Vardhman Textiles Limited		
Vardhmān Delivering Excellence. Since 1965.	**VTxL-23.04-Information Security Policy-V1.1**	Date: 21-09-2026
		Version - 1.1
		Rev No - 01

Vardhmān

INFORMATION SECURITY POLICY

Document Control Page

Document Name	:	Information Security Policy
Current Version	:	1.1

		Particulars
Document Owner	:	Information Security Head
Reviewed By	:	CIO
Approved By	:	EVP – Chairman Office, HR & IT

Classification	:	Internal
Distribution List	:	Internal Employee

All queries, suggestions and changes required may be emailed to *datacenter@vardhman.com*

Issue / Revision History

Ver. No.	Description	Author	Reviewer	Approver	Issue / Revision Date
1.0	Initial Document	Information Security Head	CIO	EVP – Chairman Office, HR & IT	31-07-2025
1.1	Annual Review (No change)	Information Security Head	CIO	EVP – Chairman Office, HR & IT	21-09-2026

Table of Contents

1. Introduction 5
2. Scope & Applicability 5
3. Policy Compliance 5
4. Objectives 5
5. Governance of Information Security 6
   - 5.1. Information Security Organization Structure 6
   - 5.2. Organisational Roles, Responsibilities and Authorities 7
   - 5.3. Policy Management 10
   - 5.4. Exception & Deviations 10
6. Information Security Policy 10
   - 6.1. Information Security management system Objectives 11
   - 6.2. Risk Management framework 11
   - 6.3. Security Metrics and Measurements 11
   - 6.4. Information Security in Project Management 12
7. Information Security Policy Domains 12
   - 7.1. Organization of Information Security 12
   - 7.2. Information Asset management 13
   - 7.3. Information Security Risk Management 15
   - 7.4. Human Resources Security 16
   - 7.5. Identity and Access Management 17
   - 7.6. Cryptography 20
   - 7.7. Physical and Environmental Security 20
   - 7.8. Communication and Operation Security 23
   - 7.9. System Acquisition, Development and maintenance 31
   - 7.10. Third Party Risk Management 33
   - 7.11. Information Security Incident Management 34
   - 7.12. Information Security Aspects of Business Continuity Management 36
   - 7.13. Cloud Security 37
   - 7.14. Information Security Assurance 38

8. Annexure 40

8.1. Definition and Abbreviations 40

8.2. References 44

8.3. Document Change Control 45

8.4. Signature 46

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.

2. Scope & Applicability

The IS 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.

3. Policy Compliance

All users shall comply with the IS policy. Intentional misuse or non-compliance with any part of the IS policy shall be construed as an offence and may result in disciplinary action.

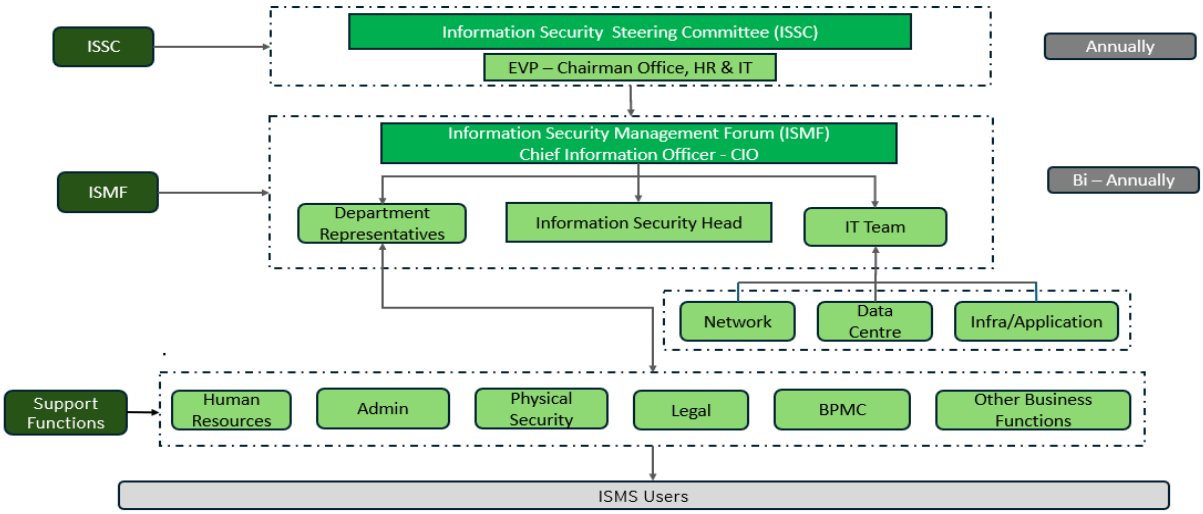
4. Objectives

The objective of the IS 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.

5. Governance of Information Security

5.1. Information Security Organization Structure



5.1.1. 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
  - Heads of Departments from Human Resources, Administration, Physical Security, Legal, BPM Cell
  - Representatives from other business functions as required

5.1.2. 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)

5.2. Organisational Roles, Responsibilities and Authorities

- **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.

- **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.

- **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.

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

- **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 IDs.
  - Approve results and recommendations from internal and external security assessments.
  - Manage onboarding of high-risk vendors based on security evaluations.
  - Report ISMS performance and risk posture to the ISSC.

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

- **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 controls.
  - Maintain the Asset Register and perform periodic Risk Assessments.
  - 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.

Authority:

- 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.

- **Information Security Team**

  Role:

  - Monitor & maintain information security within respective work areas.

  Responsibilities:

  - Create, maintain & update asset registers of respective IT sub-department and discuss with respective ISMS users and other subordinates.
  - Ensure security awareness & training programs are attended by all employees
  - Help identify information security risks within respective IT sub-department.
  - Ensure that current practices of respective IT sub-department are aligned to approved information security policies and procedures.
  - Report any management system incident / violation to authorities.
  - Coordinate periodic ISMS audits of respective IT sub-department.
  - Ensure timely closure of ISMS audit non–conformities related to respective IT sub-department.
  - Ensure all documents and records related to respective IT sub-department follow the records and document control procedure.
  - Ensure all IT assets related to respective IT sub-department are appropriately classified, labelled.
  - Ensure all information assets related to respective IT sub-department are appropriately classified and labelled.
  - Provide feedback to improve the information security posture

- **ISMS Audit (Internal Audit / External Organization)**

  Role:

  - The ISMS Audit Team shall be identified by the CIO with consent from the ISSC for periodic internal audits that are conducted against the Information Security Management System.
  - The ISMS Audit Team shall be either composed of members from VTL' Internal Audit or External organization Auditors and execute activities across VTL to ensure objectivity and the impartiality of the audit process.

  Responsibilities:

  - Carry out internal audits as per the schedule of activities defined by Information Security Head & CIO.
  - Conducts internal audits for VTL-ISMS that is falling under the scope in co-ordination with the Information Security Head
  - Submits internal audit reports to CIO & Information Security Head for review and suggestions.

- Presents summary audit reports to ISSC in coordination with Information Security Head & CIO.
- Shall submit the Audit report after the discussion in the management review meeting.
- Validate identified Non-Conformances are closed as per the agreed plan and shall report to Information Security Head & CIO.

- **ISMS Users**

  Role:
  - ISMS Users include all users (Employees, third party users) 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.

5.3. Policy Management

Information Security Head shall make the required amendments to the ISMS documents and have them reviewed by the CIO and the EVP, Chairman's Office. HR & IT shall approve the IS policy at least once a year or upon any significant change in VTL, legal, or regulatory requirements.

5.4. Exception & Deviations

- Approval for exceptions or deviations from IS policy and procedures shall be granted after assessing the risks arising out of granting the exception. This assessment shall be conducted by the IT/ IS team based on the exception management process.
- Approval for the exception shall be reviewed and approved by the department heads followed by the CIO.

6. Information Security Policy

- VTL must ensure that the confidentiality, integrity and availability of its critical information and information processing facilities are safeguarded.
- VTL must ensure that regulatory, legislative, and contractual requirements for Information Security are mutually agreed upon and adhered by the concerned parties.

