



THE SUPREME INDUSTRIES LIMITED (TSIL)

INFORMATION TECHNOLOGY & SECURITY POLICY

POLICY OWNERSHIP

Name of the Policy	Information Technology & Security Policy
Approval Date	
Approving Authority	Board of Directors
Effective from	
Version	V 2.0
Review Frequency	Yearly

VERSION CONTROL

Version No.	Issue Date	Revision Description	Approved by
2.0	05-09-2025	New IT & Security Policy will govern risk management, access control, incident response, compliance, and security-specific controls.	Board

DOCUMENT DISTRIBUTION

Primary Recipient

- Chief Information Officer
- Head of IT Infrastructure
- Application owner
- Members of IT team
- Members of IS team

Document Confidentiality

This document is confidential and intended only for internal use by The Supreme Industries Limited (TSIL). Primary recipients may circulate this document to Controllers, Heads of Departments, under their control for implementation. The recipient should ensure that this document is not reproduced or circulated to external entities without prior approval of the document owner or the primary recipients of this document.

Table of Contents

Contents

POLICY FRAMEWORK	7
Introduction	7
Purpose	7
Objectives	8
Scope.....	8
Standards & Procedures	8
Responsibilities	8
Compliance	9
Exceptions	9
Review.....	9
Organization Chart.....	10
INFORMATION TECHNOLOGY & SECURITY POLICY	11
RISK MANAGEMENT.....	11
ORGANISATION OF INFORMATION TECHNOLOGY & SECURITY	11
Roles and Responsibilities.....	11
IT Investments.....	11
IT Strategy	11
ASSET MANAGEMENT	12
Control of Assets & Ownership.....	12
Inventory of IT Assets.....	12
Information Classification	12
Business-Critical information Notification	12
PERSONNEL SECURITY	13
Background Checks	13
Confidentiality/Non-Disclosure Agreements	13
User Training and Awareness	13
Disciplinary Procedure	13
Termination of Employment.....	13
PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS	14
Physical Security and environmental controls.....	14

Data Center Management	14
Telecommunication, Support and Power utilities	14
Equipment Security.....	15
Removal of information assets	15
Secure disposal of retired IT hardware and equipment	15
ACCESS CONTROL	15
Access to Information	15
User Access Management.....	16
Account lockout policy.....	16
Password Management	16
Third-party Access.....	16
Mobile Computing	16
OPERATIONS MANAGEMENT	17
Change Management.....	17
Change Plan.....	17
Changes in applications provided by application service provider.....	17
Capacity management and system acceptance.....	17
Configuration Management.....	18
Vulnerability Management	18
Electronic messaging (email)	18
Protection against Malicious (Anti-Virus)	19
Media handling	19
Separation of development, testing and production	19
Logging & Monitoring	19
INFORMATION SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE	20
Information Systems Acquisition	20
Software Development and Control	20
Cryptographic Controls	20
BACKUP & RECOVERY MANAGEMENT	21
Backup Management	21
Data Migration Controls.....	21
NETWORK MANAGEMENT	21
Network Management.....	21
Network Redundancy.....	21

Network Monitoring	22
INFORMATION SECURITY INCIDENT MANAGEMENT	22
Incident Reporting	22
Incident Management.....	22
BUSINESS CONTINUITY AND DISASTER RECOVERY	22
OUTSOURCING / THIRD PARTY MANAGEMENT	23
Outsourcing / Third Party Security.....	23
Monitoring and Review of Third-party services.....	23
Managing Changes to Third Party Services.....	24
AUDIT & COMPLIANCE	24
Audit & Compliance	24
Audit Trail.....	24
E-WASTE MANAGEMENT	24
ACCEPTABLE USAGE.....	25
IT Strategy Committee (ITSC)	26

POLICY FRAMEWORK

Introduction

The Supreme Industries Limited (TSIL) has implemented Information Technology in its business processes for smooth functioning of the daily operations and provide seamless services to its customers. TSIL is progressively becoming more dependent upon information systems for both routine business operations and the development and delivery of new products and services. It is therefore essential for the continued successful operation of TSIL that the availability, integrity and confidentiality of its information systems and associated data are maintained, in a cost-effective manner i.e. IT resources are available & managed efficiently and at a level that is appropriate to its business.

