Malicious Code Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	11/09/2019
V 1.0	Andrew Clarke	Approved PWG	16/09/2019

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

This document requires the approval from BUL as defined in the ISMS Compliance document.

A Clarke	Mick Jenkins
Document Owner: Andrew Clarke	Document Approver: Mick Jenkins
Cyber & Information Security Manager	Chief Information Security Officer

Document Distribution

Name	Title	Version	Date of Issue

Contents

1. About this document

1.1 Purpose of Document

This Policy establishes the area within Brunel University London covering protection against malware and malicious code.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Client Computing Manager	Is responsible for ensuring that the University's selected anti-malware software is installed and maintained on client managed service infrastructure
Systems Manager	Is responsible for ensuring that the University's selected anti-malware software is installed and maintained on Server infrastructure
College IT	Are responsible for ensuring that the University's selected anti-malware software is installed and maintained on College acquired client and server infrastructure that falls outside of the client managed service infrastructure.
All Users	All users have specific responsibilities, defined in this Policy (Malicious Code and Malware Policy), Acceptable Use Policy and the Email Use policy

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A12 – Operations Security
ISO 27001:2013 Conformance Control	Information Classification Objective A.12.2 – Protection from Malware

1.4 Scope

The University's policy against malicious code and malware covers all the University's network assets, including hardware, and software, and applies to all employees, contractors, temporary workers and third parties who use, work with or connect to University information processing facilities.

1.5 References

BUL-POL-12.2.1 - Malicious Code and Malware Process
BUL-POL-6.2- Mobile Computing Policy

2.0 Policy against Malicious code

2.1 The University acts to protect the integrity of its software and its other information assets against the introduction of malicious code (malware) in its Test, Development, Operations and Production environments.

2.2 The University formally prohibits the use, on any information processing system or device it owns or operates, of any software whose procurement was not approved by the Head of Infrastructure and Operations.

2.3 Software and any other files or folders, may not be transferred or downloaded onto the University's network via or from external networks, or on any media (including CD-Roms, USB sticks), including during maintenance and emergency procedures, unless specific controls have been implemented to check the integrity of the file(s) either using sandboxing capabilities[1] provided by Cyber for media checking, verifying the source and integrity of the software, patch or file using a digital signature or some form of checksum or the individual validating the integrity of the file(s) using the local anti-malware software capabilities before opening the file(s).

2.4 The University recognises that the effective operation of the Internet depends on the use of mobile code and therefore allows the restricted use of mobile code. Permitted mobile code and any restrictions are documented in the Authorised Operating Software document [Lead Technical Architect].

2.5 Management may monitor, detect and delete unauthorised software from University assets, and disciplinary action will be taken against anyone in breach of this Malicious Code policy.

2.6 The University acts to automatically identify and patch software and system vulnerabilities in order to reduce the risk of malware attacks, this includes the patching of approved mobile code and offline virtual machines.

2.7 The installation and maintenance of approved anti-malware software MUST be correctly installed and configured on all supported (managed or owned) endpoints and servers across all University networks.

2.8 Anti-malware software MUST be kept up to date including the definitions files. Anti-malware software updates MUST be deployed across the network automatically following their receipt from the vendor and it must be configured to check for these updates every 60 minutes daily. Virus and malware signature updates MUST be deployed across the network automatically following their receipt from the vendor and it must be configured to check for signature updates every 10 minutes daily. All the endpoints must be configured with the secondary anti-malware update server so if a device is not checked in on the corporate network then updates will be installed from the secondary server.

[1] A sandbox is an isolated testing environment that enables users to run programs or execute files without affecting the application, system or platform on which they run. Sandboxes are also used to safely execute malicious code to avoid harming the device on which the code is running, the network or other connected devices. Using a sandbox to detect malware offers an additional layer of protection against security threats, such as stealthy attacks and exploits that use zero-day vulnerabilities.

2.9 Anti-malware software MUST be configured for real time scanning and regular scheduled scans. On-access scanning MUST be configured within Anti-malware software for removable media and websites.

2.10 All users are required to accept, in terms of their User Agreements, the Brunel Acceptable Use policy (BACUP) and the email Use Policy rules and to receive appropriate training in detecting and responding to malware attacks and, where appropriate, to accept specific anti-malware prevention controls.

2.11 Business continuity plans are required to make specific provision for recovering from malware attacks.

2.12 The Information Security Incident Management procedure is required to make specific provision for responding to malware attacks.

2.13 Management will take adequate steps to ensure that it is aware of and can respond to changes in the malware threat environment.

2.14 Anti-malware server MUST be monitored on a daily basis by a nominated staff within the IS Operations team for virus alerts and any issues which cannot be resolved remotely via centralised management console must be escalated to the IS Service Desk where an incident will be raised and a technician assigned to immediately investigate.

2.15 In the event of a virus infection which infects multiple devices (more than 3 devices) at the same time. A root cause analysis report should be completed by the IS Operations team for the Cyber & Information Security Manager.

