Information Security Management System

ISO/IEC 27001:2013

MALWARE POLICY

POLISI MALWARE

For PTM Use Only	Version 1.3	Date: 6th October 2015
Written By: Asiah Abu Samah Pengerusi Jawatankuasa ISMS	**Verified By:** Norain Mohamed Wakil Pengurusan Keselamatan Maklumat (ISMR)	**Approved By:** Majlis ICT

Revision History

No	Date of Change	Description	Page	Version	Approved By
1	1st Oct 2014	Change in name of policy	Header	1.1	Dr David
2	1st Oct 2014	Change MS ISO/IEC to ISO/IEC	Cover	1.1	Dr David
3	25th Nov 2014	Inserted TERHAD logo	Header	1.2	Dr David
4	5th May 2015	• 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	2nd 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	30th July 2015	Changed name of ISMR	Cover page	1.3	Dr David
7.	1st Oct 2015	Changed "The policy applies to all computers owned by UM, including but not limited to…" to : "The policy applies to all devices that are allowed to connect to UM network, including but not limited to…"	2,4	1.3	Dr David

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 audit and 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, 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.
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.
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, which is related to UM business operation and testing purposes, must be approved by the management.
3.9. Update the antivirus software regularly or configure the antivirus so that it gets updated automatically. This is to make sure your antivirus is up to date.
3.10. Always scan your computer for virus detection or set an automatic scan by scheduling your antivirus software to scan at a specified time (eg during lunchtime).
3.11. Always keep your antivirus disabled if there are additional tools used to remove virus. This is to avoid conflict with the existing antivirus software.
3.12. 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".
3.13. Delete all unnecessary emails, spam email and chain emails . Do not send or forward them to others .
3.14. Avoid downloading files from unknown sender or unreliable source.
3.15. Avoid making direct sharing of your files, folders and storage unless official.
3.16. Always scan the external media such as thumb drives, external harddisk, etc before using to detect the presence of virus.
3.17. Make a copy of your critical data and system configurations periodically and make sure it is kept in a safe place .
3.18. Remove unnecessary tools and services such as web, FTP, SNMP and others. This can minimise the risk of computer being infected by virus.
3.19. Do not install more than one antivirus software on the computer. It may cause conflicts and interfere the operations of antivirus software.
3.20. Configure your computer to receive and install updates, patches and hotfixes automatically .
3.21. Usage of pirated software in any of UM computers is strictly prohibited.

4.0 Procedure

4.1. Schedule anti-malware application to scan on a weekly or daily basis.
4.2. Configure anti-malware application to update its virus signature automatically.
4.3. Manually or automatically scan any files or external media devices that are introduced into the computer, especially which of their source are unknown or trusted.
4.4. All new PCs distributed by PTM or PTj should include the anti-virus software.

1.0 Tujuan

Tujuan polisi ini ialah untuk perkara-perkara berikut:

a) Mewujudkan syarat-syarat yang mesti dipatuhi oleh semua komputer yang bersambung kepada rangkaian UM bagi memastikan pengesanan dan pencegahan yang berkesan bagi virus dan lain-lain jenis malware.
b) Menyediakan panduan kepada pengguna bagaimana untuk mengukuhkan komputer mereka bagi melindungi daripada virus dan penggodam
c) Meminimakan insiden keselamatan ICT yang melibatkan komputer pengguna.

2.0 Skop

Polisi ini diguna pakai untuk semua peranti yang dibenarkan dihubung dengan rangkaian UM, termasuk tetapi tidak terhad kepada komputer meja, komputer riba dan pelayan

Walau bagaimanapun skop audit and pensijilan ISMS hanya meliputi komputer meja, komputer riba dan pelayan yang dimiliki oleh Pusat Teknologi Maklumat (PTM) dan berada di premis PTM.

