Vardhmān

Delivering Excellence. Since 1965.

22.0 Environment, Social & Governance

P22.18 Information Security Policy

Vardhman Group

Document Attributes

Policy Document Number	VG/ ESG/ P22.18 Information Security Policy	
Policy Owner(s)	CIO	
Process Approvers	Chairperson of the ESG Board	
Process Council	ESG Board Committee	
Applicability	Vardhman Group	
Review Frequency	As & When	
Version and Issue Date	Version 01.0	July 2025

Table of Contents

22.18.1. Introduction 3
22.18.2. Objectives 3
22.18.3. Scope & Applicability 3
22.18.4. Governance Mechanism 3
22.18.4.1. Information Security Steering Committee 4
22.18.4.2. Information Security Management Forum Members 4
22.18.5. Organizational Roles, Responsibilities and Authorities 4
22.18.6. Communication of Information Security Policy 7
22.18.7. Information Security Management Programs 7
22.18.7.1. Vulnerability/Threat Analysis & Assessment 7
22.18.7.2. Threat and Vulnerability Assessment 8
22.18.7.3. Threat Scanning, Evaluation and Mitigation 8
22.18.7.4. Information Security related Business Continuity Plan 9
22.18.7.5. Internal Audit for Information Technology infrastructure/ ISMS 10
22.18.7.6. Escalation Process for Reporting Incidents/ Vulnerabilities or Suspicious Activities: 11
22.18.7.7. Incident Reporting by VTL Personnel 12
22.18.7.8. Incident Reporting in CERT-IN 12
22.18.8. Information Security Awareness Trainings 12
22.18.9. Privacy Policy: Systems/ Procedures 13
22.18.10. Information Security in Third Party Vendor Category 14
22.18.10.1. Vendor Profile Evaluation 14
22.18.10.2. Due Deligence/ Third Party Vendor Risk Assessment Process 14
22.18.10.3. Addressing Security within Vendor Agreements 15
22.18.11. Continual Improvement 15
22.18.12. Policy Review 15

22.18.1. Introduction

Vardhman Textiles Limited (hereafter referred as 'VTL') is committed to protect its assets and data by building a uniform framework of Information Security that addresses all security related issues.

This Information Security policy (hereafter referred as 'IS policy') provides control objectives to protect and secure VTL 's information assets & data from emerging information and cyber security threats while ensuring Confidentiality, Integrity, and Availability of its information.

22.18.2. Objectives

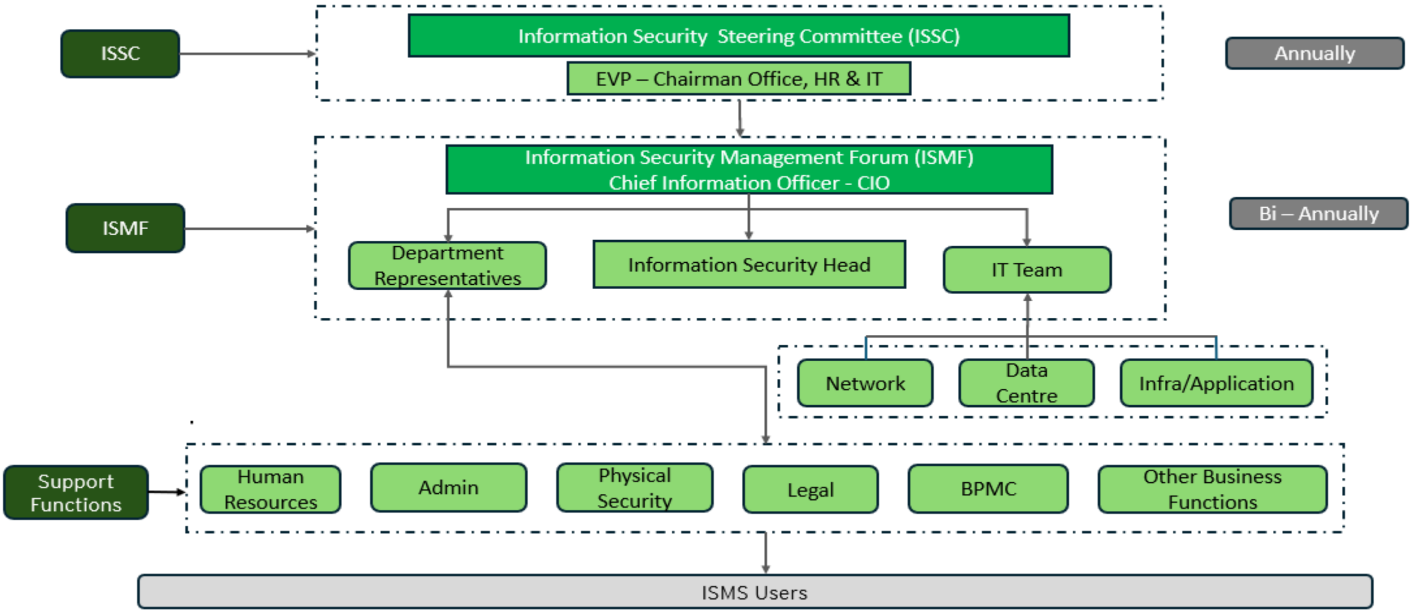
The objective of the Information Security policy is to:

- Protect confidentiality, maintain integrity, and ensure availability of the information and information processing facilities and systems.
- Manage Information Security risks to an appropriate level through design and implementation of an Information Security framework.
- Respond to and recover from Information Security incidents in a timely manner.
- Create Information Security awareness amongst employees, service providers and customers.
- Comply with applicable legal and regulatory requirements.

22.18.3. Scope & Applicability

The Information Security Policy applies to all employees, third-party employees of VTL (hereafter referred to as 'users'), and clients/ customers visiting VTL who engage in work and have access to VTL's information or information processing facilities across VTL offices.

22.18.4. Governance Mechanism


ISSC
Information Security Steering Committee (ISSC)
EVP – Chairman Office, HR & IT
Annually
ISMF
Information Security Management Forum (ISMF)
Chief Information Officer - CIO
Bi – Annually
Department Representatives
Information Security Head
IT Team
Network
Data Centre
Infra/Application
Support Functions
Human Resources
Admin
Physical Security
Legal
BPMC
Other Business Functions
ISMS Users

22.18.4.1. Information Security Steering Committee

- The Information Security Steering Committee (ISSC) is chaired by the EVP – Chairman Office, HR & IT.
- The ISSC shall meet annually (at a minimum), with additional meetings as required based on organizational needs or changes impacting information security and VTL ISMS.
- The ISSC shall comprise the following members:
  - CIO
  - Information Security Head
  - IT Team
  - Head of Department from Human Resources, Administration, Physical Security, Legal, BPM Cell
  - Representatives from other business functions as required

22.18.4.2. Information Security Management Forum Members

- The Information Security Management Forum is chaired by the CIO.
- The Information Security Management Forum (ISMF) shall meet bi-annually (at a minimum). Meetings may be conducted in case of any changes within the VTL ISMS.
- The Information Security Management Forum (ISMF) shall comprise of the following members:
  - CIO
  - Information Security Head
  - IT team
  - Department Representatives (HODs from HR, Legal, Administration, IT Infrastructure & other departments as applicable)

22.18.5. Organizational Roles, Responsibilities and Authorities

A. Information Security Steering Committee (ISSC)

Role:

- Provide strategic oversight, direction, and decision-making for the ISMS.

Responsibilities:

- Assess industry cyber threats, lessons learned, and defence measures.
- Review audit results, risk assessment status, and compliance performance.
- Monitor strategic projects and ISMS performance metrics.
- Evaluate technology-related security topics and solution effectiveness.
- Approve resource allocation and budget for continual ISMS improvement.