- VTL must respect the intellectual property rights of third parties whose products and services are used for business purposes.

6.1. Information Security management system Objectives

- 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.

6.2. Risk Management framework

- To manage Information Security, VTL adopts a risk-based approach. This approach mandates: (Refer "*VTxL-23.06 Information Security Risk Management Procedure-V1.1"):*
  - The identification of all critical information assets.
  - The identification of threats and threat probabilities that may result in exploitation of the vulnerabilities.
  - The identification of the proper set of controls to protect these assets from the identified threats.
  - To periodically (once in a year) assess the risk to ensure it is being adequately managed, and previously identified risks are being addressed.
- The risk management involves the following steps:
  - Identification and prioritization of assets
  - Evaluation of assets
  - Identification of Threats and Vulnerabilities
  - Evaluation of existing controls
  - Identification of probability of occurrence
  - Calculation of risk
  - Risk Treatment Plan

6.3. Security Metrics and Measurements

In addition to maintaining the Information Security management system, it is imperative to monitor and measure the ongoing efforts and results of the Information Security management system. KPIs shall be defined for every procedure for specific controls implemented in VTL.

6.4. Information Security in Project Management

- Information Security shall be integrated into organizations project management methods to ensure that Information Security risks are identified and addressed as part of projects. The project management methods in use shall require that:
  - A project risk assessment is conducted at an early stage of the project to identify project risks and
  - Information Security is part of all phases of the applied project methodology.
- Information Security implications shall be addressed and reviewed regularly in all projects as per feasibility.

7. Information Security Policy Domains

7.1. Organization of Information Security

7.1.1. Internal Organization

VTL shall identify and define the necessary measures for implementing Information Security and management's responsibilities. However, it is the responsibility of VTL employees to adhere to the applicable IT policies and procedures.

7.1.2. Information Security roles and responsibilities

- Information Security responsibilities related to the protection of VTL's sensitive information, information systems, and information processing facilities shall be clearly defined through job descriptions, work allocation, and delegation of tasks.
- The Information Security policy shall be approved by the EVP – Chairman Office, HR & IT.
- Standards, procedures, templates, and guidelines shall be approved by the EVP – Chairman Office, HR & IT.
- Defined Information Security responsibilities shall be formally allocated and accepted across VTL.
- Controls necessary to adequately protect assets shall be identified and implemented.
- User access privileges shall be reviewed and approved in accordance with the user access management process at VTL.
- Internal audits, fire drills, and other audit activities shall be conducted to ensure compliance with the above policies.

7.1.3. Segregation of Duties

- Roles defined to carry out business activities must consider segregation of duties to reduce opportunities for deliberate or accidental misuse of infrastructure elements and/or software.

- Wherever segregation of duties is not possible, appropriate compensatory controls such as activity monitoring, audit trails and management supervision shall be developed to detect misuse of access rights.
- Conflicting functions (e.g., functions with ability to initiate, authorize, execute, and verify transactions) shall be identified managed.

7.1.4. Contact of Authorities

- Appropriate contacts shall be established with law enforcement authorities, regulatory bodies, third party vendors such as hardware vendors, software vendors, and office security providers.
- The responsibilities to maintain those contacts shall be fulfilled by respective teams.

7.1.5. Contact with Special interest Groups

- The Information Security Team shall maintain appropriate contacts with special interest groups, forums, and professional associations related to Information Security to:
  - Improve knowledge about best practices and keep up to date with latest developments and
  - Gain access to specialist Information Security advice.
- Such Information Security related interest groups are ISACA (Information Systems Audit and Control Association), CERT (Computer Emergency Response Team), and likewise.

7.1.6. Independent review of Information Security

The implementation of Information Security policies, procedures and technical standards shall be reviewed independently on an annual basis. Review shall be carried out by experienced persons that are suitably qualified for this purpose i.e., internally by the internal audit function or by specialist third-party consultants.

7.2. Information Asset management

7.2.1. Responsibilities of Asset

7.2.1.1. Inventory of Assets

- All assets related to information systems shall be clearly identified and an inventory of all related assets shall be drawn up and maintained.
- The IT department shall register, track, and maintain the inventory of assets and review the asset list for accuracy and completeness at least annually. (Refer: "*VTxL-23.25-Asset Management ProcedureV1.1*")

7.2.1.2. Ownership of Assets

- Information asset must have an identified owner who will be responsible for safeguarding the assets.

- The asset owner shall be responsible for proper management of an asset over the entire asset life cycle and periodic review of the asset inventory shall be taken and the same shall be documented.
- The person in possession of the asset shall be responsible for its protection.

7.2.1.3. Acceptance use of Assets

- Guidelines for acceptable use of assets shall be defined for all users. (Refer: "*VTxL-23.05-Acceptable Usage PolicyV1.1")*
- All users should understand and follow rules / guidelines for the acceptable use of information and assets; and shall be accountable for its usage.

7.2.1.4. Return of Assets

All users shall return all organizational assets in their possession on last working day of employment, upon their resignation or termination or end of contract or agreement.

7.2.2. Asset Classification and Labelling

7.2.2.1. Classification of Information & Asset

- A process shall be defined to classify, label, handle and destroy assets as per their business function criticality to minimize incidents pertaining to disclosure, modification, non-availability, and/or destruction of assets.
- Owners of Information assets must ensure that information in any form is clearly classified and labelled so that all users are aware of the ownership and classification of information. All classified information must be stored and handled according to the classification guidelines.
- Information Security controls shall be defined and implemented for handling and storage of assets based on their classification to protect the asset from unauthorized disclosure or misuse.
- Refer "*VTxL-23.26-Information Classification Guidelines-V1.1"* for guidelines on data classification.

7.2.2.2. Handling of Asset

VTL shall ensure that all information assets and associated information processing facilities are identified, classified, and managed in accordance with "*VTxL-23.25-Asset Management Procedure-V1.1*"

7.2.3. Media Handling

7.2.3.1. Management of removable Media

VTL shall ensure that all removable media are used and managed in accordance with the established "*VTxL-23.19-Removable Media Management Procedure-V1.1*". The use of removable storage media, such as USB drives, by end users shall be authorized only based on business requirements and in compliance with the procedure.

7.2.3.2. Disposal of Media

- Media containing information valued as sensitive shall be disposed of securely when no longer required, using formal procedures.
- Records of disposal, including time of destruction, name of person who destroyed it and means of disposal shall be maintained.

7.2.3.3. Physical Media transfer

Media containing information during transportation beyond physical boundaries of VTL premises shall be protected against unauthorized access, misuse, or corruption in accordance with "*VTxL_Asset Management Procedure".*

7.3. Information Security Risk Management

7.3.1. Information Security Risk Assessment

- A risk assessment methodology shall be developed and implemented on basis of:
  - Information Security objectives
  - Regulatory and compliance requirements
- Risk assessments shall be performed on an annual basis for assets and information systems based on their criticality.
- Risk assessments shall also be performed in case of any specific events mentioned below.
  - Major changes to processes, applications, network, and security architecture.
  - Addition/changes to third party services.
  - Emergence of new threats or vulnerabilities due to changes in VTL's environment.
  - Triggers from business and regulatory changes, compliance, mergers, and acquisitions etc.
- Risk assessment results shall be used to prioritize risk, treatment plan and mitigate the risks to an acceptable level.

Key risks identified shall be discussed and reviewed by the ISMF and residual risks shall be approved by the CIO

7.3.2. Information Security Risk Treatment

- A risk treatment plan shall be documented based on the risk assessment activities performed and shall be communicated to the CIO for approval.
- Identified risks shall be treated to combat threats and the reduction of potential impacts to the acceptable level within VTL's risk appetite, given the level of complexity of business using the following risk treatment options:
  - Mitigate / apply appropriate controls to reduce the risks to an acceptable level.
  - Risk acceptance by Information Security Head / Head of Department/CIO.
  - Avoiding risks by not allowing actions that would cause the risks to occur.
  - Transferring the associated risks to other parties, e.g., insurers or vendors.

