Information Security Management System MS ISO/IEC 27001:2007

FIREWALL & IPS POLICY

DASAR PERANTI KESELAMATAN & IPS

UNIVERSITI MALAYSIA PERLIS

Written By:	Verified By:	Approved By:
En. Mohammad Taufik Bin Saidina Omar 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	4.5: change the word "appliance" with "firmware" (*4.5: tukar perkataan "peranti" kepada "firmware"*)	4	1.1	Nasrudin Abd. Shukor

FIREWALL & IPS POLICY
DASAR PERANTI KESELAMATAN & IPS

1. Purpose
Tujuan

The purpose of this policy is to establish a standard for the management of Firewall & IPS, Network Division in UniMAP ICT Department.

Tujuan dasar ini ialah untuk mewujudkan satu piawaian bagi pengurusan Peranti Keselamatan (Firewall & IPS) Bahagian Rangkaian, Pusat ICT UniMAP.

2. Scope
Skop

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

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 yang menguruskan peranti keselamatan (Firewall) Pusat ICT UniMAP.

3. Policy
Dasar

3.1. Firewall must implement the default **"drop all"** policy for inbound and outbound traffics.

*Semua peranti keselamatan (Firewall & IPS) mesti melaksanakan dasar default **"drop all"** untuk trafik masuk dan keluar.*

3.2. Only services that are bounded to UniMAP ICT Division business operation are explicitly allowed to pass through the Firewall & IPS.

Hanya perkhidmatan yang dibatasi kepada operasi pengurusan Pusat ICT UniMAP dengan jelas dibenarkan untuk melalui peranti keselamatan (Firewall & IPS).

3.3. Security appliances (Firewall & IPS) rules must adhere to general best practices (refer to manufacturer) and be well documented by the network department.

Peraturan-peraturan peranti keselamatan (Firewall & IPS) mesti menurut kepada amalan am terbaik (rujuk kepada pengeluar) dan didokumenkan dengan baik oleh bahagian rangkaian.

3.4. Firewall main rules - Network user (NAT) can only used port HTTP and HTTPS to access the internet services.

Bagi peraturan penggunaan internet melalui Firewall, pengguna rangkaian hanya boleh menggunakan port HTTP dan HTTPS untuk akses ke perkhidmatan internet.

3.5. All owners of hardware and application must acquire permission from Network Officer for "Public IP & Allowed Ports" so that it can be advertised on the internet.

Pemilik hardware dan aplikasi Pusat ICT UniMAP mestilah memohon kebenaran pegawai rangkaian untuk mendapatkan "Public IP & Allowed Ports" supaya ianya boleh dicapai di internet.

3.6. Firewall & IPS rules must be subjected to periodic revision to correspond with business operation.

Peraturan peranti keselamatan (firewall & IPS) mesti disemak secara berkala untuk berpadanan dengan operasi pengurusan.

3.7. Firewall & IPS rules must be tested to ensure secure implementation.

Peraturan-peraturan peranti keselamatan (Firewall & IPS) mesti diuji untuk memastikan pelaksanaan yang selamat.

3.8. All dropped inbound and dropped traffics (IPS) must be logged.

Semua kemasukan trafik yang disekat mesti dilog.

3.9. Exam the IPS logs periodically (at least once in 3 months) and the log must be synchronized with other logging systems.

Pemeriksaan log peranti keselamatan (IPS) secara berkala (sekurang-kurangnya sekali dalam 3 bulan) dan log mesti diselaraskan dengan sistem log lain.

4. Procedure
Prosedur

4.1 Review firewall & IPS rules at least every 3 months.

Menilai semula peranti keselamatan (Firewall & IPS) sekurang-kurangnya sekali dalam 3 bulan.

4.2 Administrator must exam the firewall & IPS logs weekly, with the aid of automated log monitoring and analysis tools.

Pentadbir mesti memeriksa log-log peranti keselamatan (Firewall & IPS) setiap minggu dengan bantuan pengawasan log automatik dan alat-alat analisis.

4.3 Employ penetration testing on firewall rules before fully deploying the firewall rules.

Melakukan ujian penembusan ke atas peraturan peranti keselamatan (Firewall & IPS) sebelum menggunakan peraturan peranti keselamatan tersebut sepenuhnya.

4.4 Analyze and prepare appropriate “Public IP & Allowed Ports” in Firewall for each ICT Application & Hardware that want to be advertised on the internet.

Menyediakan “Public IP & Allowed Ports” Firewall untuk setiap aplikasi ICT dan hardware yang ingin dibenarkan akses melalui internet.

4.5 Always check the latest protection pack for IPS and manually update the IPS firmware.

Sentiasa semak “Protection Pack” yang terkini untuk IPS dan kemaskini “firmware” IPS secara manual.