Information Security Management System MS ISO/IEC 27001:2007

ANTI-MALWARE POLICY

DASAR ANTI-MALWARE

UNIVERSITI MALAYSIA PERLIS

Written By:	Verified By:	Approved By:
En. Farihan Ghazali	Pn. Rohazna Wahab Deputy Director ICT	En. Nasrudin Abd. Shukor Director ICT Division ISMR

For Dept Use Only

Date: 22nd March 2013 **Version 1.1**

Revision History

No	Date of Change	Description	Page	Version	Approved By
1.	22 Mac 2013	Beberapa pembetulan ejaan iaitu digunapakai, anti-malware, dan real-time.	2, 4, 5	1.1	Nasrudin Abd Shukor

ANTI-MALWARE POLICY
DASAR ANTI-MALWARE

1.0 Purpose
1.0 Tujuan

The purpose of this policy is to establish requirements which must be met by all computers connected to UniMAP ICT Center networks to ensure effective virus and other types of malware detection and prevention.

Tujuan dasar ini ialah untuk mewujudkan syarat-syarat yang mesti dipenuhi oleh semua komputer yang disambungkan kepada rangkaian Pusat ICT UniMAP bagi memastikan pengesanan dan pencegahan yang berkesan bagi virus dan lain-lain jenis malware.

2.0 Scope
2.0 Skop

The policy applies to all UniMAP ICT Center computers, including but not limited to desktop computer, laptops and servers.

Dasar ini digunapakai atas semua komputer Pusat ICT UniMAP, termasuk tetapi bukan terhad kepada komputer meja, komputer riba dan pelayan.

3.0 Policy
3.0 Dasar

3.1 All UniMAP ICT Center computers must have anti-malware software installed and scheduled to run at regular intervals.

3.1 Semua komputer Pusat ICT UniMAP mesti mempunyai perisian anti-malware yang dipasang dan dijadualkan untuk berfungsi pada waktu berselang yang tetap

3.2 Anti-malware software automated or real-time scanning feature must be enabled.

3.2 Perisian Anti-malware automatik atau ciri pengimbasan real-time mesti diaktifkan.

3.3 Anti-malware software and malware signature must be kept up-to-date.

3.3 Perisian Anti-malware dan tandatangan malware mesti sentiasa dikemaskini.

3.4 Malware-infected computers must be cleaned immediately upon the detection of malware.

3.4 Komputer-komputer yang dijangkiti Malware mesti dibersihkan segera sebaik sahaja malware dikesan.

3.5 Malware-infected computers must be isolated from the production network until they are verified as malware-free.

3.5 Komputer-komputer yang dijangkiti Malware mestilah diasingkan dari rangkaian pengeluaran sehingga mereka ditentusahkan sebagai bebas malware.

3.6 Users are responsible to ensure files or external media devices introduced into their computers are free from malware. They should scan all external drives before introducing into their computers.

3.6 Pengguna-pengguna bertanggungjawab untuk memastikan fail-fail atau alat-alat media luar yang diperkenalkan ke dalam komputer mereka bebas dari malware. Mereka sepatutnya mengimbas semua pemacu luaran sebelum memperkenalkan ke dalam komputer mereka.

3.7 Any activities with the intention to create or distribute malicious programs into UniMAP ICT Center networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

3.7 Sebarang aktiviti dengan niat untuk mewujudkan atau mengagihkan program-program perosak ke dalam rangkaian Pusat ICT UniMAP (misalnya, virus-virus, worms, Trojan horses, bom e-mel, dan lain-lain) adalah dilarang.

3.8 Activities that require the usage of malicious programs, which is related to UniMAP ICT Center business operation and testing purposes, must be approved by the management.

3.8 Aktiviti-aktiviti yang memerlukan penggunaan program-program perosak, yang berkaitan dengan operasi Pusat ICT UniMAP dan tujuan ujian, mesti diluluskan oleh pengurusan.

4.0 Procedure
4.0 Prosedur

4.1 Schedule anti-malware application to run on a weekly basis.

4.1 Menjadualkan aplikasi anti-malware untuk berjalan secara mingguan.

4.2 Configure anti-malware application to update its virus signature automatically.

4.2 Aplikasi anti-malware dikonfigurasikan untuk mengemaskini tandatangan virus secara automatik.

4.3 Manually scan any files or external media devices that are introduced into the computer, especially which of their source are unknown or trusted.

4.3 Secara manual imbas sebarang fail atau alat-alat media luar yang diperkenalkan ke dalam komputer, terutamanya dari sumber yang tidak dikenali atau dipercayai.

4.4 Refer to the anti-malware manufacturer's instructions for proper installation and operations.

4.4 Rujuk arahan-arahan pengeluar anti-malware untuk pemasangan dan operasi yang betul.

4.5 Usage of pirated software in any of UniMAP ICT Center's properties is a breach of law. This is strictly condemned across the university and shall be reported to the police.