Consequently, access to, confidence in, and reliability of information is integral to TSIL's business processes and critical to the success of TSIL's mission. The need for such protection arises because information systems are potentially vulnerable to two main categories of unwanted events, or threats. These are accidental threats (human error/equipment failure/ natural hazards) and deliberate or malicious threats (fraud/sabotage/vandalism/theft). There is also the threat of legal action if information systems are misused, which TSIL and its employees should be aware of.

TSIL's Information Technology Service Management Policy is aimed at enhancement of its ability to collect, store, process and transmit information electronically & focuses on the overall management and use of IT resources. Information and information systems which are vital assets to TSIL in the pursuit of its business objectives, and it is important that information is managed regarding:

- Confidentiality – Ensuring access to information to authorized users only.
- Integrity – Ensuring accuracy and reliability of information by ensuring that there is no modification without authorization.
- Availability – ensuring that authorized users have access to information and associated assets when required.

TSIL must therefore ensure that IT resources are managed efficiently & appropriate levels of information security are maintained, to assure the confidentiality, integrity, and availability of TSIL's information systems always.

Purpose

The purpose of Information Technology and Security Policy is

- To enunciate management's commitment and directives for use & initiatives related to Information technology & Information Security.
- To govern the use, management, and implementation of IT resources within an organization.
- To establish a framework in TSIL for the development of Standards & Procedures for effective and efficient use of IT resources, Information Security, their implementation, and compliance.

Objectives

There are six main policy objectives:

- To ensure information and information systems are available to authorized users as per the business needs and information systems are used in an effective manner to promote TSIL's mission.
- To ensure that all TSIL's information assets including information, intellectual property and information systems are adequately and consistently protected from damage, inappropriate alteration, loss, and unauthorized use or access. The level of protection should be commensurate with the availability of information required by TSIL to conduct its business.
- To provide IT infrastructure to users & ensure proper allocation and use of IT resources.
- To maintain and enhance the performance and reliability of IT systems & develop an approach for adopting new technologies.
- To create within TSIL, a level of awareness of information technology & security as part of the day-to-day operations of TSIL and to ensure that all employees understand their responsibilities for usage of information technology.
- To create detailed information technology & security standards and procedures document based on this policy and ensure compliance against such standards and procedures.

Scope

This policy is applicable to:

- All IT supported business processes and IT operations.
- Information assets of TSIL.
- Employees of TSIL and third parties.

Standards & Procedures

The policies will be supported by Standards & Procedures as and when required, which detail the technology specific requirements and implementation process for complying with the policies. Such standards & Procedures will be implemented with the approval of ED / CIO.

Responsibilities

- The Board shall approve the policies and any subsequent modifications.
- The CIO is responsible for ensuring that policies are current, reflecting the requirements of TSIL and for ensuring development of underlying standards, procedures, and roles for managing security.
- Head of Compliance is responsible for disseminating the policies and ensuring compliance with the policies.
- The CIO and IT team are responsible for enforcing the policies across TSIL.
- The Compliance Department is responsible for conducting audits to check the level of compliance with the policies.
- All employees of TSIL have a responsibility to understand and comply with the policies.

Compliance

TSIL expects all employees to comply with the policies. Failure to comply with the policies will entail appropriate action which may include disciplinary action.