Refer "*VTxL-23.06-Information Security Risk Management Procedure-V1.1*"

7.4. Human Resources Security

7.4.1. Prior Employment

7.4.1.1. Screening

- VTL is committed to ensure that all full-time employees go through a relevant screening process before starting employment to maintain a trustworthy work environment. (Refer: "*VTxL-23.13-Human Resources Security Procedure-V1.1*")
- For contractors and third-party users, if applicable, VTL shall ensure that the contract or agreement clearly specifies the responsibilities for screening and the relevant procedures they need to follow.

7.4.1.2. Terms and Conditions of Employment

- Information Security responsibilities shall be specified in terms and conditions of employment.
- Employees shall acknowledge and sign the terms and conditions including confidentiality/ non-disclosure agreement (NDA) and "Code of Conduct" as their acceptance to protect confidential and sensitive information of VTL and abide by their Information Security responsibilities.

7.4.2. During Employment

7.4.2.1. Management Responsibilities

- The user's reporting manager shall ensure that VTL employees and contractual employees under their management conform to security in accordance with the established policies and procedures.
- All users hold primary responsibility to comply with the information security policy. When in doubt, users shall seek guidance and clarifications from their line management or Information Security Team for policy interpretations.

7.4.2.2. Security Awareness

- All employees, contractors and third-party users should receive appropriate initial and ongoing security awareness training by various means for relevant organizational policies, procedures, emerging threats such as ransomware, malware, phishing etc. (Refer: "VTxL-23.15-Information Security Training & Awareness Procedure-V1.1").
- Security awareness status should be maintained as appropriate.
- Effectiveness of training shall be measured through an assessment.

7.4.2.3. Disciplinary Process

- A disciplinary process shall be established for employees, contractors and third-party users who have committed security breach and violations of any information security policy.

- VTL is committed to enforcing its Information Security policies and procedures. Any violation of those policies or procedure will be dealt with via the Disciplinary Process.

7.4.2.4. Exit, Termination or Transfer of Employment

- Access rights of employees and third-party users to information, information processing facilities and information systems shall be revoked upon termination of their employment, contract, or agreement.
- In the case of change of employment, the access rights and/or privileges granted to employees shall be formally reviewed and accordingly adjusted.
- Information Security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractors, and enforced.

7.5. Identity and Access Management

7.5.1. Business Requirements for Access Controls

7.5.1.1. Access Control Policy

- A process shall be implemented for user registration, modification, de-registration of user accounts and user access to information systems based on business requirements with approvals from authorized personnel.
- The access to information and information systems shall be based on “least privilege” and "need to know" principles as per business requirement and against formal authorization.
- Refer “VTxL-23.23-Access Control Procedure-V1.1” for detailed guidance.

7.5.1.2. Role Based Access Control

- Access to information should be based on well-defined user roles by ensuring segregation of duties.
- Clear delegation of authority for access rights to upgrade/change user profiles and permissions should be assigned and documented.

7.5.1.3. Access to Network and Network Services

Users should only have network access to the information and information systems that they are authorized to use and shall be protected through appropriate mechanism.

7.5.2. User Access management

7.5.2.1. User Provisioning, Revocation, Modification of Access Rights.

- A formal user provisioning, revocation and modification of access rights process shall be defined and implemented.
- Every user shall have a unique user ID and password for access to VTL’s systems and networks.

- The access rights of end user should be removed on the last working day (LWD) of employment, upon their resignation or termination or end of contract/agreement; and modified suitably basis change of their employment, contract/agreement.
- Generic IDs shall be restricted unless a business / technical need is identified and appropriate approvals are obtained.

7.5.3. Management of Privileged Access Rights

- The allocation and use of privileged access rights shall be restricted and controlled.
- Privileged IDs and their accesses shall be assigned to authorized users based on job role and approvals; Ownership of these IDs shall be documented and approved.
- Privilege user accounts shall be reviewed bi-annually to detect any unwanted privileges, orphan accounts, and dormant accounts.

7.5.4. Management of Secret Authentication Information of Users

- An initial password shall be communicated to the users securely during the user creation process.
- All user passwords should remain confidential and should be stored securely.
- Access to information systems shall be controlled using strong passwords. Minimum requirements for passwords shall be defined.
- Additional authentication mechanisms shall be implemented for users performing critical/privileged activities.
- Procedure shall be established and adopted for complex passwords and the frequency of change.

7.5.5. Review of Users Access Rights

Asset/application owners in coordination with business heads must review users' access rights on a Annual basis.

7.5.6. Internet Browsing Access

- Internet browsing access shall be restricted based on business needs and security risks.
- Internet browsing shall be governed by "*VTxL-23.05-Acceptable Usage Policy-V1.1*" of the company.
- User access for the purpose of internet browsing shall be only through organization's secure web proxy gateways.
- Use of anonymous proxies, anonymizers is strictly prohibited.
- Internet usage shall be monitored.

7.5.7. User Responsibilities

7.5.7.1. Password Use

- Users shall be made aware to follow good security practices in the selection and use of passwords.

- Users shall not have any such password characteristic that is predictable or easily guessed including, but not limited to, words in a dictionary, common character sequences, personal details, etc.
- Passwords shall never be shared or revealed to anyone other than the authorized user
- Users shall not store passwords in any system files, such as logon scripts or computer programs.
- All User passwords (Individual as well as Administrator) shall remain confidential and shall not be shared, posted, or otherwise divulged in any manner.

7.5.8. System and Application Access Control

7.5.8.1. Information Access Restriction

Access to VTL information and application system function shall be tied to access control procedure. Key considerations should include:

- Role-based access control
- Levels of access
- Read, write, delete, and execute permissions.
- Limiting output of information and
- Physical and/or logical access controls sensitive applications, data, and systems

7.5.8.2. Secure Log-on Procedure

Access to any information and information system should be controlled by a secure log-on process as necessary.

7.5.8.3. Password Management System

- The purpose of password management is to ensure quality passwords which meet the required level are consistently applied. It should be carefully implemented to ensure adequate and proportionate levels of protection.
- Systems for managing passwords should be interactive and should ensure quality passwords in accordance with password policy documented in "VTxL_Access Control Procedure_V1.1".

7.5.8.4. Use of Privileged Utility Program

The use of utility programs that might be capable of overriding access controls should be restricted and tightly controlled.

7.5.8.5. Access to Program Source Code

- Read and write access to source code, development tools, and software libraries shall be appropriately managed (As applicable) to ensure the integrity and security of the development environment.
- Access controls shall be implemented to restrict permissions to authorized personnel only, with different levels of access granted based on roles and responsibilities.

- Changes to source code and libraries shall be logged, monitored, and reviewed to detect and prevent unauthorized modifications. (As applicable)
- All personnel with access to source code shall be trained in secure coding practices and the importance of following established protocols for managing access.

7.6. Cryptography

7.6.1. Use of Cryptographic Controls

- Procedure for the use of cryptographic controls for protection of information should be developed and implemented. (Refer: "*VTxL-23.12-Cryptography Procedure-V1.1"*).
- Encryption shall be adopted for information assets based on the criticality of information. Standard encryption technology would be deployed for encryption unless required by regulatory requirements.
- Cryptographic controls with respect to the business requirements shall be identified and implemented.
- Digital signature certificates may be used to protect the authenticity and integrity of important electronic documents and for high value fund transfer, as necessary.

7.6.2. Key management

- Key management procedures shall be developed and adopted to define the use, protection, and lifetime of cryptography keys through their lifecycle.
- Personnel responsible for key management shall be identified.

7.7. Physical and Environmental Security

7.7.1. Secure Areas

7.7.1.1. Physical Security Perimeter

- Security perimeters shall be clearly defined, established, and maintained to protect areas containing sensitive information and associated assets. (Refer: "*VTxL-23.24-Physical and Environmental Security Procedure-V1.1*")
- These perimeters shall include physical barriers such as walls, fences, and locked doors, as well as access control measures like key cards and biometric systems to restrict entry to authorized personnel only. Regular inspections and continuous monitoring shall ensure that any breaches or vulnerabilities are promptly addressed.
- Additionally, environmental safeguards such as climate control and fire suppression systems shall be integrated to mitigate risks from physical threats. All personnel with access shall be trained and regularly updated on the importance of maintaining these security measures.

