Information Security Management System MS ISO/IEC 27001:2007

END USER MACHINE SECURITY POLICY

DASAR KESELAMATAN MESIN PENGGUNA AKHIR

UNIVERSITI MALAYSIA PERLIS

Written By:	Verified By:	Approved By:
En. Mohd Nasri Md Saat IT Officer	Pn. Rohazna Wahab Deputy Director ICT Centre	En. Nasrudin Abd. Shukor Director ICT Centre ISMR

For Dept Use Only

Date: 25th July 2013 **Version 1.1**

Revision History

No	Date of Change	Description	Page	Version	Approved By
1.	15/07/2013	Nama asal Penulis Dokumen iaitu Pn Ummi Naiemah Saraih ditukar kepada En. Mohd Nasri Md Isa @ Md Saat	0	1.1	Nasrudin Abd Shukor

1.0 Purpose
1.0 Tujuan

The purpose of this policy is to establish a standard security baseline for UniMAP ICT Center owned desktop machines and laptops or machines connected to UniMAP ICT Center network.

Tujuan dasar ini ialah untuk mewujudkan garis dasar keselamatan piawaian untuk Pusat ICT UniMAP yang memiliki mesin komputer meja dan komputer riba atau mesin-mesin yang berhubung dengan rangkaian Pusat ICT UniMAP.

2.0 Scope
2.0 Skop

The policy applies to all employees, contractors, consultants, temporaries (Staff, Interns), and other workers including all personnel that are affiliated with UniMAP ICT Center.

Dasar ini diguna pakai atas semua staf, kontraktor, konsultan, staf atau pelatih sementara dan pekerja lain termasuk semua staf yang bergabung dengan Pusat ICT UniMAP.

3.0 Policy
3.0 Dasar

3.1 All desktops/laptops must be registered within the Asset Register management system.

3.1 Semua komputer meja / komputer riba mesti didaftarkan dalam sistem pengurusan Pendaftaran Aset.

3.2 Desktop/laptop configuration must be in accordance with approved guidelines from MAMPU.

3.2 Konfigurasi komputer meja / komputer riba mesti sejajar dengan garis panduan yang diluluskan dari MAMPU.

3.3 Access to the user machines must be protected with strong password. (Alpha Numeric with minimum 6 characters)

3.3 Akses bagi mesin-mesin pengguna mesti dilindungi dengan kata laluan yang kukuh. (Angka Alfa dengan minimum 6 karakter)

3.4 Desktop/laptop must have up-to-date security patches.
3.4 Komputer meja / komputer riba mesti mempunyai patches keselamatan terkini.

3.5 Anti-malware with up-to-date malware signature must be installed on the machine.
3.5 Anti - malware dengan tandatangan malware terkini mesti dipasang di mesin.

3.6 Personal firewall must be installed on the machine.
3.6 Peranti Keselamatan (Firewall) peribadi mesti dipasang di mesin.

3.7 Use only the least amount of privilege to perform the required task.
3.7 Hanya gunakan sejumlah kecil keistimewaan untuk melakukan tugas yang diperlukan.

3.8 Remote access must be performed over secure channels. (VPN Client)
3.8 Akses jarak jauh mesti dilakukan atas saluran-saluran yang selamat. (VPN Client)

3.9 Users are responsible for performing their own data backups.
3.9 Pengguna bertanggungjawab untuk melakukan sokongan/sandaran/penduaan untuk data mereka sendiri.

4.0 Procedure
4.0 Prosedur

4.1 Services and applications that will not be used must be disabled where practical.
4.1 Perkhidmatan-perkhidmatan dan aplikasi-aplikasi yang tidak akan digunakan mesti dimansuhkan di mana praktikal.

4.2 Do not use administrative/root access when a non-privileged account will do.
4.2 Jangan gunakan akses pentadbiran / root apabila akaun tidak istimewa adalah sudah memadai.

4.3 Use SSH when performing a remote access.
4.3 Guna SSH apabila melakukan akses jarak jauh.

4.4 Refer Patch Management Policy on security patches requirements.
4.4 Rujuk Dasar Pengurusan Tampung keselamatan (Patch) untuk keperluan tampung keselamatan (patches)

4.5 Refer Password Policy on creating strong password
4.5 Rujuk Dasar Kata Laluan untuk mewujudkan kata laluan yang kukuh.

4.6 Refer Anti-Malware Policy on anti-malware requirements.
4.6 Rujuk Dasar Anti-Malware untuk keperluan-keperluan anti-malware.

Note: This policy is connected to Acceptable Use of IT Assets Policy and shall be used in conjunction with each other.

Nota: *Dasar ini dikaitkan kepada Dasar Penggunaan Yang Diterima Pakai Untuk Aset-aset IT dan akan digunakan dalam gabungan bersama antara satu sama lain.*