Authorities:

- Approve ISMS policies, risk management methodology, and major initiatives.
- Authorize residual risk acceptance.
- Mandate compliance with ISMS objectives and policies across all stakeholders.

B. Information Security Management Forum (ISMF)

Role:

- Coordinate operational implementation, monitoring, and continual improvement of the ISMS.

Responsibilities:

- Ensure that VTL has identified the actions necessary to implement its Information Security Policy, has adequate resource to perform those actions and has integrated information security into all relevant processes.
- Ensure that activities of all individuals and entities within or from outside VTL involved in or affected by development and implementation of the ISMS are effectively coordinated.
- Review the current risk and re-evaluate risk levels as per 'Risk Management Methodology'.
- Oversee the implementation of information security controls throughout VTL, ensure adequacy and recommend amendment where necessary.
- Provide clear direction and visible support for Information Security initiatives.

Authorities:

- Recommend operational changes to ISMS controls.
- Escalate risks, compliance gaps, and resource needs to ISSC.
- Approve operational actions for risk mitigation.

C. Executive Vice President – Chairman Office, HR & IT (EVP)

Role:

- Provide executive-level endorsement and final approval for ISMS governance documents.

Responsibilities:

- Approve ISMS policies, manuals, and major governance documents after review by the CIO.
- Endorse ISMS objectives and strategic direction from a management perspective.
- Ensure adequate resources are allocated for ISMS activities.
- Demonstrate top management commitment to continual improvement of the ISMS.

Authorities:

- Sign off on final ISMS governance documents.
- Approve strategic ISMS objectives proposed by the CIO.

D. CIO – IT Head

Role:

- Provide strategic oversight, review, and approval authority for ISMS activities and risk related decisions.

Responsibilities:

- Review and approve ISMS documents, procedures, and major initiatives before EVP approval.
- Approve residual risk acceptances and Risk Treatment Plans

- Approve creation and use of generic/shared/Privileged User ID's.
- Approve results and recommendations from internal and external security assessment,
- Manage on boarding of high-risk vendors based on security evaluations.
- Report ISMS performance and risk posture to the ISSC.

Authorities:

- Approve risk acceptance and policy exceptions.
- Authorize ISMS control changes and major projects before final EVP Sign off.

E. Information Security Head

Role:

- Serve as the single point of contact for operational management, monitoring, and continual improvement of the ISMS.

Responsibilities:

- Establish, maintain, and implement ISMS policies, procedures and control.
- Maintain the Asset Register and perform periodic Risk Assessment.
- Implement the Risk Treatment Plan in accordance with the approved methodology.
- Coordinate with internal audit teams, external assessors, and relevant stakeholders.
- Organize and deliver security awareness and training programs.
- Monitor incidents, vulnerabilities, and risks, and initiate corrective actions.
- Track and close nonconformities from audits and security events.
- Submit ISMS documents and recommendations to the CIO for review.

Authorities:

- Recommend risk acceptance, policy changes, and control updates to the CIO.
- Direct operational ISMS activities and assign responsibilities to relevant teams.
- Initiate preventive and corrective measures within approved scope.

F. ISMS Users(Employees)

Role:

- ISMS Users include all users (Employees, third party users and contractual employees) that are covered (directly or indirectly) under the scope of VTL-ISMS to proactively support the ISMS management processes.

Responsibilities:

- Implements and acts in accordance with VTL's ISMS policies and procedures.
- Protects assets / services from unauthorized access, disclosure, modification, destruction, or interference.
- Executes defined ISMS processes or activities.
- Does not use systems or access information without authorization; and
- Adheres to controls put in place to protect IT assets.
- Reports for anomalies in the ISMS operations and provides suggestions in case of any improvements in the existing systems.

22.18.6. Communication of Information Security Policy

Information Security Policy is communicated and acknowledged by the employees of the entire organization through SAP Success Factor portal. The same needs to be acknowledged by the new joinees as well.

