# NAME OF THE STOCKBROKER

---

# CONFIGURATION SECURITY MANAGEMENT POLICY

# POLICY CONTROL

| | |
|---|---|
| Version: | 1.0 |
| Version Date: | _____ (Date of Passing Board Resolution) |
| Approved by: | Board of Directors |
| Department in Charge: | |
| Frequency of Review: | Yearly or as and when any update comes change in the Relevant Regulation comes or any change in the Company's internal control or Structure whichever is earlier. |

# TABLE OF CONTENTS:

# CONFIGURATION SECURITY MANAGEMENT POLICY

## I. PURPOSE:

The purpose of this policy is to enhance security and quality operating status for workstations utilized at organization. IT resources are to utilize these guidelines when deploying all new workstation equipment. Workstation users are expected to maintain these guidelines and to work collaboratively with IT resources to maintain the guidelines that have been deployed.

## II. GOAL/OBJECTIVE:

The overriding goal of this policy is to reduce operating risk. Adherence to the Configuration Security Policy will:

1. Eliminate configuration errors and reduce work station outages
2. Reduce undocumented configuration changes that tend to open up security vulnerabilities
3. Facilitate compliance and demonstrate that the controls are working
4. Protect data, networks, and databases from unauthorized use and/or malicious attack

## III. APPLICABILITY:

This policy applies to all company-owned, company operated, or company controlled equipment. All established standards and guidelines for the company's IT environment are documented in an IT storage location.

## IV. MINIMUM SYSTEM REQUIREMENTS:

The following outlines company's minimum system requirements for work station equipment.

- Operating System (OS) configuration must be in accordance with approved procedures.
- Unused services and applications must be disabled, except where approved by the VP of IT.
- All patch management to hardware will be monitored through reporting with effective remediation procedures. Company has deployed a patch management process; reference the Patch Management Policy.

- All workstations joined to the company's domain will automatically receive a policy update configuring the asset to obtain future updates from our desktop management system.
- All systems within company are required to utilize anti-virus, malware, and data leakage protection. IT will obtain alerts of infected workstations and perform certain remediation tasks.
- All asset will utilize the company domain so that all general policies, controls, and monitoring features are enabled for each of them. No system should be managed manually but should be managed through some central tool or model in order to efficiently manage and maintain system security policies and controls.
- Third-party applications, including browsers, shall be updated and maintained in accordance with the patch management program.
- Any critical security updates for all applications and operating systems need to be reviewed and appropriate actions taken by the IT Department to guarantee the security
- By default, all hardware asset joined to the company domain will obtain local security settings through policies.

This policy is complementary to any previously implemented policies dealing specifically with security and network access to company's network. It is the responsibility of each employee to protect technology-based resources from unauthorized use and/or malicious attack that could result in the loss of member information, damage to critical applications, loss of revenue, and damage to company's public image. Procedures will be followed to ensure resources are protected.

## V. CLARIFICATION/INFORMATION:

In case of any clarification/information required on the implementation of the Policy, please contact the IT Head/Compliance Officer on Email -_____, Tel No._____.

## VI. REVIEW:

The said policy shall be reviewed by the Board of the Directors on a yearly basis or as and when any update comes change in the Relevant Regulation/Circular comes or any change in the (Name of the Stock Broker)'s internal control or Structure. The Compliance officer has the authority to give direction to undertake additions, changes, and modifications, etc. to this Policy, and the same shall be effective per the authority of the Compliance Officer and thereafter be ratified by the Board of the Directors at its next review.

**X-X-X-X-X**