4.5 Penggunaan perisian cetak rompak dalam mana-mana harta hak milik Pusat ICT UniMAP ialah satu pelanggaran undang-undang. Ini dengan tegasnya dilarang di seluruh universiti dan akan dilaporkan kepada pihak polis.

Procedure to ensure Avira Anti Virus Control is configured properly in Windows XP, are as followed:
Prosedur untuk memastikan kawalan Avira Anti Virus dikonfigurasi dengan betul dalam Windows, ialah seperti yang berikut:

1.0 Avira Anti Virus
1.0 Avira Anti Virus

Below is the procedure to ensure Avira Anti Virus is enabled and running properly.
Di bawah ialah prosedur bagi memastikan Avira Anti Virus diaktifkan dan berjalan dengan betul.

1. Click **Start** > **Control Panel**, double-click **Administrative Tools**, then double click **Services**.
1. *Klik **Mula** > **Panel Kawalan**, klik dua kali **Alat- alat Pentadbiran**, kemudian klik dua kali **Perkhidmatan-perkhidmatan**.*

2. On the list of services shown on the right pane, ensure the following 5 services configurations are the same as shown in Figure 1.
2. *Di senarai perkhidmatan yang ditunjukkan di tingkap kanan, pastikan konfigurasi 3 perkhidmatan berikut ialah sama seperti yang ditunjukkan dalam Figure 1.*

Service Name	Status	Startup Type
Avira AntiVir Guard	Started	Automatic
Avira AntiVir MailGuard		Disable
Avira AntiVir Scheduler	Started	Automatic
Avira AntiVir WebGuard		Disable
Avira Management Console Agent	Started	Automatic