The main objective of organization's information security policy is:

- To ensure that the confidentiality, integrity and availability of its critical information and information processing facilities are safeguarded.
- To ensure that regulatory, legislative, and contractual requirements for Information Security are mutually agreed upon and adhered by the concerned parties.
- To respect the intellectual property rights of third parties whose products and services are used for business purposes.
- Protect confidentiality, maintain integrity, and ensure availability of the information and information processing facilities and systems.
- Manage Information Security risks to an appropriate level through design and implementation of an Information Security framework.
- Respond to and recover from Information Security incidents in a timely manner.
- Create Information Security awareness amongst employees, service providers and customers.
- Comply with applicable legal and regulatory requirements.

Information Security Awareness Policy is shared and communicated with the company's employees as well as for general public through Vardhman's Website under the section ESG Policies.

22.18.7. Information Security Management Programs

The main objective of information security management procedure is to protect confidentiality, maintain integrity and ensuring availability of the information and information processing facilities and system.

- Manage Information Security risks to an appropriate level through design and implementation of an Information Security framework.
- Respond to and recover from Information Security incidents in a timely manner.
- Create Information Security awareness amongst employees, service providers and customers.
- Comply with applicable legal and regulatory requirements.

22.18.7.1. Vulnerability/Threat Analysis & Assessment

- Vulnerability analysis has been performed to set up to setup a standardized approach for conducting vulnerability assessment and penetration testing.
- Proactively detect vulnerabilities in elements of deployable or deployed information systems and/ or networks before those vulnerabilities are exploited.

- Setup a standardized process for patching which is crucial to fix vulnerabilities, enhance overall cybersecurity posture, maintain system stability, thereby maintaining compliance.

22.18.7.2. Threat and Vulnerability Assessment

Security risks associated with technical vulnerabilities, throughout the lifecycle, shall be managed through activities such as:

- Identification, evaluation, and monitoring of applicable technical vulnerabilities.
  Note: *The parameters of the vulnerability scans shall ideally conform to the requirements of industry best standards such as OWASP, SANS and CIS*

- Vulnerability scan shall be performed as per defined frequencies:

Sr. No.	Scanning to be Performed	Frequency
1	Scanning for outdated or unsecure software versions as well as unsecure configurations	Annually
2	Scanning Critical servers such as domain controllers, anti-malware servers, DNS servers, web application servers, any servers interfacing or storing confidential data, and any other servers deemed necessary	Annually
3	Scanning critical network hardware such as perimeter routers and firewalls, switches, open communications ports, host operating system patch levels or other network and hardware deemed necessary	Annually
4	Scanning Workstations and endpoints, which handle confidential or restricted data	Annually
5	Scanning Applications and services running on target systems to identify known vulnerabilities or high-risk weaknesses	Annually

- External parties shall conduct vulnerability scans and penetration testing on the VTL's assets after seeking necessary approvals from Information Security Head & CIO.
- All vulnerability/Threat scan findings shall be secured from unauthorized disclosure with compliance to the NDA signed between the VTL and the external party. Also, all documentation related to Technical Vulnerability Management shall be classified as "Confidential", protected accordingly, and shall be made available only on a need-to know basis.

22.18.7.3. Threat Scanning, Evaluation and Mitigation

- Each relevant technical vulnerability shall be evaluated for both applicability and criticality.
- Applicable technical vulnerabilities shall be recorded against applicable assets.
- The recommendations and corrective actions should be provided by the external party (in case services availed) for the prioritized vulnerabilities as a part of vulnerability remediation plan.
- Information asset owners along with IT Team shall follow the below mentioned remediation timeframes.

- If short term remediation is not possible, compensating controls should be identified in order to mitigate the risk. These compensating controls should be applied for High and Medium vulnerabilities.

