WEST COAST DISTRICT MUNICIPALITY

Firewall Configuration Policy

Table of Contents

1. Terminology

Definitions of specific terminology used within the document

Firewall	a device or set of devices configured to permit, deny, encrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria.
Configuration	the arrangement or set-up of the hardware and software that make up a computer system.
VPN	a virtual private network that uses a public telecommunications infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.
Traffic	the load on a communication device or system.
Inbound and Outbound	Inbound refers to incoming traffic originate elsewhere and arrive at the machine – Outbound refers to traffic which originate at the machine and arrive elsewhere.
Proxy	a process that accepts request for some service and passes them on to the real "server". A proxy may be intended to increase security.
Encrypt	Encryption is a form of effectively protect and achieve data security.

2. Purpose

The purpose of this document is to establish and maintain control over the firewall rule sets that are applied within the organization.
This document will enforce the guidelines set out in the Corporate Security Policy and all related documents.

3. Target area

The target area of this document is the configuration of all firewalls or other network elements providing network security within the organization.

4. Responsibilities

Preparation and maintenance of this document related to the operation

- Information Technology Manager

Review and approval of documents and procedures

- IT Steering Committee
- Management
- Council

Execution of documented activities:

- IT Manager
- Network Administrator

Review of executed activities

- IT Manager
- Internal Auditor

5. Detailed policy description

The following items describe a sample policy. They should not be detailed from-to pair, that is the job of the actual configuration on the firewalls.

Permit Inbound VPN access on custom port (TCP 3456) from any address on the internet.

5.1 Configuration policy for Network Core Firewalls

Deny all traffic which is not explicitly permitted in both directions (inbound and outbound).

5.2 Role responsibilities within the process

Role	Responsibility
IT Manager	Manages the Firewall Configuration Policy pertaining to the Corporate Security Policy - Performs periodic verification of applied and configured rules on production firewalls - Recommends upgrades to applied rules, and changes to the policy - Evaluates and Approves/Denies urgent or non- standard rules required by the organization
Security Administrators	Applies the Firewall Configuration Policy into specific firewall rules on the firewalls - Logs and analyses requests for urgent or non- standard rules required by the organization - Assists the Information Security Officer in managing the Firewall Configuration Policy
Network Administrators	Applies the Firewall Configuration Policy into specific firewall rules on the network devices utilized as security devices - Logs and analyses requests for urgent or non- standard rules required by the organization - Assists the Information Security Officer in managing the Firewall Configuration Policy
Internal Auditors	- Applies the Firewall Configuration Policy into specific firewall rules on the network devices utilized as security devices - Logs and analyses requests for urgent or non- standard rules required by the organization - Assists the Information Security Officer in managing the Firewall Configuration Policy

5.3 Dependence on other documents and procedures

Vendor delivered User Manuals for firewalls
Vendor delivered Administration Manuals for firewalls
Vendor delivered User Manuals for network equipment
Vendor delivered Administration Manuals for network equipment

6. Audit of compliance to the documented process

Responsibility for audit of the proper compliance to this document is delegated to
- Information Security Officer
- Internal Audit Department

Audit is mandated at least annually, and report of audit findings are delivered to
- Top management – summary report
- Line management of departments where responsible personnel is positioned – detailed report

In case of non-compliance to the policy defined in this document, the organization can apply the penalties and disciplinary action as defined within the Corporate Employee Conduct Guidelines.

7. Control documents

- Review Firewall Audit Trail Log
- Review Configuration Database Log

8. Reference documents

Corporate Security Policy
Corporate Employee Conduct Guidelines

9. Recipients

All employees performing the following roles

- IT Manager
- Network Administrator
- Internal Auditor
- Direct Line managers of specified roles

Appendices

Any appendices relating to the document in question (attendance sheets, forms, printouts etc)