are being actively used on a device

Principles

P1. The University managed devices will have anti-malware installed, actively running (on access scanning) and updating on a frequent basis. The presence of malware on a device can provide a foothold for unauthorised access, alteration and/or information loss. If anti-malware is not installed, maintained and operational then it is not providing the appropriate protection to the information.

P2. Infected devices will be quarantined, where deemed appropriate and in accordance with Service Desk incident response times. This will prevent infection spreading across the network. Any identified device will have no access to internal resources, yet outbound access to the Internet will be provided in order for remedial actions to be taken.

P3. Any software selected as a corporate anti-malware solution must be capable of supporting the security landscape over and above anti-malware scanning. Logs generated from enterprise grade anti-malware products provide a wealth of knowledge to aid the complete understanding of our threat landscape. The collection of security and event logs provide visibility over the informational estate and allow for corrective measures to be taken as and when problems arise; these logs must be consumable by other security aggregator tools.

Goals

G1. To secure the University's network by minimising its vulnerability to active threats.

G2. To provide visibility of malware threats to appropriate parties.

Objectives

O1. Install and maintain enterprise capable anti-malware on all corporately managed devices. **(P1, P3)**

O2. An appropriate network area is provided to receive devices requiring isolation. **(P2)**

O3. Ensure the selection of a corporate anti-malware product can support the enterprise view of security. **(P3)**

Responsibilities

Role	Responsibility
SIRO	is responsible for all information and sets the acceptable level of risk of the University's informational estate.
IT Director	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 disseminate foundation level information to their students on how to protect their own (and the University's) data; they also have delegated responsibility in order to maintain secure systems, services and servers that are not centrally managed.
Enterprise Security Team	has responsibility for: • advising of appropriate software for anti-malware protection across the environment; • analysing security logs and advising of any corrective measures that may need applying; • defining University-wide policies to protect its systems, services and underlying data.
IT Service Management	has responsibility for installing and maintaining anti-malware software and associated network components as described within this policy.
Everyone	has a role to play in information security and ensuring that their personal devices are not infected with malware.

Requirements under this policy

In accordance with the objectives stated in this policy, responsible parties must ensure the following in order to protect the University's data:

- Install and maintain contemporary anti-malware software;
- Configure and maintain a quarantine network;
- Ensure all logs from corporate software are captured and available for interrogation is required;
- Periodic review of events and log files.

Supporting documentation

EA-ISP-009 – Use of Computers Policy
Sets out the governance around computer usage throughout the organisation.

EA-POL-020 – Network Protection Policy
Sets of the governance surrounding the protection of the organisations 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 leading to disciplinary action for the responsible party.

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.