Vulnerability Risk	Resolution time frame (after scan report)
Critical	01 - 07 days
High	< 30 days
Medium	Resolved in 30 - 45 days
Low	No specific SLA

22.18.7.4. Information Security related Business Continuity Plan

It is the ability and readiness to combat identified disasters to ensure continuity of critical business processes at an acceptable level and limit the impact of the disaster on people, processes, and infrastructure.

A. Ensuring Continuity of IT Infrastructure

- Identification of minimum infrastructure including IT resources and office automation equipment.
- Arrangements for restoring/sourcing assets.
- Adequate insurance coverage for assets (As applicable)

While ensuring the continuity of People, Processes, and Infrastructure the information security requirements for each should be taken into consideration.

B. IT Continuity Team

The IT Team should take primary responsibility of creation, testing and implementation of an IT Continuity Plan. This should at a minimum include:

- Business Impact Analysis.
- Formulation of IT continuity strategy taking into consideration the applicable processes and the Company’s objectives and priorities.
- IT Continuity Plan.
- Review and approval of IT Continuity Plan.
- The IT team should make all final decisions regarding all aspects of the IT Continuity Plan.

C. Implementing Information Security Continuity

The VTL shall establish, document, implement and maintain process to ensure the required level of continuity for information security during adverse situation.

VTL shall ensure that:

- An adequate team is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience, and competence.

- Documented plans, response and recovery procedures are developed and approved, detailing how the VTL shall manage a disruptive event and shall maintain its information security to a predetermined level, based on management-approved information security continuity objectives.
- The DR environment along with Disaster Recovery (DR) processes shall be implemented in such a way, to provide the product/service/application to the business within signed off RTO and RPO, which includes the time for invocation of disaster.

22.18.7.5. Internal Audit for Information Technology infrastructure/ ISMS

Internal Audit will be carried out on an annual basis or whenever any significant changes are being made to check the compliance level of ISMS as well to check whether ISMS policies and procedures are being implemented properly.

A. Guidelines for Internal Audit:

- The Internal Audit will be conducted by a team of independent Information Security Auditors.
- The Audit shall be carried out to check the compliance level as compared to the ISO 27001 standard.
- The Audit shall be conducted to check whether the security policies and procedures defined are being implemented properly
- Auditors cannot audit their own function.
- The Auditor shall also check whether the controls selected are efficient enough.
- The process/department head should follow up with the concerned people and close or fill the gaps identified.
- The security team shall monitor the corrective actions.
- The Audit report should be presented to Information Security Head & CIO and appropriate timelines, and owner should be designated to close the findings.

B. External Audit:

Vardhman has been gone through the external audit of the IT infrastructure and/or information security management systems under ISO 27001:2022. It consititute the detailed audit of IT Infra/ Access, Leadership, Planning, Controls over third party communications , Performance evaluations , People controls, Information transfer, Interaction with customers, Physical and Environmental security, Resources, Equipment and Utility, Physical Assets, Networks and IT Operations. Prime Locations covered under the scope were:

Corporate Office:

- Vardhman Textiles Limited, Corporate Office, Chandigarh Road, Ludhiana, Punjab-141010, India.

Data Center:

- Data Center (DC Site) Store Building, Ground Floor, Vardhman Spinning & General Mills, Unit of Vardhman Textiles, Chandigarh Road, Ludhiana, Punjab-141010, India.

Disaster Recovery Site:

- Data Center (DR Site) Production Hall No-1Vardhman Yarns Satlapur, Mandideep – Madhya Pradesh, India

Departments Under Scope:

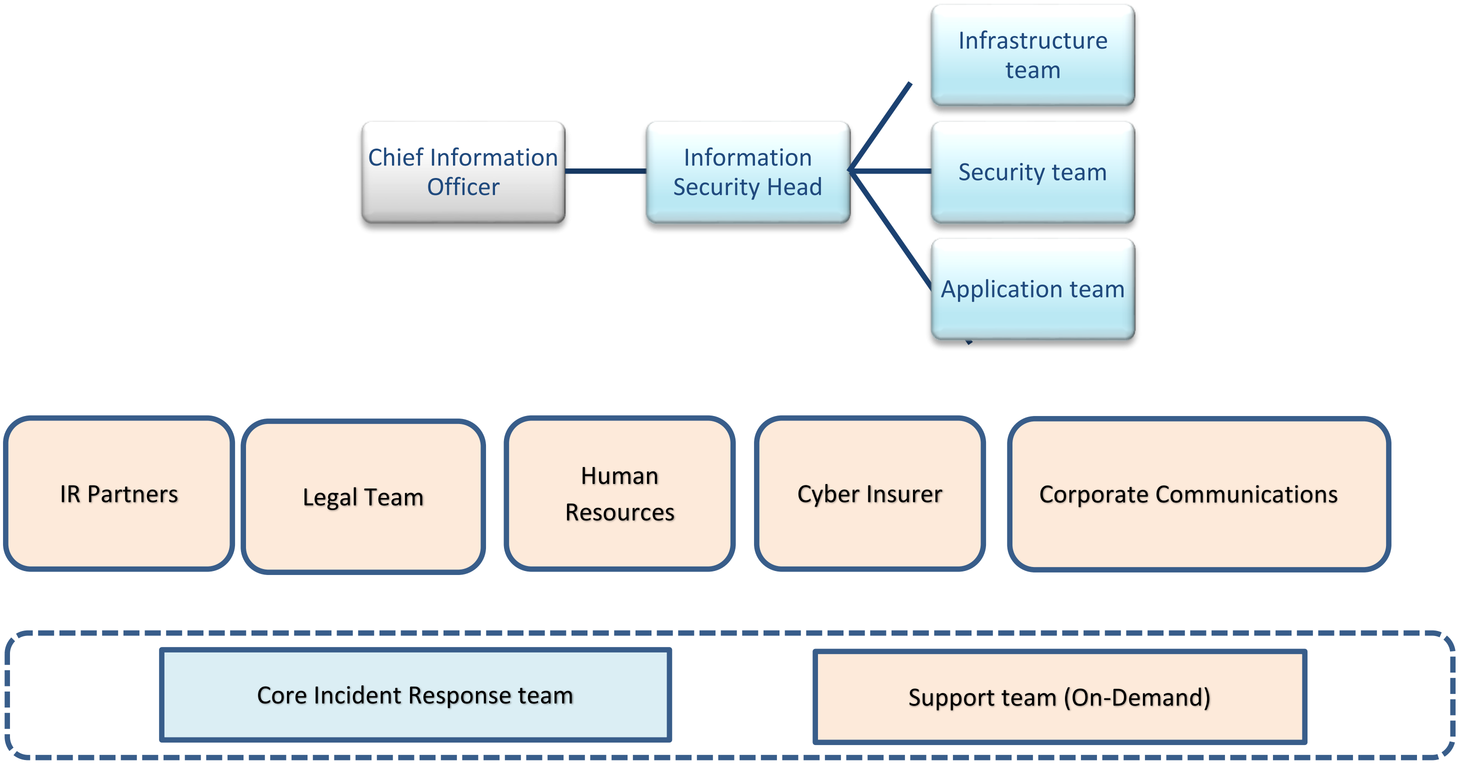
- Information Technology
- Human Resources
- Administration
- Legal

22.18.7.6. Escalation Process for Reporting Incidents/ Vulnerabilities or Suspicious Activities:

The Information Security Head shall have the overall accountability for security incident management. The Information Security Head shall be responsible for conducting a review of this procedure as triggered by any of the following:

- Any change in Incident Management team structure,
- Result of post incident
- One year has passed since the last review of the procedure.