7.7.1.2. Physical Entry Controls

- Secure areas should be protected by appropriate entry controls and access points. These controls shall include mechanisms such as key cards, biometric systems, and security personnel to ensure that only authorized individuals gain access.
- Access points shall be designed and monitored to prevent unauthorized entry, with logs maintained to track all access attempts.
- Regular audits and inspections shall be conducted to verify the effectiveness of these controls, and any identified weaknesses shall be promptly addressed.
- All personnel accessing secure areas shall be trained in the proper use of entry controls and the importance of adhering to access protocols.

7.7.2. Securing Office, Rooms, and Facilities

Appropriate physical security controls shall be implemented to secure offices, rooms and facilities that contains sensitive information.

7.7.3. Working in Secure areas

Physical protection and guidelines for working in secure areas should be designed and applied.

7.7.4. Protecting Against External and Environmental Threats

- Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.
- Controls should be implemented to protect equipment and assets from environmental threats to prevent business disruption.

7.7.5. Delivery & Loading Areas

- A secure intermediate holding area shall be used for computer supplies, equipment, and other deliveries.
- The security guard / team shall issue appropriate entry pass before allowing such staff inside office premises.
- The security guard / team shall appropriately check baggage's/ vehicle/ carrier (As required) to make sure VTL's assets/ computer are not getting carried by third parties or unauthorized personnel.
- Access points such as delivery and loading areas, as well as other publicly accessible areas, shall be appropriately isolated from information assets and information processing facilities.

7.7.6. Equipment Security

7.7.6.1. Equipment Siting and Protection

- Equipment shall be sited securely and protected to prevent unauthorized access, damage, or interference. This includes placing equipment in secure locations, using physical barriers, and implementing access controls to restrict access to authorized personnel only.
- Environmental factors such as temperature, humidity, and power supply shall also be managed to protect equipment from potential harm. Regular inspections and maintenance shall be conducted to ensure the continued security and functionality of the equipment.
- All personnel responsible for managing equipment should be trained in the proper security protocols and procedures.

7.7.6.2. Supporting Utilities

- Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities such as electricity, water supply, sewage, heating/ventilation, and air conditioning.
- UPS, back-up generator, air-conditioning supporting equipment shall be adequate and periodically tested/monitored.
- Periodic drills, like fire evacuation drills, etc., shall be conducted.

7.7.6.3. Cabling Security

- Power and telecommunications cables carrying data or supporting information services shall be protected from interception or damage within VTL's premises.
- Power cables should be segregated from communications cables to prevent interference.

7.7.6.4. Equipment maintenance

- Equipment should be correctly maintained to ensure its continued availability and integrity.
- All hardware and software products shall be registered with the appropriate vendors for maintenance.
- The maintenance contracts for all hardware and software products, if applicable, shall be monitored and reviewed on a need basis.

7.7.6.5. Secure Disposal or Re-use of Equipment

Any sensitive data and licensed software shall be removed or securely overwritten prior to disposal or re-use of equipment containing storage media. Refer: "VTxL-23.25-Asset Management Procedure_V1.1" for guidelines on secure disposal of assets.

7.7.6.6. Security of Equipment and Assets off – premises

- Off-site assets shall be protected through appropriate security measures to ensure their integrity, confidentiality, and availability.

- These measures shall include secure transportation, storage in protected facilities, and the use of access controls to limit handling to authorized personnel only.

7.7.6.7. Unattended User Equipment

Appropriate security measures such as password protected screen savers or key locks, automated termination of active sessions, etc. shall be adopted by the users to protect the unattended equipment. Periodicity of timeout for the screen lock shall be set as per best practices. For laptops, the screen must be locked if the screen is closed.

7.7.6.8. Clear Desk and Clear Screen Policy

- Clear desk and clear screen guidelines should be defined and adopted by all users.
- Work areas should be free from sensitive/ critical documents. Hard copies of sensitive/ critical documents shall be kept in locked cabinets/areas.
- Sensitive/ critical documents which are no longer required shall be shredded.
- Desktop screens should not reveal any sensitive information.

7.8. Communication and Operation Security

7.8.1. Operational Procedures and Responsibilities

7.8.1.1. Documented Operations Procedures

All operating procedures for critical IT processes shall be documented and maintained within the "*VTxL_Operations Procedure_V1.1*."

7.8.2. Change Management

- Changes to systems shall be performed in a controlled manner to ensure that the risks associated with such changes are managed to an acceptable level.
- Changes to systems shall be tested (As applicable) in test environment prior to production deployment. (Refer: "*VTxL-23.18-Operations Procedure-V1.1, Section – 6. Change Management"*).

7.8.3. Configuration Management

- Configurations, including security configurations, of hardware, software, services, and networks shall be established, documented, implemented, monitored, and reviewed to maintain a secure and consistent operating environment. These configurations should be based on best practices and tailored to the specific security requirements of VTL.
- Documentation shall be maintained to ensure that all configurations are clearly defined and accessible for reference.
- Continuous monitoring and regular reviews shall be conducted to identify and address any deviations or vulnerabilities, ensuring that configurations remain effective and up to date.

- All personnel responsible for managing configurations shall be trained in the procedures and the importance of adhering to these standards. (Refer: *VTxL-Minimum Baseline Security Standards-V1.1)*

7.8.4. Patch Management

- Patch management shall include identification, classification, and application of patches in a defined timeframe.
- All VTL's systems should be updated with the latest supported stable patches and signatures.
- Periodic tests shall be conducted to verify installation of critical patches.
- Exceptions shall be maintained for patches that are not applied, due to reasons such as adverse impact on the business applications. Refer: "VTxL-23.22-Vulnerability & Patch Management Procedure-V1.1".

7.8.5. Performance and Capacity Management

- The use of resources should be monitored and tuned. Projections shall be made of future capacity requirements to ensure the required system performance.
- Critical IT resources related to each of the business processes, which need to be provided with maximum availability, shall be identified by the IT Team.
- Critical parameters and their thresholds shall be monitored for critical infrastructure elements (As applicable) and software(s) at periodic intervals to ensure required performance levels and availability. Refer: "*VTxL-23.18-Operations Procedure Section 8.2 - Capacity Monitoring Guidelines*

7.8.6. Separation of Development, Test and operational Environment

- Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational environment.
- Development personnel should not have access to production systems to prevent the introduction of unauthorized, untested, or malicious code or alter production data.

7.8.7. Segregation of Duties / Functions

- Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of VTL's information/data and assets.
- There should be segregation of the duties between Information Security function, physical security function and information technology function.
- There should be a clear segregation of responsibilities relating to system administration, database administration and transaction processing.

7.8.8. Threat Intelligence

- The IT Team Shall gather threat intelligence feeds or alerts from various external sources such as Vendor (OEM) Reports, Government Agencies, Subscription to publicly available Threat Intel web sources and analyse the feeds as per the existing threat vector or landscape and maintaining the feeds in a centralized manner to take appropriate mitigation actions.
- The IT Team shall update the appropriate Indicators of Compromise (IOCs) in their respective security devices such as Firewalls, IDS, IPS, Anti-Malware, SIEM tools to prevent VTL's environment from having any potential cyber-attack.

7.8.9. Protection from Malware

7.8.9.1. Controls against Malware

- Detection, prevention, and recovery controls to protect against malware and emerging threats shall be implemented, combined with appropriate user awareness.
- Endpoint protection software should be configured on all servers, desktops, and laptops to protect the system on a real time basis (Each file accessed should be first scanned for malware). Users should not be allowed to change these settings.
- Anti-malware tools shall be implemented to efficiently detect, prevent, and recover against malware.
- Use of unauthorized, malicious, and pirated software is prohibited by any user.
- Users should be made aware of the risks from malicious code and procedures to handle them.
- Refer: "*VTxL-23-18-Operations Procedure-V1.1, Section – 10.1 Protection Against Malware/ Threats"*)

7.8.9.2. Information Backup

- All information resources that VTL requires to carry out its daily operations shall be securely backed up at predefined frequency and retained as per business and regulatory requirements. (Refer: "*VTxL-23.18-Operations Procedure-V1.1, Section – 11. Backup & Restoration"*)
- Back-ups shall be protected from loss, damage, and unauthorized access, by use of appropriate mechanisms and stored at an offsite location.
- Restoration tests shall be carried out of the stored back-up to ensure reliability and readability.

