**Firewall Policy**

Prepared By

**IT Security**

**VERSION: 1.0**

All rights reserved. This document is a proprietary product of IT Security and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission from IT Security, is strictly prohibited. Any printed copy of this document is uncontrolled

**CHANGE HISTORY**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Summary of changes** | **Author** | **Pages affected** | **Remark** |
| 1.0 |  |  |  |  |  |

Table of Contents

**GENERAL FIREWALL GUIDELINE 4**

**FIREWALL ADMINISTRATION 4**

**PHYSICAL ACCESS & ENVIRONMENT 5**

**LOGICAL ACCESS & REMOTE ADMINISTRATION 5**

**SYSTEM BACKUP 5**

**UPGRADE AND PATCHES 5**

**LOGS AND AUDIT TRAILS 6**

**DOCUMENTATION 6**

**ENCRYPTED CHANNEL OVER PUBLIC/ENTRUSTED NETWORK 7**

***ENFORCEMENT 7***

1. **GENERAL FIREWALL GUIDELINES**
	1. The firewall software should run only on dedicated computer system. Except for the firewall-related utilities or its safeguarding components (e.g. Intrusion Detection System), no other non-firewall related software should co-exist/installed in the firewall system.
	2. Restricted policy shall be enforced in the firewall such that all services are denied unless specifically permitted.
	3. If a different users/network community requires different firewall policies, network segregation should be in place to isolate the more permissive users/network on a subnet apart from the more securely protected network. All access from the said subnet should comply with the established firewall policy and guidelines.
	4. Details of the internal trusted network should not be visible from the entrusted network side of the firewall.
	5. Arrangement should be made (whether system-automated or through manual detection) to promptly notify the Firewall Administrator(s), the Backup Firewall Administrator(s) and escalated to the Information Security Manager[[1]](#footnote-1) of any intrusion or break-down in the firewall system.
	6. Deployment of firewalls should comply with the established Network Trust Model and the recommended firewall-layers required.
	7. For gateway connection to the Internet, consideration should be given at management’s discretion, to deploy two-tiered hybrid-platform firewalls.
	8. For any systems hosting critical applications, or providing access to critical information, internal firewalls or filtering routers should be used to provide access control and support for auditing and logging. These controls should be used to segment the internal network to support the access policies developed by the designated owners on information.
	9. All hosts (servers) protected behind a firewall should be segmented through physical-ports at the firewall and not through logical-segmentation via a VLAN-switch, for example.

## FIREWALL ADMINISTRATION

## Designated Firewall Administrator(s)[[2]](#footnote-2) and Backup Firewall Administrator(s) should administer the firewall.

# Any modification on the firewall shall be under the charge of the Firewall Administrator(s) or Backup Firewall Administrator(s) and requires approval from IT Security.

# The Firewall Administrator(s) should validate on periodic basis (e.g. quarterly) with application-systems/hosts owners all previously defined connections, and allowed rules and services in the firewall. Such definitions, when no longer valid, should be confirmed by the application-systems/hosts owners and promptly removed by the Firewall Administrator(s).

# There should be authorization by users, application-systems owners and the Information Security Manager for any request for connections and rules/services definition on the firewall. Prior to authorization, all such request should be first reviewed and the acceptable security controls established by the Information Security department.

1. **PHYSICAL ACCESS & ENVIRONMENT**
	1. The firewall should be located in restricted access area where access is allowed on a need to basis.
	2. The firewall should be installed in a controlled environment appropriate for 24x7 computer operations, with air-conditioning, and uninterruptible power supply.
2. **LOGICAL ACCESS & REMOTE ADMINISTRATION**
	1. Logical access to the firewall should be restricted only to the Firewall Administrator(s), Backup Firewall Administrator(s) and the Information Security Manager[[3]](#endnote-1). Any other access granted should be on a need to basis and with prior approval by the IT Security.
	2. The Information Security Manager shall approve all access and privilege-level attributes.
	3. Access previously granted which is invalid or no longer required should be removed immediately.
	4. Logical access to the firewall, through administration workstation or direct terminal, should be controlled with authentication, with for example with user id and password.
	5. Remote connection for firewall administration should only be considered if operational environment requires. If via entrusted network, remote connection should be secured with session encryption.
3. **SYSTEM BACKUP**[[4]](#footnote-3)
	1. The following files in the firewall should be periodically backed up for recovery in case of system failure or for forensic-related activity in case of incidents: -