The Security Incident Management team shall comprise of multi-disciplinary teams and will be headed by Information Security Head. The team shall perform their respective allocated function as per this procedure and ensure that the incident is remediated within least resolution time possible and the escalation shall be raised as per below:



22.18.7.7. Incident Reporting by VTL Personnel

- Any information security events, incidents, and/or weaknesses shall be reported to the IT team via emails.
- The reporter shall note relevant and important details (like occurrence of malfunction, type of messages on screen, strange/ suspicious behaviour, etc.) and share it when reporting the incident.
- The employee shall take necessary steps to ensure that the site of event/incident is kept intact, and the evidence is not tampered. He/she shall not try to resolve the event/incident on his/her own and in effect tamper with the evidence.
- After reporting an event/incident which has impacted an asset, the employee shall not continue work from the same system on which the incident was reported until explicit clearance is given to do so.
- Reporting system shall be attended during official working hours and shall capture incident details received.
- The Information Security Head shall determine if external agencies, law enforcement, or other entities need to be involved in resolution of the incident.

22.18.7.8. Incident Reporting in CERT-IN

Following type of cyber security incidents shall be reported to CERT-IN, post review from Information Security Head and approval from CIO, if there is an impact in continuity of normal business functions.

- Attack on servers such as Database, Mail, DNS, and network devices such as Routers, Firewalls, Switches
- Identity Theft, spoofing and phishing/spear phishing attacks.
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Data Breach/ Data Leak.
- Targeted scanning/probing of critical networks/systems
- Compromise of critical systems/information
- Unauthorized access of IT systems/data
- Defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code, links to external websites, etc.
- Malicious code attacks such as spreading of virus/worm/Trojan/Bots/ Spyware/Ransomware
- Attacks or incident affecting Digital Payment systems.
- Attacks or malicious/ suspicious activities affecting Cloud computing systems/ servers/ software/ applications.

22.18.8. Information Security Awareness Trainings

- All users joining VTL's shall undergo information security awareness training as part of their induction process managed by the HR department.
- Refresher training in security awareness should be conducted annually for all users who have access to VTL's information systems.

- This procedure will be updated and re-issued at least annually to reflect changes to applicable law, update, or changes to VTL's requirements, technology, and the results or findings of any audit.
- In general, this procedure applies to all VTL employees and users with access to VTL systems, networks, company information, non-public personal information, personal identifiable information, and/or customer data.
- VTL's may allocate role-based training to the IT team, if required, from time to time.

Note: *No breach incidents occurred in vardhman, hence not reported.*

22.18.9. Privacy Policy: Systems/ Procedures

The Vardhman group recognizes the importance of having effective and meaningful privacy protections in place when it collects, uses, and discloses 'Personal Information'. These protections are necessary to instill confidence in Vardhman group's membership, whose employees may furnish 'Personal Information' to Vardhman group and are themselves subject to local privacy and data protection laws, as well as to ensure Vardhman group's own compliance with such laws.

This policy applies to the collection, use, and disclosure of 'Personal Information' by Vardhman group or authorized third-party agents in any format, including electronic, paper, or verbal. Vardhman group may develop more detailed guidance or procedures to address discrete privacy concerns involving individual Vardhman Group programs, activities, or initiatives, as appropriate.

This policy shall be applicable to each & every employee (Staff & above cadre only) of Vardhman group. Privacy related issues shall be looked after by the Corporate Legal Department of the Vardhman group.

A. Privacy and Protection of Personally Identifiable Information:

Organisation shall identify all personal identifiable information residing in their environment. The following information (but not limited to) shall be protected:

- Name, such as full name, maiden name, mother's maiden name, or alias.
- Personal identification number, such as government ID details, passport number, driving license number, taxpayer identification number, or financial account or credit card number.
- Personal characteristics, including photographic image, fingerprints, handwriting, or other biometric data.
- Organisation shall minimize the use, collection, and retention of PII to what is necessary to accomplish their business purpose.
- Organisation shall categorize PII by confidentiality impact level and apply appropriate safeguard. The following can be followed to serve the purpose-
- Creating Policies and Procedures
- Conducting Training
- Using Access
- Implementing Access Control for Mobile Devices accessing corporate data
- Providing Transmission Confidentiality

- Auditing Events
- Organisation incident response plans shall be referred while handling breaches involving PII.
- Organisation shall implement appropriate technical and governance measures to protect personally identifiable information.