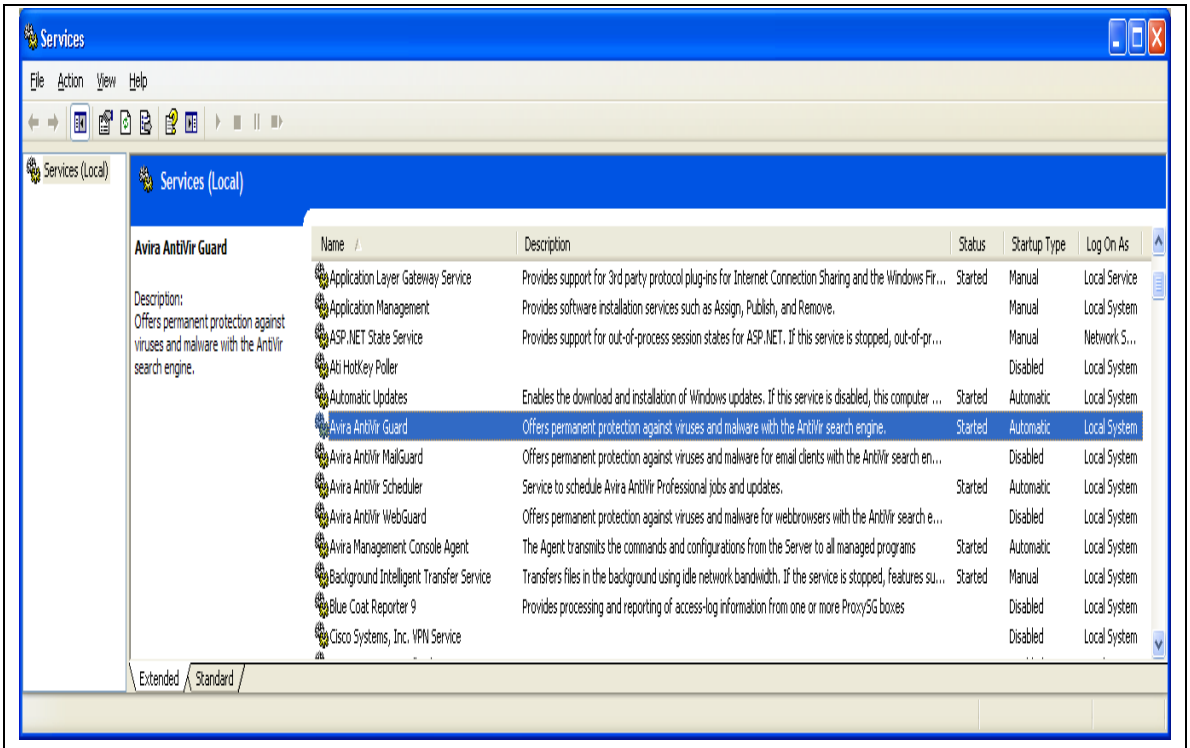


Figure 1

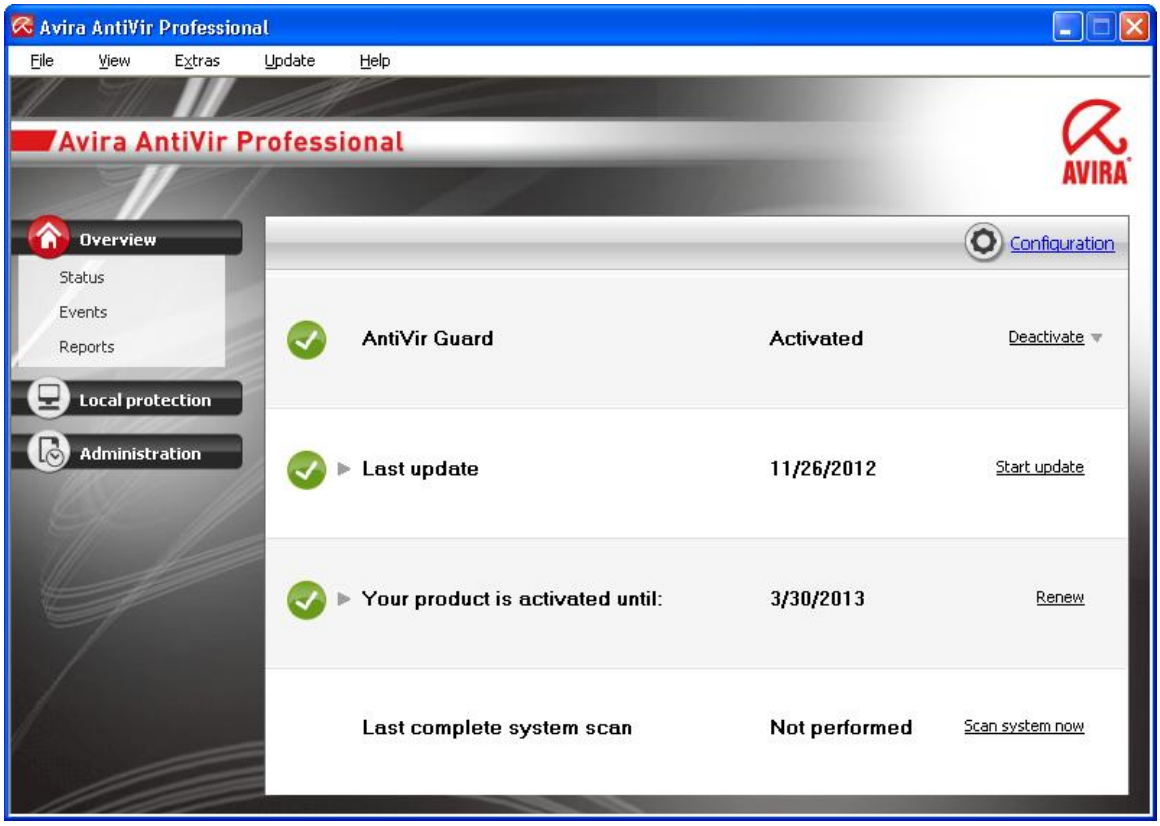
2.0 Real-time Malware Monitoring
2.0 Pemantauan Malware Real-time

Below is the procedure to ensure AntiVir Guard real-time monitoring is enabled.
Di bawah ialah prosedur bagi memastikan pengawasan real-time AntiVir Guard diaktifkan

1. Click **Start** > **All Programs** > **Avira** > **Avira Desktop** > **Start AntiVir**.
1. *Klik **Mula** > **Semua Program-program** > **Avira** > **Avira Desktop***

2. Select '**Overview'** on the left pane. Ensure all configurations on the **Status** tab are the same as shown in Figure 2.
2. *Pilih '**Overview'** di tingkap kiri. Pastikan semua konfigurasi- konfigurasi di tab **Status** adalah sama dengan yang ditunjukkan di Figure 2.*

Figure 2



3.0 Avira AntiVir Control Automatic Update
3.0 Pengemaskinian Automatik Avira AntiVir

Below is the procedure to ensure Avira AntiVir will automatically update anti-malware signature.

Di bawah ialah prosedur bagi memastikan Avira AntiVir akan mengemaskini secara automatik tandatangan anti-malware.

1. Click **Start** > **All Programs** > **Avira** > **Start AntiVir**.
1. *Klik **Mula** > **Semua Program-program** > **Avira** > **Start AntiVir**.*

2. Select '**Overview'** on the left pane. Ensure all configurations on the **Status** tab are the same as shown in Figure 3.
2. *Pilih '**Overview'** di tingkap kiri. Pastikan semua konfigurasi- konfigurasi di tab **Status** adalah sama dengan yang ditunjukkan di Figure 3.*

Figure 3