NAME OF THE STOCKBROKER

PATCH 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:

PATCH MANAGEMENT POLICY

I. OVERVIEW:

Patch management policies are a set of guidelines to ensure controlled, efficient and secure patching. These guidelines contain steps and procedures that one should follow when patching bugs and vulnerabilities. There are different types of patches - security patches, hotfixes, service packs, and so on.

II. SCOPE:

This policy applies to all resources that connect to the organization's network, enable the organization's mission, or host the organization's data. The organization will maintain and track a formal list of resources within the scope of this policy.

Patch management relies upon accurate lists of existing systems and software for updates.

III. PATCH AND UPDATE ACQUISITION:

The IT Department will continuously monitor and scan a variety of sources to obtain information regarding the release of updates and patches for all assets. Sources may include, but are not limited to: security mailing lists, vendor notifications, and websites.

When a patch or update becomes available, the IT Department will find and verify the validity of the source prior to downloading the update. The preferred method is to obtain patches directly from the source vendor or from a service provider that obtains updates directly from the source vendor.

IV. POLICY:

- Stock Brokers should establish and ensure that the patch management procedures include the identification, categorization and prioritization of patches and updates.
- An implementation timeframe for each category of patches should be established to apply them in a timely manner and simultaneously patching should not hamper the work and progress of teams
- Patches and hot fixes for correcting errors must be tested (possibly on separate environment) before using on operational systems, to ensure that the availability of the operational system is not compromised.

- If vulnerabilities cannot be eliminated, they must be monitored appropriately to prevent abuse.
- Stock Brokers should perform rigorous testing of security patches and updates, where possible, before deployment into the production environment so as to ensure that the application of patches does not impact other systems.

V. PROCEDURE OF PATCHING:

Once a patch has been obtained and prioritized, the following steps should be followed:

- ***Patch Testing***
  - The IT Department may decide to test the patch in a test environment to check for possible business disruption or other issues. Patches that fail the testing process may be excluded from the patching process so long as the IT Department follows the Exception and Mitigation process.
  - Third-party vendors and patch management services or tools will test patches in generic environments. However, unintended consequences may be experienced for specific IT architectures or dependent systems.
  - Testing patches in a test environment allows the IT Department to discover those issues in an environment that will not affect business processes. Not all organizations have the resources to perform patch testing and patch testing for low value resources may not be a cost-effective use of time or resources.

- ***Patches Management Preparation***
  - Not all patches will be applied successfully or without issue. In some cases, a patch may render a device unusable or cause cascading problems to other IT systems or software. To prepare for this possibility, the IT Department must ensure that the Disaster Recovery Policy has been executed prior to the Patch Management process.
  - For firmware updates to critical systems (routers, servers, etc.), a backup system may be required to be in place should the firmware update render the original device non-functional.
  - For unsuccessful updates, the IT Department will attempt to roll back the system or software to a previous version to recover functionality.

- ***Automated Patch and Update Management***
  - Many vendors enable automated patching procedures for their individual applications. Additionally, there are a number of third-party tools and service providers to assist in the patch management process.
  - The IT Department must ensure that all patch management preparation has been completed successfully prior to allowing any automated processes to proceed.
  - iv. Manual Patch Management
  - Some patches and updates (especially firmware) will require a manual process. For updates that do not disrupt business processes the IT Department may apply

the patch at their discretion within the allocated time given the urgency of the patch and update.

- Some patches may require the shutdown of critical business systems. To avoid excessive disruption, these Maintenance Windows need to be scheduled and approved in advance by the Patch Management Authority, preferable with the consent of the appropriate business managers affected by the disruption.
- For emergency patches required in the absence of the Patch Management Authority, the next available executive in the organization chart can approve the maintenance window.

➢ ***Patch Verification and Testing***

- Once the patching and updating process completes, the IT Department should check that the patches applied successfully or report and fix unsuccessful patches. The IT Department should also verify that vulnerabilities addressed by the patch have indeed been mitigated or eliminated by the patch.
- Vulnerabilities that remain exposed must be addressed as required under Exceptions and Mitigations.

VI. 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._____.

VII. 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. Periodic audits will be conducted to ensure compliance with this policy.

X-X-X-X-X