NAME OF THE STOCKBROKER

VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) 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:

VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) POLICY

I. OVERVIEW:

VAPT is process of identifying, evaluating, treating and monitoring/reporting on software insecurities and misconfigurations of endpoints.

II. PURPOSE:

The purpose of this policy is to grant authorized entities access to networking, computing, and information resources for the purpose of conducting audits, including vulnerability assessments and penetration tests.

Audit is conducted to:

- Investigate possible security threats.
- Test the security of information systems.
- Make sure that the information is only accessible by the individual who should be able to access it.
- Make sure system is protected from any unauthorized modification.

III. POLICY:

- Company should regularly conduct vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet.
- With systems publicly available over the internet should also carry out penetration tests, at-least once a year, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks that are exposed to the internet.
- In addition, vulnerability scanning and penetration testing be conducted prior to the commissioning of a new system that is accessible over the internet.
- Member shall report any vulnerabilities observed to the vendors and the exchanges in a timely manner.
- Remedial actions should be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.

IV. VULNERABILITY MANAGEMENT:

Vulnerability management includes the following functions:

- Assessing assets for known vulnerabilities
- Prioritizing those vulnerabilities based on risk and impact
- Remediating vulnerabilities through patching, configuration management or deployment of compensating controls

V. PATCH MANAGEMENT:

- IT Team of the company is responsible for patch management, operations, and procedures.
- All devices must be scanned on a regular basis to identify missing updates.
- All missing software patches must be investigated by IT Team.
- The status of the software deployment must be periodically checked.

VI. PENETRATION TESTING:

- Penetration testing of the internal network must be conducted annually.
- Exploitable vulnerabilities found during the assessment shall be corrected and re-tested by IT Team.

VII. PERIODIC VULNERABILITY ASSESSMENT:

- VAPT shall be conducted on an annual basis.
- The tools used to scan and assess must be enterprise-class and must be capable of scanning the systems from a central location and also provide remediation suggestions.
- Scans must be performed during appropriate business hours and minimize disruptions to normal business functions.
- All data from scans are to be treated as confidential.
- Any temporary changes to the internal systems shall not be made for the purpose of passing the vulnerability assessment.
- Any attempt to tamper with the results will be referred for disciplinary action.

VIII. CONCLUSION:

This policy is to be reviewed on an annual basis to ensure that proper security procedures are being followed. If the results of the security audit result in an identified weakness, company will act immediately to resolve the issue.

IX. 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._____.

X. 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