Information Security Management System MS ISO/IEC 27001:2007

PATCH MANAGEMENT POLICY

DASAR PENGURUSAN TAMPUNG (PATCH)

UNIVERSITI MALAYSIA PERLIS

Written By:	Verified By:	Approved By:
En Farihan Ghazali 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.	15/07/13	Nama asal Penulis Dokumen iaitu Pn Ummi Naiemah Saraih ditukar kepada En. Farihan Ghazali	0	1.1	Nasrudin Abd Shukor

PATCH MANAGEMENT POLICY
DASAR PENGURUSAN TAMPUNG (PATCH)

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 up-to-date patches installation.

Tujuan dasar ini ialah untuk mewujudkan keperluan-keperluan yang mesti dipenuhi oleh semua komputer yang bersambung kepada sistem rangkaian Pusat ICT UniMAP untuk memastikan penambahbaikan (patches) yang terkini dapat dipasang.

2.0 Scope
2.0 Skop

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

Dasar digunapakai ke atas semua komputer di Pusat ICT UniMAP, termasuk tetapi bukan dihadkan kepada komputer meja, komputer riba dan pelayan.

3.0 Policy
3.0 Dasar

3.1 All systems that are connected to UniMAP ICT Center networks must have up-to-date security patches.

3.1 Semua sistem yang bersambung kepada sistem rangkaian Pusat ICT UniMAP mesti mempunyai penambahbaikan (patches) keselamatan terkini.

3.2 For application that features automatic update functionality, it must be configured to check for updates automatically and the updates must be automatically applied.

3.2 Untuk aplikasi yang menampilkan fungsi kemaskini automatik, ia mesti dikonfigurasi untuk semakan bagi kemaskini secara automatik dan kemaskini tersebut mesti diaplikasikan secara automatik.

3.3 For application that requires manual checking of application updates or manual patch installation, the respective users or administrators must be notified on the available updates.

3.3 Untuk aplikasi yang memerlukan pemeriksaan manual kemaskini aplikasi atau pemasangan penambahbaikan (patches) manual, pengguna-

pengguna berkenaan atau pentadbir-pentadbir mesti diberitahu tentang kemaskini yang boleh didapati.

3.4 Security patch must be applied immediately after it is released, unless immediate application (To Apply) would interfere with business requirements.

3.4 Penambahbaikan (patches) keselamatan mesti dipasang sebaik sahaja selepas ia dikeluarkan, melainkan pemasangan segera akan mengganggu keperluan sistem.

4.0 Procedure
4.0 Prosedur

4.1 Turn on automatic security updates featured in most applications.

4.1 Aktifkan pengemaskinian ciri keselamatan automatik dalam kebanyakan aplikasi.

4.2 Administrator should subscribe to 3rd party security mailing list to keep them informed on the available security patches.

4.2 Pentadbir sepatutnya melanggan/menyertai senarai mel keselamatan pihak ketiga untuk mendapat makluman tentang penambahbaikan (patches) keselamatan yang boleh didapati.

4.3 For critical applications or servers that require patches, these patches must be validated before being applied to the system/ application.

4.3 Untuk aplikasi-aplikasi kritikal atau pelayan yang memerlukan penambahbaikan (patches), ianya mesti disahkan/disemak terlebih dahulu sebelum digunakan ke atas sistem / aplikasi.