7.8.10. Logging and Monitoring

7.8.10.1. Event Logging and Monitoring

Security logging shall be enabled for critical systems. Minimum information required for Information Security monitoring shall be defined and captured. Networks, systems, and applications logs shall be monitored to identify malicious behaviour, and appropriate actions must be taken to evaluate potential Information Security incidents. Monitoring records shall be retained in line with defined retention periods. (Refer: *VTxL-23.18-Operations Procedure-V1.1, Section – 7. Monitoring, Auditing & Logging*)

7.8.10.2. Administrator and Operator Logs

- System administrator and system operator activities shall be logged and shall be monitored to identify security anomalies as per incident response plan.
- Event logs shall be captured and stored for administrator activities. It should also be ensured that system administrator and operator do not edit /delete their logs.

7.8.10.3. Protection of Log information and Clock Synchronization

- Logging facilities and log information should be protected against tampering and unauthorized access.
- The clocks of all information systems within VTL shall be synchronized with an external time source as appropriate in line with CERT-In requirements.

7.8.11. Control of Operational Software

7.8.11.1. Installation of Software on operational System

- Only software's that has been approved by the IT department must be used.
- The installation of new software and changes to existing software on production systems shall be in line with the change management policy.
- The risks of relying on unsupported software (software for which support has been ceased by the vendor) for business-critical applications should be considered and appropriate remediation action shall be taken on the same.

7.8.12. Technical Vulnerability Management

7.8.12.1. Management of Technical Vulnerabilities

- Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, VTL's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk as per "VTxL_Vulnerability & Patch Management Procedure_V1.1".
- Vulnerability assessment (VA) shall be carried out annually for all critical infrastructure and application components in use and prior to any new or major change put into production to identify vulnerabilities.
- Applicable operating systems and platform security patches shall be applied periodically; emergency patches shall be updated on priority to address known/identified vulnerabilities.
- Application security patches/fixes shall be applied to address known/identified vulnerabilities as applicable.
- The operating system and platforms should be updated to their latest stable and supported version on a periodic basis as appropriate.

7.8.12.2. Technical Compliance Review

Information systems shall be regularly reviewed for compliance with VTL's Information Security policies and standards.

7.8.12.3. Contacts with Special interest Groups

Appropriate contacts with special interest groups or security forums or professional associations shall be maintained to receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities.

7.8.12.4. Information Systems audit Controls

Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

7.8.13. Communication Security

7.8.13.1. Network and Telecom Controls

- Networks should be adequately managed and controlled, to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
- Adequate control shall be implemented while providing remote access to end users and external partners. Refer: "VTxL-23.10-Communications Security Procedure-V1.1"

7.8.13.2. Security of Network and Telecom Service

- Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements.
- Network architecture diagrams including wired/wireless devices shall be maintained and reviewed on an annual basis or upon changes in the network.
- Systems shall be compartmentalized based on threat profile and access requirements, thereby limiting their exposure to authorized users.
- Critical network connections (internal and external) shall be maintained and periodically reviewed.

7.8.13.3. Segregation in Networks

- Groups of information services, users, information systems and external partners shall be segregated on networks through creation of virtual LANs, zones to prevent unauthorized access and
- Appropriate logical segregation shall be done and physical security infrastructures through creation of zones. Traffic flows between different zones shall be managed.

7.8.13.4. Wireless Network Security

Wireless Communication shall be used in secure manner and access shall be allowed only to authenticated users. The wireless service should protect authentication credentials using latest data encryption algorithms.

7.8.13.5. Remote Access Management

Remote access to VTL is permitted based on management approval only. Refer: "VTxL-23.23-Access Control Procedure-V1.1, Section 6 – Remote Access Management"

7.8.13.6. Firewall Policy

Firewall shall be used to control inbound and outbound network traffic to organization's data-centre network from external and internal networks to prevent unauthorized network access. Refer: "VTxL-23-10-Communications Security Procedure-V1.1, Section 5.5 – Managing Network"

7.8.13.7. Web Filtering

- Access to external websites should be managed to reduce exposure to malicious content.
- To be able to reduce the risks of employees accessing websites that contain illegal information or are known to contain viruses or phishing material, IT team shall block the IP address or domains of the website(s) that are prohibited. The IT team shall identify the types of websites which need to be blocked.
- The IT team shall block the following types of websites:
  - websites that have an information upload function unless permitted for valid business reasons.
  - known or suspected malicious websites (e.g., those distributing malware or phishing content)
  - command and control servers.
  - malicious website acquired from threat intelligence.
  - websites sharing illegal content.

7.8.13.8. Data Leakage Prevention

VTL Shall:

- Identify and classify information to protect against leakage (e.g., personal information).
- Monitor channels of data leakage (e.g., email, file transfers, mobile devices, and portable storage devices).
- Act to prevent information from leaking (e.g., quarantine emails containing sensitive information).
- Where data is backed up, care should be taken to ensure sensitive information is protected using measures such as encryption, access control and physical protection of the storage media holding the backup. Refer: "VTxL-23.18-Operations Security Procedure-V1.1, Section 10 – Endpoint Security"

7.8.14. Information Transfer

7.8.14.1. Information transfer Policies

- Adequate controls shall be in place to protect the transfer of information using different types of electronic communication channels such as secure file transfer protocol (SFTP) which should be preferred instead of file transfer protocol (FTP) as per business needs and authorization.

- Exchange of critical business information with third parties, outside organizations, and within VTL shall be protected and controlled to prevent loss, modification, destruction, or misuse of information.
- Usage of removable media shall be controlled.

Information shall be shared only with authorized recipients over electronic channels and be protected against any misuse / leakage

7.8.14.2. Agreements on Information Transfer

Agreements between organization and external parties should address the secure transfer of business information.

7.8.14.3. Electronic Messaging (Email)

- Adequate controls shall be implemented to protect the information involved in electronic messaging (e.g., emails, instant messengers) from unauthorized access, modification, or denial of service.
- Public email accounts and public instant messengers shall not be used for conducting VTL's operations, unless authorized.
- VTL's official emails shall not be forwarded to personal email account(s).
- Unless authorized, automatic forwarding of emails to an external/ internal email address shall be prohibited and all emails shall carry a legal disclaimer in the footer.

7.8.14.4. Social Media Risks

Adequate controls shall be implemented to address social media risks such as account takeover and malware distribution.

7.8.15. Confidentiality or Non- disclosure Agreements

- Non-disclosure agreements shall be defined, implemented, and maintained to address organization's information confidentiality/ non-disclosure requirements.
- All employees shall sign and comply with the non-disclosure agreement maintained by the Human Resource Team.

7.8.16. User Endpoint Device Security

Information stored on, processed by, or accessible via user endpoint devices shall be protected through robust security measures. This includes implementing encryption, access controls, and security software to prevent unauthorized access, data breaches, or malware infections. Endpoint devices shall be regularly updated with the latest security patches, and users shall be trained on safe practices for handling sensitive information. Regular monitoring and audits shall be conducted to ensure compliance with security protocols and to address any vulnerabilities promptly. Refer: "VTxL-23.18-Operations Security Procedure-V1.1, Section 10 – Endpoint Security"

7.8.17. Mobile Computing and Remote Working

7.8.17.1. Mobile Computing and Communications

- Security measures should be defined and adopted to manage the risks introduced using mobile devices. Refer: "VTxL-23.17-Mobile Device Management Procedure-V1.1"
- Mobile devices should be protected with appropriate controls.
- The necessary guidelines shall be followed while handling a mobile device in accordance with the Acceptable Usage Policy.