5.1.1 System Configuration

* + - 1. Firewall software (e.g. Rules/Policies, Network objects, definitions, etc)
			2. Operating system (e.g. inetd.conf, rc3.d)
			3. Network definitions (e.g. routing tables, hostname)
		1. Logs
			1. Firewall software (e.g. fwlog, etc)
			2. Operating system (e.g. syslog, etc)
			3. Removable media when used to back up the above files should be labelled and securely stored.
1. **UPGRADE AND PATCHES**
	1. Patches recommended by firewall vendor should be promptly implemented with management’s approval.
	2. The Firewall Administrator[[5]](#endnote-2) shall evaluate new version or release of the firewall or its platform capacity requirement to determine if upgrading is necessary. Prior approval from the Information Security Manager should be obtained before implementation.
	3. After any upgrade, the firewall’s proper operation shall be verified prior to going operational.
2. **LOGS AND AUDIT TRAILS**
	1. Where available in the firewall system, the following logging should be enabled: -
		* 1. The firewall’s filtering activity (*e.g. TCP connect attempts, in-bound and out-bound proxy traffic information, etc*)
			2. The firewall’s audit trail (*e.g. login/logout activity, connect time, rules/definition changes etc.*)
			3. At the firewall’s system level (*e.g. disk media errors, configuration/parameter changes, etc*).
	2. Depending on operational requirement OR business criticality environment, the Information Security Manager should establish if the logs (in total or selectively) be reviewed: -
		* 1. On a periodic basis (*from standpoint of accountability or for detective control purpose*) OR
			2. On situational required basis (*for problem determination or for forensic investigative purpose*).
	3. For the review of the logs, where accountability over firewall administration is concerned, it should be carried out internally either by the Information Security Manager or an independent party.
	4. The logs should be archived for an established period.
	5. At the end of archival, the logs should be dispensed with securely, either through total irrecoverable erasure or by overwriting its data.
3. **DOCUMENTATION**
	1. All operational procedures for the firewall should be documented. At the minimum, they consist of the following: -
		* 1. Administration procedures
			2. Backup procedures
			3. Troubleshooting guide
			4. Review of firewall logs and audit trails
			5. House keeping procedures[[6]](#footnote-4)
	2. The firewall’s configurable parameters should be documented and kept in confidence, accessible only by Firewall Administrator(s), Backup Firewall Administrator(s) and the Information Security Manager. At the minimum, the configuration documents should include: -
		* 1. Network diagram(s)
			2. IP addresses of all relevant network devices, internal hosts and relevant hosts of the Internet Service Provider (ISP) e.g. DNS server, router, etc
			3. Routing tables
			4. Firewall rules
	3. All the above documentation should be updated following any changes to the firewall.
4. **ENCRYPTED CHANNELS OVER PUBLIC/ENTRUSTED NETWORK**
	1. Any connection between internal host to an external organization’s host over the public network or entrusted network for business-related exchange (e.g. B2B) shall use encrypted channel such as Virtual Private Network (VPN), router-to-router encryption, Secured-Socket-Layer (SSL), Secure-Shell (SSH), etc to ensure privacy and integrity of its data communication.
	2. For establishing encrypted channel, there should be secured means for distributing the encryption keys prior to its operational use.
5. ***ENFORCEMENT***

# *All staffs are required to comply with this security policy and its appendices. Disciplinary actions including termination may be taken against any Organization staffs who fail to comply with the Organization’s security policies, or circumvent/violate any security systems and/or protection mechanisms.*

# *Staff having knowledge of personal misuse or malpractice of IT Systems must report immediately to management and IT Security.*

* 1. ***Organization’s staff must ensure that Organization’s contractors and others parties authorized by the Organization using its internal computer systems, comply with this policy.***
	2. ***Where the role of the service provider is outsourced to a vendor, the outsourced vendor should ensure compliance with this policy.***
1. *See End of Document* [↑](#footnote-ref-1)
2. *See End of Document* [↑](#footnote-ref-2)
3. *Outside of Head Office, for subsidiaries or oversea centre, the resident manager in charge of Information Systems would assume the role of the Information Security Manager.* [↑](#endnote-ref-1)
4. [↑](#footnote-ref-3)
5. *As in the above, outside of Head Office, local Firewall Administrator(s) would be appointed by the resident manager in charge of Information Systems.* [↑](#endnote-ref-2)
6. *Further details please refer to Organization Firewall Clean up Procedures*  [↑](#footnote-ref-4)