





Information Security Management System ISO/IEC 27001:2013

MALWARE POLICY

POLISI MALWARE



ORIGINAL COPY

For PTM Use Only	Version 1.4	Date: 26 th July 2019
Written By: Cik Junnaini Ismun Bahagian Pengurusan Pusat Data	Verified By: Nor'ain Mohamed Wakil Pengurusan Keselamatan Maklumat (ISMR)	Approved By: Asiah Abu Samah Pengarah Pusat Teknologi Maklumat

 UNIVERSITI MALAYA	MALWARE POLICY POLISI MALWARE	
Doc No : UM-ISMS-POL-PTM-009	Version 1.4	Effective Date : 6th Disember 2019

Revision History

No	Date of Change	Description	Page	Version	Approved By
1	1 st Oct 2014	Change in name of policy	Header	1.1	Dr David
2	1 st Oct 2014	Change MS ISO/IEC to ISO/IEC	Cover	1.1	Dr David
3	25 th Nov 2014	Inserted TERHAD logo	Header	1.2	Dr David
4	5 th May 2015	<ul style="list-style-type: none"> • Inserted Clause – 3.9 This Policy also complement to Malware Policy for UM. • Add 2 Purposes • Add 12 Policies 	2,3,5	1.3	Dr David
5	2 nd June 2015	Added policy statement on responsibility of users to ensure their computers are installed with anti-malware software (item 3.1)	2,4	1.3	Dr David
6	30 th July 2015	Changed name of ISMR	Cover page	1.3	Dr David
7.	1 st Oct 2015	<p>Changed “The policy applies to all computers owned by UM, including but not limited to...”</p> <p>to :</p> <p>“The policy applies to all devices that are allowed to connect to UM network, including but not limited to...”</p>	2,4	1.3	Dr David
8.	25 th July 2019	Reformatting policy based on ISMS Document Guidelines	Entire Document	1.4	Asiah Abu Samah
		Reviewed statement 3.1, 3.2, 3.8 & 3.15	2, 3 & 4		
		Remove statement 3.9, 3.10, 4.0	3 & 4		
		Remove BM version 1.0 -4.0	5-7		

 UNIVERSITI MALAYA	MALWARE POLICY POLISI MALWARE	
Doc No : UM-ISMS-POL-PTM-009	Version 1.4	Effective Date : 6th Disember 2019

1.0 Purpose

The purpose of this policy is to :

- a) Establish requirements which must be met by all computers connected to UM networks to ensure effective virus and other types of malware detection and prevention.
- b) Provide guidance for the user to harden and strengthen their computer to protect against viruses and hackers.
- c) Minimising ICT security incidents involving users' computer.



2.0 Scope

The policy applies to all devices that are allowed to connect to UM network, including but not limited to desktop computer, laptops and servers.

However, the scope for ISMS certification only covers desktop computer, laptops and servers belonging to Centre for Information Technology (PTM) and located in PTM premises.

3.0 Policy

- 3.1. Users must install licensed anti-malware software provided by PTM, Responsibility Centers (PTj) or individually purchased in their computers and schedule to scan at regular intervals.
- 3.2. Anti-malware software automated or real-time scanning feature must be enabled and configured to scan on periodic basis such as daily or weekly.
- 3.3. Anti-malware software and malware signature must be kept up-to-date.
- 3.4. Malware-infected computers must be cleaned immediately upon the detection of malware either automatically or manually.
- 3.5. Malware-infected computers must be isolated from the UM network until they are cleaned and verified as malware-free.

 UNIVERSITI MALAYA	MALWARE POLICY POLISI MALWARE	
Doc No : UM-ISMS-POL-PTM-009	Version 1.4	Effective Date : 6th Disember 2019

- 3.6. Users are responsible to ensure files or external media devices used are free from malware. They should scan all external drives before connecting to their computers.
- 3.7. Any activity with the intention to create or distribute malicious programs into UM networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.
- 3.8. Activities that require the usage of malicious programs, such as for the purpose of research and testing, must be approved by the management.
- 3.9. Avoid opening files or email attachments received from unknown parties or unreliable sources. Delete the emails and the attachments immediately and make sure it is also deleted from "trash".
- 3.10. Delete all unnecessary emails, spam email and chain emails . Do not send or forward them to others .
- 3.11. Avoid downloading files from unknown sender or unreliable source.
- 3.12. Avoid making direct sharing of your files, folders and storage unless official.
- 3.13. Always scan the external media such as thumb drives and external harddisk before using to detect the presence of virus.
- 3.14. Make a copy of your critical data and system configurations periodically and make sure it is kept in a safe place .
- 3.15. Remove unnecessary tools and services such as web, FTP, SNMP and others. This can minimise the risk of computer being infected by virus.
- 3.16. Do not install more than one antivirus software on the computer. It may cause conflicts and interfere the operations of antivirus software.
- 3.17. Configure your computer to receive and install updates, patches and hotfixes automatically.
- 3.18. Usage of pirated software in any of UM computers is strictly prohibited.