7.8.17.2. Remote Working

- Remote work should only be allowed after approval from the Head of Department & CIO. Security measures should be defined and adopted to prevent unauthorized access to information processing facilities from untrusted networks. Refer: "VTxL-23.23-Access Control Procedure-V1.1, Section 6 – Remote Access Management"
- Remote access to information systems through mobile devices shall be granted based on business requirement and shall be restricted to authorized users.
- Appropriate authentication and authorization mechanisms should be implemented to provide access for mobile devices connecting to the internal network.
- Only authorized applications shall be accessed through mobile devices.

7.8.18. Data Masking

Where the protection of sensitive data (e.g., PII) is a concern, VTL should consider concealing such data by using techniques such as data masking, pseudonymization, or anonymization, as applicable and in line with legislative requirements.

7.8.19. Information / Data Deletion

- Data/ Information stored in information systems, devices or in any other storage media shall be deleted when no longer required. Refer: "VTxL-23.39-Information Security Data Retention Procedure_V1.1"
- When deleting data/information on systems, applications and services, the following should be considered:
  - selecting a deletion method (e.g., electronic overwriting or cryptographic erasure) in accordance with business requirements and taking into consideration relevant laws and regulations.
  - recording the results of deletion as evidence.
  - when using service vendors for information deletion, obtaining evidence of information deletion from them.
- Where third parties store VTL's information on its behalf, requirements of information deletion (As applicable) should be included in the third-party agreements and enforced during and upon termination of such services.

- Where cloud services are used, VTL should verify if the deletion method provided by the cloud service provider is acceptable, and if it is the case, VTL should use it, or request that the cloud service provider delete the information.

7.9. System Acquisition, Development and maintenance

7.9.1. Security Requirements of Information Systems

7.9.1.1. Information Security Requirements Analysis and Specifications

The Information Security related requirements shall be identified and included in the requirements for new or enhancements to existing information systems. (Refer: "*VTxL-23.21-Systems, Acquisition and Development Management Procedure-V1.1*")

7.9.1.2. Security Application Services on Public Networks

- Adequate controls shall be implemented to protect information involved in application services published over public networks (internet) from fraudulent activity, contract dispute and unauthorized disclosure and modification.
- To maintain the security of application services on public networks the following regulations must be maintained but not limited to:
  - All publicly available systems shall be tested against vulnerabilities, and it shall be ensured that the identified vulnerabilities are fixed prior to publishing any information in such systems.
  - The integrity of the information being made available on a publicly available system shall be protected to prevent unauthorized modification and the authorization process in line with adequate controls (such as key management, security controls etc.) shall be applied at critical endpoints.

7.9.1.3. Protecting Application Services Transactions

- Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or reply.
- A secure communication channel shall be set up between all parties involved for application services transactions to ensure that the transactions and parties remain confidential.

7.9.2. Security in Development and Support Processes

7.9.2.1. Secure Development Policy

Procedure shall be established to define rules for the development of software and systems and applied to developments within VTL and all software developed in-house that runs on production systems shall be developed according to secure coding guidelines.

7.9.2.2. System Change Control Procedures

- All changes to systems within the development of the life cycle shall be controlled using formal change control procedures.
- Documentation reflecting nature, approval, and performance of all significant changes to production servers and communications systems owned by VTL shall be prepared and approved before the change takes place in accordance with change management process.

7.9.2.3. Technical Review of Application after Operating Platform changes

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

7.9.2.4. Restriction on Changes to Software Packages

Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled.

7.9.2.5. Secure System Engineering Principles

Secure engineering techniques in development of applications shall be established, documented, maintained, and applied.

7.9.2.6. Secure Development Environment

- Organization shall establish and appropriately protect secure development environments for software development and integration efforts that cover the entire software development lifecycle.
- Production environments shall be separated from non-production environments to reduce the risks of unauthorized changes to the production systems.
- Transfer of information between the development, test and production environments shall be controlled.
- Migration of data to new/upgraded systems shall be managed and controlled to ensure integrity, confidentiality, completeness, consistency, and continuity.

7.9.2.7. Outsourced Development

VTL shall oversee and monitor all outsourced system development activities, as applicable. It shall be ensured that all necessary licensing agreements, code ownership, and intellectual property rights related to outsourced work, are properly established before work is commenced.

VTL remains accountable for compliance with applicable laws and verifying control efficiency. VTL also retains the right to audit the quality and accuracy of outsourced work. Additionally, evidence that adequate testing has been conducted to protect against known vulnerabilities shall be obtained from outsourced service provider.

7.9.2.8. System Security Testing

Testing of security functionality should be carried out during development such as input and output data validation to ensure data stored and processed is correct and appropriate.

7.9.2.9. System Acceptance Testing

- Acceptance criteria for new information systems, upgrades and new versions shall be established, and suitable tests of the system shall be carried out prior to acceptance.
- Application security testing and system vulnerability assessment (VA) should be carried out for new information systems, upgrades and new versions in application services published over public networks (internet) and all major findings should be closed prior to go live.
- VA for all existing applications & infra should be done at least annually.
- Risk of deviation of not conducting VA or not closing major findings as stated above should be accepted and approved by the CIO

7.9.2.10. Test Data

- Test data shall be sanitized before being used for test purposes. It shall be always ensured that 'Confidential' information is not utilized during testing.

7.10. Third Party Risk Management

7.10.1. Information Security in Third Party Relationships

7.10.1.1. Information Security for Third Party Relationships

- Information Security requirements for mitigating the risks associated with third party's access to organization's information or information processing facilities shall be agreed with the vendor and documented in the form of agreements or contracts. Refer: ("*VTxL-23.20-Third-Party Risk Management procedure-V1.1*")
- VTL shall identify the critical vendors based on confidential, integrity and availability of the services associated with the third party.

7.10.1.2. Addressing Security within Vendor Agreements

All agreements with third parties shall have a defined Service Level Agreement (SLA), as applicable and include the following clauses (including but not limited to):

- Confidentiality / non-disclosure of information
- Sub-contracting
- Roles and responsibilities
- Termination
- Right to inspect/ audit by organization or its authorized auditors, Law enforcement agencies and regulating agencies including applicable regulations
- ESCROW Agreement as applicable.

- Data return/ destruction.

7.10.1.3. Managing Information Security in ICT Supply Chain

- VTL shall maintain security in line with Confidentiality, Integrity, and Availability for its ICT systems.
- Agreement with vendors shall include requirements to address the Information Security risks associated with information and information processing facilities and product supply chain.
- A Continuity strategy should be developed for ICT systems.
- Periodic risk assessments or security assessments shall be performed to ensure the risks are treated appropriately.

7.10.2. Third Party Service Delivery Management

7.10.2.1. Monitoring and Review of Third-Party Services

Periodic assessment for critical third parties shall be carried out and risks shall be managed appropriately.

7.10.2.2. Managing Changes to Third Party Services

Significant changes to third party services (e.g., enhancement to networks, new technologies, new products, or newer versions, change of vendors, change of physical location etc.) shall be informed to the Information Security team.

7.11. Information Security Incident Management

7.11.1. Management of Information Security Incident

7.11.1.1. Responsibilities and Procedures

- Procedures for monitoring, detecting, reporting, classifying, and responding to security events and incidents shall be defined and implemented. Refer: VTxL-23.14-Incident Management Procedure-V1.1"
- Management responsibilities shall be assigned to ensure a quick, effective, and orderly response to Information Security incidents.

7.11.1.2. Preparation of Cyber Security Incident

VTL shall plan and prepare to safeguard from potential cybersecurity incidents by means including but not limited to:

- conducting periodic cyber security assessments
- conducting annual review of Incident Response framework
- establishing incident response playbooks
- training staff on incident response protocols

7.11.1.3. Detection and reporting of Security events and weaknesses

- Information Security events/alerts should be detected through various security monitoring mechanisms.
- Automatic monitoring of systems, alerts, and vulnerabilities shall be used to detect Information Security events in addition to reporting incidents.
- All employees/contractors should be made aware of their responsibility to report the incident as soon as possible. They should also be aware of the process and procedure to report the security incident.
- End users shall report any observed security events or weaknesses in information systems and services through appropriate reporting channels.

