



# Information Security Management System ISO/IEC 27001:2013

FIREWALL POLICY

*POLISI FIREWALL*

For PTM Use Only	Version 1.0	Date: 25 <sup>th</sup> Nov 2014
<b>Written By:</b> Asiah Abu Samah Pengerusi Jawatankuasa ISMS	<b>Verified By:</b> Haslina Abd Hamid Wakil Pengurusan Keselamatan Maklumat (ISMR)	<b>Approved By:</b> Dr David Asirvatham Pengarah Pusat Teknologi Maklumat

 <b>UNIVERSITI MALAYA</b>	<b>FIREWALL POLICY</b>  <b>POLISI FIREWALL</b>	
<b>Doc No :</b> <b>UM-ISMS-POL-NW-002</b>	<b>Version 1.0</b>	<b>Effective Date :</b> <b>1st Dec 2014</b>

## Revision History

<b>No</b>	<b>Date of Change</b>	<b>Description</b>	<b>Page</b>	<b>Version</b>	<b>Approved By</b>
1	1st October 2014	Remove 'MS' from Front Page.	Front Page	1.1	Dr David Asirvatham
2	25 <sup>th</sup> Nov 2014	Upgrade "Firewall Guidelines" to "Firewall Policy"		1.0	Dr David Asirvatham
3	25 <sup>th</sup> Nov 2014	Changed Doc No from "UM-ISMS-GL-NW-001" to "UM-ISMS-POL-NW-002"		1.0	Dr David Asirvatham
4	25 <sup>th</sup> Nov 2014	Changed the guideline statements to policy statements	2, 3	1.0	Dr David Asirvatham
4	25 <sup>th</sup> Nov 2014	Inserted TERHAD logo	Header	1.0	Dr David Asirvatham

 <b>UNIVERSITI MALAYA</b>	<b>FIREWALL POLICY</b>  <b>POLISI FIREWALL</b>	
<b>Doc No :</b> <b>UM-ISMS-POL-NW-002</b>	<b>Version 1.0</b>	<b>Effective Date :</b> <b>1st Dec 2014</b>

## 1.0 Purpose

The purpose of this policy is to establish a standard for the management of UM Centre For Information Technology (PTM) firewall.

Create a firewall policy that specifies how firewalls should handle inbound and outbound network traffic.

## 2.0 Scope

The policy applies to all employees, contractors, consultants, temporaries (Staff, Interns), and other workers including all personnel that are affiliated with PTM, who manage PTM's firewall.

## 3.0 Policy

3.1 A firewall policy defines how an organization's firewalls should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the organization's information security policies. By default all ports must be closed. Any request to open ports must be submitted officially to the respective division.

3.2 Only services that are bounded to PTM's business operation are explicitly allowed to pass through the firewall.

3.3 Firewall rules must adhere to general best practices and be well documented.

3.4 Firewall rules must be subjected to periodic revision at least every 6 months to correspond with business operation.

3.5 Firewall rules must be tested to ensure secure implementation.

3.6 All dropped inbound traffics must be logged.

3.7 Examine the firewall logs periodically (at least once a month).

 <b>UNIVERSITI MALAYA</b>	<b>FIREWALL POLICY</b>  <b>POLISI FIREWALL</b>	
<b>Doc No :</b> <b>UM-ISMS-POL-NW-002</b>	<b>Version 1.0</b>	<b>Effective Date :</b> <b>1st Dec 2014</b>

## 1.0 Tujuan

Tujuan polisi ini ialah untuk mewujudkan satu piawaian bagi pengurusan *Firewall* Pusat Teknologi Maklumat (PTM) UM.

Mewujudkan polisi firewall yang khusus menunjukkan bagaimana pengurusan trafik rangkaian diuruskan.

## 2.0 Skop

Polisi ini diguna pakai untuk semua kakitangan, kontraktor, konsultan, pekerja dan pelatih sementara dan pekerja lain termasuk semua kakitangan yang bergabung dengan PTM, yang menguruskan *Firewall* PTM.

## 3.0 Polisi

3.1 Polisi *firewall* mendefinisikan bagaimana *firewall* di sesebuah organisasi menguruskan trafik rangkaian untuk alamat IP spesifik dan julat alamat, protokol, aplikasi dan asas bentuk kandungan polisi keselamatan maklumat. Semua *port* mesti ditutup. Sebarang permohonan membuka *port* mestilah dimajukan secara rasmi kepada bahagian berkaitan.

3.2 Hanya perkhidmatan yang terbatas kepada urusan rasmi PTM dibenarkan untuk melalui *firewall*.

3.3 Peraturan *firewall* mesti mematuhi amalan am terbaik dan didokumenkan dengan baik.

3.4 Peraturan *firewall* mesti disemak secara berkala sekurang-kurangnya sekali dalam 6 bulan untuk disesuaikan dengan operasi perkhidmatan.

3.5 Peraturan *firewall* mesti diuji untuk memastikan pelaksanaan yang selamat.

3.6 Semua trafik masuk yang tidak berjaya mesti di log.

3.7 Periksa log *firewall* secara berkala (sekurang-kurangnya sekali dalam 6 bulan) dan log mesti diselaraskan dengan sistem-sistem log lain.