22.18.10. Information Security in Third Party Vendor Category

- VTL shall identify and mandate information security controls to specifically control and govern third party vendor access to the organization's assets.
- VTL shall identify and document the types of third-party vendors whom the organization shall allow to access its information.
- Information access to the third-party vendors shall be controlled and monitored.
- VTL shall identify minimum information security requirements for each type of information and type of access to serve as the basis for individual third-party vendor agreements
- Vendors shall be informed of their obligations to protect VTL's information.
- An agreement signed by both parties shall include information security requirements and controls.

22.18.10.1. Vendor Profile Evaluation

- The HOD / Engagement Manager/CPPD originating the requirement of the vendor services shall perform an initial background check over the Third parties. This could be done by: Reference checks if required, with the list of clienteles provided by the vendor.
- Before onboarding any vendor, the IT/IS team in co-ordination with the EM shall ensure that vendor profiling/evaluation is done, and a vendor profile is assigned in line with section 6.1.2. Vendor Profiling Framework (Tier 1, Tier 2, Tier3). Further, in accordance with the vendor profile, assessment criterion shall be derived.

22.18.10.2. Due Diligence/ Third Party Vendor Risk Assessment Process

- Due diligence should be conducted for all vendors before selecting and entering into contracts or relationships.
- Prior experience and/or knowledge of the vendor is not an acceptable alternative for due diligence.
- A standardized vendor risk assessment should be leveraged to assess the criticality and/or sensitivity of services provided by the Tier 1 – High Profile vendor.
- The following factors shall be considered as part of due diligence processes at minimum:
  - i. Compliance with legal, regulatory, and industry requirements.
  - ii. Adequacy of internal controls including Legal, Privacy, Information, and Physical security controls.
  - iii. Ability to comply with service level performance commitments to VTL.
  - iv. Adequacy of the third party's business continuity planning and capabilities.
  - v. Adequacy of the third party's governance program over Subcontractors (4th party).
  - vi. If highly confidential / confidential information is shared with the third party, information security controls that specifically address use, applicable laws, regulations, industry

requirements, or other identified physical and information security risks and background check requirements must be included in the contract.

- The risk assessment results shall be communicated to Information Security Head, CIO followed by respective Department Head/EM & CPPD.

22.18.10.3. Addressing Security within Vendor Agreements

- All relevant information security requirements shall be established and agreed with each vendor that shall access, process, store, communicate, or provide products/services to VTL.
- VTL shall establish and document the vendor agreement to ensure that there is no misunderstanding between VTL and vendor regarding both parties' obligations to fulfil information security requirements.
- Once the vendor is selected, a formal contract shall be signed with the service provider. Contract shall include all legalities followed by VTL. The contract shall be bound by a strong Service Level Agreement (SLA) to ensure that the service provider provides a defined level of service continuously and efficiently without disrupting the operations in VTL.

22.18.11. Continual Improvement

To ensure that continual improvement takes place, internal audits are conducted at least once every year. The controls are evaluated thoroughly during internal audit by Information Security Head. Based on the outcome of various audits, non-conformities are identified, tracked and closed.

VTL is also indulged in continually improving the suitability, adequacy and effectiveness of the information security management system.

22.18.12. Policy Review

- This policy will be reviewed As & When needed.
- The policy will be reviewed to ensure it remains up-to-date, effective, and compliant with evolving legal, regulatory, and operational requirements. The review will focus on ensuring the Information Security in accordance with applicable regulations, while aligning with the organization's core values and long-term objectives, particularly in relation to data privacy and security.