2.16 Monthly Anti-Malware compliance reports MUST be provided to the Cyber & Information Security Manager by the third working day of the month. In the event that systems are found to be non-compliant a report including suggested remediation will be created which will be provided to the Cyber & Information Security Manager.

2.17 Tamper protection MUST be enabled to prevent end users or malware altering the anti-virus software's configuration or disabling the protection.

2.18 All IT equipment and removable media MUST be scanned for viruses and malware before being introduced or prior use on the corporate network, system or device (see 2.2).

2.19 Users MUST not accept, or run, software from non-trusted sources.

2.20 Users must not undertake any activities with the intention to create and/or distribute malicious programs (e.g. viruses, worms, Trojans, e-mail bombs, etc.) into corporate network(s) or system(s).

2.21 Users MUST inform the IT Service Desk immediately if a virus is detected on their system.

2.22 IT system(s) infected with a malware/virus that the anti-malware software has not been able to deal with MUST be disconnected/quarantined from the University network until virus free.

3.0 Exceptions

3.1 Exceptions to this anti-malware policy require a formal documented risk assessment including steps taken to mitigate the risk and formal approval from the Chief Information Security Officer. Once approved, exceptions will be implemented via the Change Management process.

3.2 Any server or workstation that do not comply with policy must have an approved exception recorded in the Anti-Malware exceptions file detailing the reason for the exception and the steps taken to mitigate the risk.

3.3 Systems will only have exception to the policy if scheduled updates or patches are deemed likely to cause major disruption to the system, resident software or service functionality or to facilitate problem diagnosis. All systems recorded within the Anti-Malware exceptions file must be reviewed on a quarterly basis by the Cyber & Information Security team and the risk will be re-evaluated.

4.0 Non-Conformance

4.1 Any system or workstation found to be without adequate protection as defined by this policy will be removed from the network until adequate protection is implemented.

4.2 Any user being found to be wilfully violating the anti-virus policy may be subject to one or more of the following sanctions:

- Removal of any equipment used from the network until adequate protection is implemented
- Revocation of rights to access University systems
- Any costs incurred by the IS department to remove the virus may be passed on to the department or organisation responsible for the outbreak
- Disciplinary action

Appendix A – Glossary of terms

Adware	Software that automatically plays, displays, or downloads advertisements to a computer, often in exchange for the right to use a program without paying for it. The advertisements seen are based on monitoring of browser habits. Most adware is safe to use, but some can serve as spyware, gathering information about you from your hard drive, the websites you visit, or even your keystrokes. Certain types of adware have the capability to capture or transmit personal information.
Antivirus Software	A type of software that scans a computer's memory and disk drives for viruses. If it finds a virus, the application informs the user and may clean, delete, or quarantine any files, directories, or disks affected by the virus. The term antimalware is preferred because it covers more threats.
Browser Hijacker	A type of malware that alters your computer's browser settings so that you are redirected to websites that you had no intention of visiting. Most browser hijackers alter browser home pages, search pages, search results, error message pages, or other browser content with unexpected or unwanted content.
Dat Files	Also known as a data file, these files are used to update software programs, sent to users via the Internet. .DAT files contain up-to-date virus signatures and other information antivirus products use to protect your computer against virus attacks. .DAT files are also known as detection definition files and signatures.
Keylogger	Software that tracks or logs the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. This is usually done with malicious intent to collect information including instant messages, email text, email addresses, passwords, credit card and account numbers, addresses, and other private data.
Malware	A generic term used to describe any type of software or code specifically designed to exploit a computer or the data it contains, without consent. Malware includes viruses, Trojan horses, spyware, adware, most rootkits, and other malicious programs.
Phishing	A form of criminal activity using social engineering techniques through email or instant messaging. Phishers attempt to fraudulently acquire other people's personal information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. Typically, phishing emails request that recipients click on the link in the email to verify or update contact details or credit card information. Like spam, phishing emails are sent to a

	large number of email addresses, with the expectation that someone will act on the information in the email and disclose their personal information. Phishing can also happen via text messaging or phone.
Ransomware	Malicious software created by a hacker to restrict access to the compute system that it infects and demand a ransom paid to the creator of the malicious software for the restriction to be removed. Some forms of ransomware may encrypt files on the system's hard drive, while others may simply lock the system and display messages to coax the user into paying.
Spam	An unwanted electronic message, most commonly unsolicited bulk email. Typically, spam is sent to multiple recipients who did not ask to receive it. Types include email spam, instant messaging spam, web search-engine spam, spam in blogs, and mobile phone-messaging spam. Spam includes legitimate advertisements, misleading advertisements, and phishing messages designed to trick recipients into giving up personal and financial information. Email messages are not considered spam if a user has signed up to receive them.
Spyware	Spyware spies on a user's computer. Spyware can capture information like web browsing habits, email messages, usernames and passwords, and credit card information. Just like viruses, spyware can be installed on a computer through an email attachment containing malicious software
Trojan	Malicious programs disguised as legitimate software. Users are typically tricked into loading and executing it on their systems. One key factor that distinguishes a Trojan from viruses and worms is that Trojans don't replicate.