3.0 Polisi

3.1 Pengguna mesti memasang perisian anti-virus atau anti-malware yang berlesen yang disediakan oleh PTM atau PTj atau yang dibeli sendiri pada komputer masing-masing dan jadualkan supaya imbasan dilaksanakan pada waktu-waktu tertentu secara tetap.

3.2 Ciri pengimbasan automatik atau real-time pada perisian anti-malware mesti diaktifkan.

3.3 Perisian Anti-malware dan *malware signature* mesti sentiasa dikemas kini.

3.4 Komputer yang dijangkiti malware mesti dibersihkan dengan segera sebaik sahaja malware dikesan.

3.5 Komputer yang dijangkiti malware mestilah diasingkan dari rangkaian UM sehingga ia dibersihkan dan disahkan sebagai bebas malware.

3.6 Pengguna bertanggungjawab untuk memastikan fail atau alat media luar yang digunakan adalah bebas dari malware. Mereka perlu mengimbas semua peranti mudah alih sebelum disambung kepada komputer.

3.7 Sebarang aktiviti dengan niat untuk mewujudkan atau mengagihkan program perosak ke dalam rangkaian UM (seperti virus, worms, Trojan horses, *e-mail bomb*, dan lain-lain.) adalah dilarang.

3.8 Aktiviti yang memerlukan penggunaan *malicious programs*, yang berkaitan dengan operasi perkhidmatan UM dan untuk tujuan pengujian, mesti diluluskan oleh pengurusan.

3.9 Kemaskini antivirus secara berkala atau konfigur antivirus supaya antivirus tersebut dikemaskini secara automatik.

3.10 Imbas komputer selalu untuk mengesan virus atau jadualkan imbasan virus dijalankan secara automatik pada waktu tertentu (contoh semasa waktu makan tengahari).

3.11 Disable'kan antivirus sekiranya menggunakan *tool* tambahan untuk menghapuskan virus. Ini adalah untuk mengelak konflik dengan virus sediaada di dalam komputer.

3.12 Elakkan daripada membuka fail atau lampiran emel yang diterima daripada pihak yang tidak diketahui atau sumber yang tidak dipercayai. Mansuh/buang emel dan lampiran tersebut dengan segera dan pastikan ianya juga dibuang dari *trash*.

3.13 Mansuh/buang semua emel yang tidak diperlukan, emel spam dan emel berantai. Jangan hantar atau panjangkan/majukan kepada orang lain.

3.14 Elakkan daripada muaturun fail dari penghantar yang tidak diketahui atau sumber yang tidak dipercayai.

3.15 Elakkan daripada pengkongsian fail, *folder* atau *storage* kecuali di atas tujuan rasmi.

3.16 Sentiasa imbas media *external* seperti *thumb drives, external harddisk* dan lain-lain sebelum menggunakannya untuk mengesan kewujudan virus

3.17 Buat salinan data kritikal dan konfigurasi sistem secara berkala dan pastikan ianya disimpan di tempat yang selamat.

3.18 Buangkan tools dan servis yang tidak diperlukan seperti web, FTP, SNMP dan seumpamanya. Ini akan meminimakan risiko komputer dijangkiti virus.

3.19 Jangan pasang lebih dari satu antivirus di dalam komputer. Ianya boleh mengakibatkan konflik dan mengganggu operasi antivirus.

3.20 Konfigur komputer untuk menerima dan mengemaskini patches dan hotfixes secara automatik.

3.21 Penggunaan perisian cetak rompak dalam mana-mana komputer UM adalah dilarang sama sekali.

4.0 Prosedur

4.1 Jadualkan perisian anti-malware untuk melaksanakan imbasan secara mingguan atau harian.

4.2 Konfigur perisian anti-malware untuk mengemaskini *signature* secara automatik.

4.3 Imbas sebarang fail atau media mudah alih yang disambung ke komputer secara manual, terutamanya jika fail dari sumber yang tidak dikenali atau dipercayai.

4.4 Semua komputer meja baru yang diagihkan oleh PTM atau PTj mestilah mengandungi perisian antivirus.