7.11.1.4. Detection of Information and Cyber Security incidents

- A centralized monitoring system with the ability to collate and analyze logs shall be implemented.
- Mechanisms for continuous monitoring and detection of advanced threats shall be implemented.
- Information Security events shall be assessed, and it shall be decided if they are to be classified as information and cyber security incident as per "*VTxL_ Incident Management Procedure_V1.1"*

7.11.1.5. Response to Information and Cyber Security Incidents

- Information and cyber security incidents shall be responded to in accordance with the documented procedures.
- In case of an incident the first response shall be to establish the normal security level and then initiate necessary control or recovery.
- The overall response to reported incidents shall include identification of corrective action(s).
- VTL shall establish protocols for communicating about the incident, both within VTL and with external stakeholders, such as partners, vendors, and regulatory bodies.

7.11.1.6. Learning from Information and Cyber Security Incidents

- The review and result of the resolution of the incident should be monitored and saved properly.
- Learnings from security incidents shall be documented and communicated to stakeholders. This information shall be used in improving the processes and systems to reduce the recurrence and/or future impact of a similar security incident.
- Resolution of previously occurred incidents shall be made available to all the incident response team members to make use of known errors and workarounds in restoring normal service to the business.
- All-in-scope personnel shall be made aware of the procedures to ensure they are mindful of Information Security threats and concerns encountered in the course of their normal work at VTL.

7.11.1.7. Collection of Evidence

- VTL shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence for security incidents.

- Evidence and logs shall be collected and maintained to comply with legal and regulatory requirements as deemed necessary.
- Evidence shall be protected from unauthorized access and from modification or damage. Transfers or copies of evidence should be approved and witnessed.
- Evidence along with a chain of custody shall be provided in case of involvement of the external cyber forensics team.

7.12. Information Security Aspects of Business Continuity Management

7.12.1. Information Security Continuity

7.12.1.1. Planning Information Security Continuity

VTL shall determine its requirements for Information Security and the continuity of Information Security management in adverse situations, e.g., during a crisis or disaster. Refer: VTxL-23.16-Information Security Aspects of Business Continuity Procedure-V1.1"

7.12.1.2. Implementing Information Security in Business Continuity Management

- Impact to IT and network infrastructure, shall be mitigated through resiliency at design stage, ongoing architectural reviews, identification of single points of failures, identification of mitigating controls and their costs and implementation of business approved controls to minimize/mitigate such single points of failure.
- Impact to IT application, shall be mitigated through identifying business critical applications, identifying their Maximum Time to Recovery (MTR), Recovery Time Objective (RTO) and Recovery Point Objective (RPO), sign off from the business on these MTR and RPO values and implementation of DR solution to meet business needs.
- The DR along with Disaster Recovery (DR) processes should be implemented in such a way, to provide the product/service/application to the business within signed off MTR, RTO and RPO, which includes the time for invocation of disaster. The DR solution shall ensure the confidentiality, integrity and availability of information remains intact.
- VTL shall develop recovery strategies for critical business processes to minimize the period of disruption and limit the impacts that such disruptions may have on delivery of key products and services, mitigate risks on account of people safety issues, site safety, business process disruption, technology, and network disruptions. Recovery Strategies for IT and network infrastructure should ensure that points of failure within the infrastructure are mitigated, and disruption risks are either eliminated or reduced to the bare minimum.

7.12.2. Verify, Review, Evaluate information Security in Business Continuity Management

- VTL shall verify the established and implemented Information Security continuity controls at regular intervals to ensure that they are valid and effective during adverse situations.

- IT continuity plans should be tested and updated annually to ensure that they are up to date and effective.
- Emergency contact information shall be validated and revised on an annual basis.
- The roles and responsibilities for both information systems contingency planning and information systems recovery shall be reviewed and updated annually.

7.12.3. Business Continuity for Information and Communication Technology (ICT)

- Readiness for ICT systems shall be planned, implemented, maintained, and tested in line with organization's business continuity requirements.
- Business impact analysis should be done to identify ICT continuity requirements and resources needed for ensuring continuity shall be identified.
- ICT continuity strategies and plans should be developed, implemented, and tested to meet the required availability level of ICT services and in the required time frames following interruption to, or failure of, critical processes.

7.12.4. Redundancies

7.12.4.1. Availability of Information Processing facilities

Infrastructure components, systems and information processing facilities shall be identified as per business requirements and redundancy shall be established to prevent single point of failure.

Refer: *VTxL-23.16-Information Security Aspects of Business Continuity procedure-V1.1*

7.13. Cloud Security

7.13.1. Cloud Security Guidelines

- VTL shall ensure that cloud security controls are implemented in alignment with security best practices (as applicable).
- Access to cloud environments shall be restricted to authorized personnel, with robust identity verification measures, including multi-factor authentication.
- Sensitive data stored or transmitted in the cloud shall be encrypted to protect its confidentiality and integrity.
- Cloud service providers shall be carefully selected and regularly assessed to verify compliance with VTL's security requirements.
- Continuous monitoring and logging of cloud activities shall be in place to detect and respond to security incidents promptly.
- Data in the cloud shall be backed up at defined intervals.
- Compliance with applicable data protection regulations shall be enforced, and cloud environments shall be configured according to established security baselines.

- For detailed guidance on implementing cloud security controls, Refer "*VTxL-23.27-Cloud Security Guidelines-V1.1*".

7.14. Information Security Assurance

7.14.1. Compliance with legal and Contractual requirements

7.14.1.1. Identification of Applicable legislation and Contractual requirements

- All relevant statutory, regulatory, and contractual requirements related to security should be identified and kept up to date; and the approach to meeting these requirements shall be documented.
- Compliance with statutory, regulatory, and contractual requirements such as guidelines / recommendation by applicable regulations, Information Technology (IT) act and other directives shall be ensured.

7.14.1.2. Intellectual Property rights (IPR)

- Software used must be acquired from legitimate (known and reputable sources) to ensure copyright is not violated.
- Proof and evidence of ownership of licenses, master disks, manuals etc. shall be maintained.
- Compliance with terms/ conditions and license requirements for the usage of copyright software(s) or any other proprietary information/ material shall be ensured.
- Controls shall be implemented to ensure the maximum number of users permitted to use the software is not exceeded.
- Only authorized software and licensed products shall be installed and
- Copying, storage, duplicating, converting to another format, extracting of electronic content (eBooks, media files, articles, reports etc.) must not violate copyright laws.

7.14.2. Protection of Records

- Important records required for meeting statutory and regulatory requirements shall be identified and their retention periods shall be defined and
- Records shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

7.14.3. Privacy and Protection of personally identifiable information

Data protection and privacy shall be ensured as required in relevant legislations, regulations, and, if applicable, contractual clauses for each business. Refer: "11.03-Privacy and Data Protection Policy"

7.14.4. Regulation of Cryptographic Controls

Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations. Refer: "*VTxL-23.12-Cryptography Procedure-V1.1*".

7.14.5. Information Security Review

7.14.5.1. Independent review of Information Security

- VTL's approach to managing Information Security and its implementation shall be reviewed independently at planned intervals and findings shall be reported to appropriate authorities.
- Audits of operational Information Systems shall be planned and performed at periodic intervals with the agreement of the Information Systems' owner to minimize the risk of disruption to business processes.

7.14.5.2. Compliance with Security policies and Standards

- Continued compliance with VTL's Information Security policies and procedures shall be maintained.
- Any detected non-compliance with the Information Security policies shall be investigated and corrective action shall be taken and reviewed and
- Such non-compliances as well as their preventive actions shall be further reported at the time of independent reviews.

7.14.5.3. Technical Compliance review

- Compliance with VTL information systems with technical security standards shall be maintained. Security control measures shall be regularly reviewed to ensure continued compliance and
- In case of any non-compliance, a root-cause analysis shall be performed to ascertain the reasons and possible preventive actions for the future.

