Vardhmān

Delivering Excellence. Since 1965.

22.0 Environment, Social & Governance

P22.16 Information Security Awareness Policy

Vardhman Group

Document Attributes

Policy Document Number	VG/ ESG/ P22.16 Information Security Awareness Policy	
Policy Owner(s)	Functional Head	
Process Approvers	Board Chairperson	
Process Council	ESG Committee	
Applicability	Vardhman Group	
Review Frequency	As & When	
Version and Issue Date	Version 01.0	January 2025

Table of Contents

22.16.1. Objectives

The purpose of this policy is to establish controls for all users with access to Vardhman Group's information technology-based resources. This policy aims to ensure that all users understand their roles and responsibilities regarding the potential risks to information security, privacy, and risk management in maintaining confidentiality and data integrity of the Group's data and systems.

This policy aims to mitigate the potential risks related to information security, privacy, and risk management.

22.16.2. Scope & Applicability

This policy applies to all employees, business partners, custodians, system administrators, software developers, and users of information who are authorized to use IT facilities and applications provided by the company.

22.16.3. General Principles

1. An Information Security awareness program should ensure that all users achieve and maintain an understanding of Information Security matters, such as general obligations as per Information Security policy, information security domain policies, standards, procedures, guidelines, laws, regulations, contractual terms plus generally held standards of ethics and acceptable behavior.

2. Additional training is appropriate for users with specific obligations towards Information Security that are not satisfied by basic training, e.g., Information Risk and Security Management, Security Administration, Site Security, and IT/Network Operations personnel. Such training requirements must be identified in users' personal training plans and funded accordingly. The particular training requirements shall reflect users' relevant prior experience, training, and/or professional qualifications, as well as anticipated job needs.

3. Information Security awareness session shall be included in the induction program and acknowledgment shall be obtained from the user. The awareness activities should continue on a continuous/rolling basis thereafter in order to maintain a reasonably consistent level of awareness of current issues and challenges in this area.

4. The Head of Information Security shall ensure a review of the Information Security Awareness program annually and appropriate updates are applied based on the findings of the annual reviews.

5. The information Security team shall use all possible channels for providing training in order to fully utilize modern training technologies. The types of channels that may be used include:

   - Classroom training sessions;
   - Yearly question and answer sessions.
   - The training channels may also be integrated with the organization's regular activities like the following:
   - Employee induction programs;

- Town Halls; and
- Security Moments" in meetings.

6. To promote security awareness and ensure all users understand the importance of maintaining information security, the IT security lead may implement the following programs:

- **Security Awareness Week** – A week designated as "Security Awareness Week" may be announced and observed with every security awareness project possible. Such a week shall act as a focus point to initiate or enhance other projects and to raise employee awareness regarding the importance of information security.

- **Electronic Mail** – Bulletins addressing information security topics may be developed and may include descriptions of security incidents, the possible impact of security breaches, and how an effective security posture can act as an enabler for business operations.

- **Posters** – Posters may be created with Information Security themes and posted at common meeting locations to heighten user awareness of security issues.

- **Screensavers** – The security awareness project team could develop screensavers to provide and improve information security awareness.

22.16.4. Escalation

1. In case of complaints related to the breach of this policy below escalation matrix shall be followed:

Level	Escalated to	Mail Ids
Level 1	IT Security Manager	sanjaygoyal@vardhman.com
Level 2	CIO	rakeshmishra@vardhman.com

2. If any Employee is found guilty with this respect to an Information Security Breach, there would be penal measures according to employment regulations for employees.

22.16.5. Training & Awareness Program

1. When a new employee joins the organization, a general orientation program is conducted for all the new joiners (up to E2 level) in which the senior / IT head gives knowledge transfer about department functionality.

2. HR department maintains the program sheet and gets this sheet signed by all new joiners, which is periodically reviewed.

3. An annual review of users who completed IT Awareness training should be approved by HR and the respective HOD of the departments.

4. All existing employees must attend mandatory IT Awareness training on an annual basis.

22.16.6. Governance

- The Environment, Social & Governance (ESG) Committee of the Board shall govern the Information Security Awareness policy.
- A designated committee oversees the implementation and adherence to this policy.
- This committee is responsible for periodic assessments and reporting compliance to the management.

22.16.7. Policy Review

- This policy will be reviewed As & When needed.
- The review will primarily focus on evaluating its relevance, effectiveness, and alignment with organizational goals and security best practices, ensuring that it addresses current security threats and meets the organization's evolving needs.