Firewall Policy

Document Classification:	
Document Ref.	
Version:	**1**
Date:	
Document Author:	
Document Owner:	

Revision History

Version	Date	Revision Author	Summary of Changes

Distribution

Name	Title

Approval

Name	Position	Signature	Date

1 Purpose

In accordance with industry 'best practices' and to comply with numerous compliance regulations, $Company$ has prepared various Information Security policies and procedures which are intended to protect the confidentiality, integrity and availability (CIA) of their critical client data and their computing resources. This document describes firewall policy at $Company$ in defining and administering these policy and procedures.

2 Policy Statement

The role of the firewalls are to regulate, monitor and provide access control between the trusted internal network and untrusted external networks. In addition, the firewall provides authentication and hides the $Company$ network information from untrusted networks.
All employees of $Company$ are subject to this policy and required to abide by it.

2.1 Responsibilities

$Company$ IT Dept is responsible for implementing and maintaining $Company$ firewalls, as well as for enforcing and updating this policy. Logon access to the firewall will be restricted to a primary firewall administrator and IT personnel assigned to backup this function. Password construction for the firewall will be consistent with the strong password creation practices outlined in $Company$'s Password Policy.

Any questions or concerns regarding the firewall should be directed to the IT Department.

2.1.1 Roles

- Firewall Administrator
- Firewall Lead
- Change Control Board

2.2 Firewall policy details

$Company$'s firewalls will be implemented in accordance with the following high-level policies and guidelines:

- All non-essential networking or system services must be eliminated or removed from the firewall.
- The system logs generated from the firewall must be reviewed periodically to detect any unauthorized entry attempts. These logs should be backed up and archived periodically.

- All unauthorized access through the firewall must be reported to the security manager and network administrator.
- Networking traffic will be subject to filtering based on current security requirements.

2.3 Firewall configuration

The approach adopted to define firewall rule sets is that all services will be denied by the firewall unless expressly permitted.

The firewall permits outbound and inbound Internet traffic:

- Outbound – List all authorized traffic allowed outside of $Company$ network.
- Inbound – Only Internet traffic from outside $Company$ that supports the business mission of $Company$.

2.4 Operational Procedures

2.4.1 Firewall change management

$Company$ employees may request changes to the firewall's configuration in order to allow previously disallowed traffic. A change request form, with full justification, must be submitted to the IT department for approval. All requests will be assessed to determine if they fall within the parameters of acceptable risk. Approval is not guaranteed as associated risks may be deemed too high. If this is the case, an explanation will be provided to the original requestor and alternative solutions will be explored.

2.4.2 Approval for inbound connections

$Company$ employees may request access from the Internet for services located on the internal $Company$ network. Typically, this remote access is handled via a secure encrypted virtual private network (VPN) connection. In certain cases, firewalls are used to establish such VPN connections.

From time to time, outside vendors, contractors, or other entities may require secure, short-term, remote access to $Company$'s internal network. If such a need arises, an access request form, with full justification, must be submitted to the IT department for approval and approval must be granted by the CISO.