7.14.5.4. Information and Cyber Security Measurements and preparedness Indicators

- The adequacy of and adherence to cyber security requirements should be assessed and measured through development of indicators to assess the level of risk/preparedness.
- VTL shall define key metrics to evaluate the performance, and the effectiveness of the Information Security controls.

8. Annexure

8.1. Definition and Abbreviations

8.1.1. Definition

Terms	Definitions
Acceptable Use	Acceptable use is a set of rules applied by the owner, creator or administrator of a network, website, or service, that restrict the ways in which the network, website or system may be used and sets guidelines as to how it should be used
Encryption	Encryption is the process of converting information into a code using a secret key, readable to individuals having decryption key
Backup	A backup is a copy of one or more files created as an alternate in case the original data is lost or becomes unusable
Cyber Security Incident	A cyber security incident is an adverse event in an information system and/or a network that poses a threat to computer or network security in respect of availability, integrity, and confidentiality
Mobile Device Management	Mobile device management (MDM) is a type of security software used to monitor, manage, and secure employees' mobile devices
Threat	The potential for a specific vulnerability to be exercised either intentionally or accidentally
Affiliate	Affiliate means with respect to any person, any entity that directly or indirectly through one or more intermediaries Controls or is Controlled by such person or is under direct or indirect common Control with such person
Vendor	Vendor means a third-party provider of goods or services.

Removable Media	Removable media refers to any type of storage device that can be easily removed from a computer or other electronic device, such as USB flash drives, external hard drives, memory cards, and optical disks. These devices are used for storing and transferring data between different systems or for backup purposes.
Asset	Any Logical or Physical entity storing, processing, or transmitting information perform the act.
Retention Period	It is the amount of time in which a given set of data will remain available for restore
Authentication	The process to verify that someone is who they claim to be when they try to access a computer or online service
Firewall	Hardware or software designed to prevent unauthorized access to a computer or network from another computer or network
Server	Computer that provides data or services to other computers over a network
Control or controlled	Control or Controlled means in respect of an entity, the ability (whether it is legally enforceable or not) to control, whether directly or indirectly, the composition of the board of directors (or other governing body) of that entity, the voting rights of the majority of voting securities of the entity, or the management of the affairs of that entity
Accountability	A security principle indicating that individuals shall be able to be identified and be held responsible for their actions
Information assets	Assets are economic resources. It is anything tangible or intangible that is capable of being owned or controlled to produce value and that is held to have positive economic value. The form of this type of asset can be software, hardware,

	information, communication systems, people, dataset, printed documents, etc.
Cyber Security	Cybersecurity, as per ISMS (Information Security Management System), refers to the protection of information assets and systems from unauthorized access, use, disclosure, disruption, modification, or destruction, ensuring confidentiality, integrity, and availability. It encompasses measures, processes, and practices designed to safeguard digital resources against cyber threats and vulnerabilities.
Screening	A process to verify facts about individuals related to their identity, professional credentials, previous employment, education, and skills
Confidentiality	Confidentiality refers to the principle that ensures that information is accessible only to authorized individuals, entities, or processes. It involves protecting sensitive data from unauthorized access, disclosure, or exposure, thereby maintaining its secrecy and privacy. Measures such as encryption, access controls, and data classification are implemented to enforce confidentiality and prevent unauthorized parties from gaining access to sensitive information.
Risk appetite	Risk appetite is the level of risk that an organization is prepared to accept in pursuit of its objectives before action is deemed necessary to reduce the risk.
Risk management	Risk management is the coordinated activities to direct and control VTL with regards to risk
Risk assessment	Risk assessment is the overall process of risk analysis (systematic use of information to identify sources and to estimate the risk) and risk evaluation (process of comparing the estimated risk against given risk criteria to determine the significance of risk)

Risk treatment plan	Risk treatment plan is a uniform template to keep a record of relevant Risk information about identified Risks.
Risk Register (RR)	It is a uniform template to keep record of relevant Risk information about identified Risks.
Residual Risk	The risk remaining after risk treatment
Data Leakage Prevention	DLP stands for Data Loss Prevention. It refers to a set of tools and techniques used to prevent the unauthorized transmission or leakage of sensitive or confidential data.
Segregation of Duties	A control mechanism whereby a process is broken into its constituent components and the responsibility for executing each component is divided among different individuals. Segregation of duties segments the process so that no individual has an excessive ability to execute transactions or unilaterally cover irregularities without detection
Access	The right or permission that is granted to an identity. These informational access rights can be granted to allow users to perform transactional functions at various levels
Perimeter	Boundary of offices and facilities of VTL
Information System	All devices and equipment used in processing or storage of information. For example, computer devices, servers, telephones, CCTV, etc.
CCTV	Closed Circuit Television system used for surveillance and monitoring
Drills	Tests to ensure that evacuation plan works as designed in case of any emergency
Allocation	Allocation refers to issuance of devices to a particular induvial.
Vendor Agreement	Vendor Agreement means any written agreement signed by VTL pursuant to the terms of which a vendor is to supply goods or services to VTL

8.1.2. Abbreviations

Abbreviations	Descriptions
IT	Information Technology
USB	Universal Serial Bus
PII	Personally Identifiable Information
RPO	Recovery Point Objective
RTO	Recovery Time Objective
ISO	International Organization for Standardization
SIEM	Security Information and Event Management
OEM	Original Equipment Manufacturer
IDS	Intrusion Detection Centre
NDA	Non-disclosure agreements
DR	Disaster Recovery
MTR	Maximum Time to Recovery
LAN	Local Area Network
UPS	Uninterruptible Power Supply
CCTV	Closed Circuit Television
NCCA	Non-Conformity and Corrective Action
ISC	Information Security Coordinator
SPOCs	Single Point of Contact(s)
IRT	Incident Response Team
KPA	Key Performance Area

8.2. References

Sr. No.	Document Name
1.	*VTxL-23.05-Acceptable Policy-V1.1*

2.	*VTxL-23.06-Information Security Risk Management Procedure-V1.1*
3.	*VTxL-23.10-Communications Security Procedure-V1.1*
4.	*VTxL-23.11-Compliance Management Procedure-V1.1*
5.	*VTxL-23.12-Cryptography Procedure-V1.1*
6.	*VTxL-23.13-Human Resources Security Procedure-V1.1*
7.	*VTxL-23.14-Incident Management Procedure-V1.1*
8.	*VTxL-23.15-Information Security Training Procedure-V1.1*
9.	*VTxL-23.16-Infosec Aspects of BCM Procedure-V1.1*
10.	*VTxL-23.17-Mobile Device Management Procedure-V1.1*
11.	*VTxL-23.18-Operations Procedure-V1.1*
12.	*VTxL-23.19-Removable Media Mgmt. Procedure-V1.1*
13.	*VTxL-23.20-Third Party Risk Management Procedure-V1.1*
14.	*VTxL-23.21-System Acquisition Development and Maintenance Procedure-V1.1*
15.	*VTxL-23.22-Vulnerability & Patch Management Procedure-V1.1*
16.	*VTxL-23.23-Access Control Procedure-V1.1*
17.	*VTxL-23.24-Physical & Env Security Procedure-V1.1*
18.	*VTxL-23.25-Asset Management Procedure-V1.1*
19.	*VTxL-23.26-Information Classification Guidelines-V1.1*
20.	*VTxL-23.27-Cloud Security Guidelines-V1.1*
21.	*VTxL-23.28-Procedure for Control of Documented Information -V1.2*
22.	*11.03-Privacy and Data Protection Policy-V1.1*

8.3. Document Change Control

All amendments and updates to this document must be initiated and formally routed through the Business Process Management Cell. This unit is responsible for reviewing, validating, and approving any changes to ensure alignment with organizational governance standards.

8.4. Signature

Description	Author	Reviewer	Approver
Name	Information Security Head	CIO	EVP – Chairman Office, HR & IT
Date	21-09-2026	21-09-2026	21-09-2026