Woodstock Broking Pvt. Ltd.

1201, 12th Floor, B Wing, 81 Crest,
Linking Road, Next to HDFC Bank,
Santacruz (w), Mumbai – 400 054
Tel. No. 022 69699000

SEBI Regn. No. INZ 000242835

Information Security Awareness and Training Policy

1. Purpose

The purpose of this policy is to establish a structured Information Security Awareness and Training Program for all employees, contractual staff, consultants, interns, and vendors to ensure awareness of information security risks, regulatory requirements, cybersecurity threats, and their responsibilities in protecting organizational information assets.

2. Scope

This policy applies to:

- Permanent and temporary employees.
- Directors and senior management.
- Contractual staff, consultants, and interns.
- Third-party vendors, service providers, and outsourced personnel having access to the organization's information systems, networks, data, or premises.

3. Objectives

The Awareness and Training Program aims to:

- Promote a culture of information security and cybersecurity awareness.
- Ensure compliance with applicable regulatory requirements, including SEBI, Exchange, Depository, and applicable cyber security guidelines.
- Educate personnel about emerging cyber threats and security best practices.
- Reduce the risk of security incidents caused by human error.
- Ensure that vendors understand and comply with the organization's security requirements.

4. Roles and Responsibilities

Management

- Support and promote security awareness initiatives.
- Ensure adequate resources are available for training programs.

Information Security Officer (ISO) / Compliance Officer

- Develop and maintain the awareness training program.
- Conduct periodic training sessions.
- Monitor participation and effectiveness.
- Maintain training records and attendance.

Employees

- Attend mandatory awareness training sessions.
- Complete assigned security assessments.
- Follow organizational security policies and procedures.

Vendors and Third Parties

- Participate in awareness programs where applicable.
- Comply with organizational information security requirements.
- Acknowledge understanding of security obligations before being granted access.

5. Awareness Training Program

Employee Training

The organization shall conduct awareness training covering:

- Information Security Policy.
- Cybersecurity risks and threats.
- Password and authentication security.
- Phishing and social engineering attacks.
- Data protection and privacy requirements.
- Email and internet usage security.
- Safe use of mobile devices and remote working.
- Incident reporting procedures.
- Physical security requirements.
- Regulatory and compliance obligations.

Vendor Training

Vendors with access to organizational information assets shall:

- Receive security awareness guidelines during onboarding.
- Be informed of applicable security controls and contractual obligations.
- Participate in awareness sessions whenever required.
- Confirm compliance through acknowledgments or declarations.

6. Training Frequency

Training Type	Frequency
New Employee Induction	At Joining
Employee Awareness Training	At least Annually
Refresher Training	Half-Yearly or As Needed
Phishing Awareness Campaigns	Quarterly
Vendor Awareness Program	Annually or During Onboarding
Specialized Training for IT Personnel	Annually

7. Training Delivery Methods

Training may be conducted through:

- Classroom sessions.
- Online webinars.
- E-learning modules.
- Awareness emails and newsletters.
- Posters and security advisories.
- Mock phishing exercises.
- Workshops and interactive sessions.

8. Assessment and Evaluation

The effectiveness of the awareness program shall be measured through:

- Training attendance records.
- Online assessments and quizzes.

- Phishing simulation results.
- Employee feedback.
- Reduction in security incidents attributable to human error.

9. Record Retention

The organization shall maintain:

- Training calendars.
- Attendance records.
- Assessment results.
- Awareness communications.
- Vendor acknowledgments.

Training records shall be retained for a minimum period of **five (5) years** or as required by applicable regulatory requirements.

10. Non-Compliance

Failure by employees or vendors to complete mandatory awareness training may result in:

- Restriction of system access.
- Corrective actions as per organizational policies.
- Contractual actions in case of vendor non-compliance.

11. Review of Policy

This policy shall be reviewed at least annually or whenever there are significant changes in regulatory requirements, business operations, technology, or security threats.