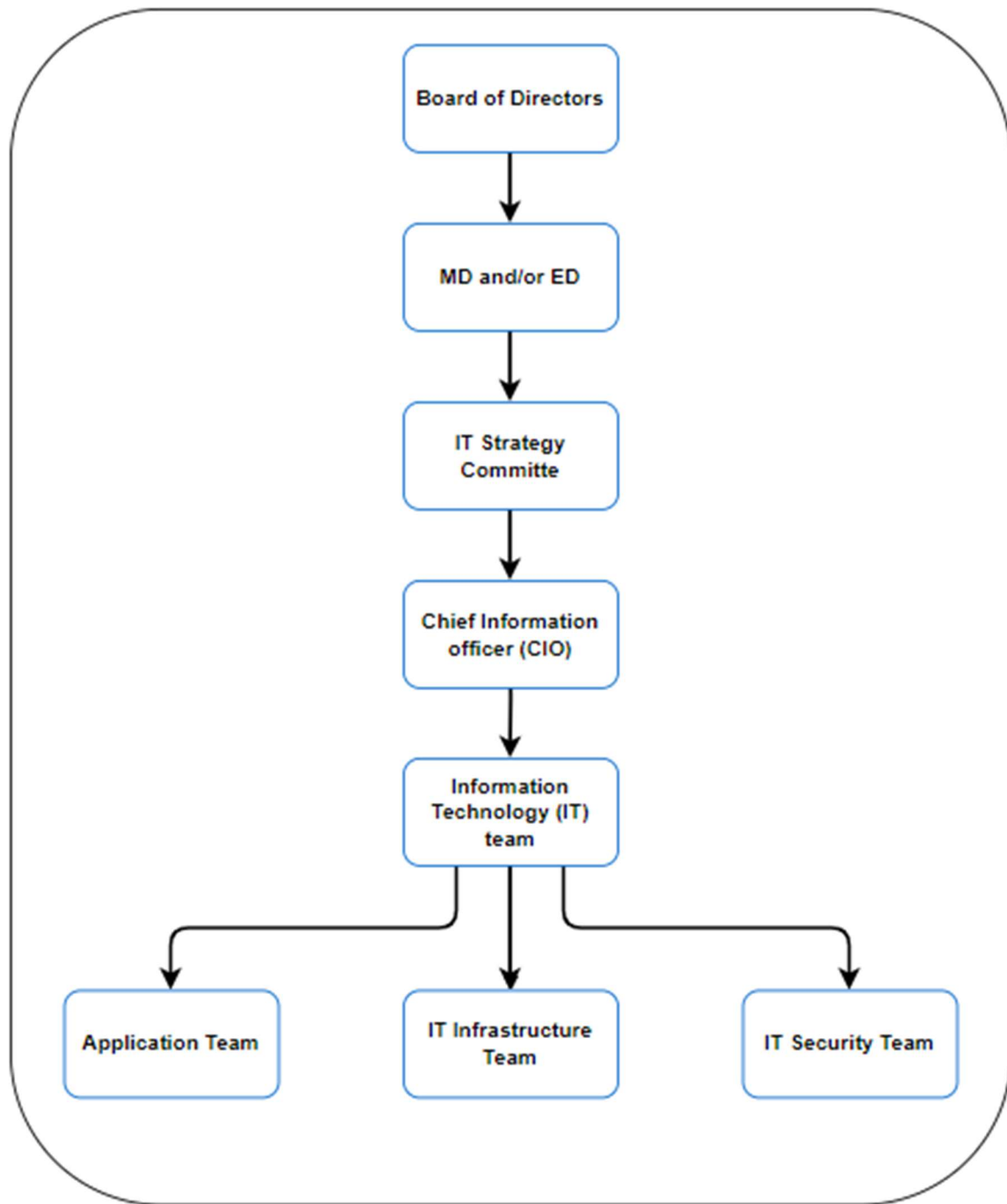
Exceptions

Approval for exceptions or deviations from the policies, wherever warranted, will be provided by the Head of IT with recommendation from CIO.

Review

The policies shall be reviewed and updated annually by the Board. The CIO and IT team will assist the Board in the review process and recommend necessary changes.

Organization Chart



INFORMATION TECHNOLOGY & SECURITY POLICY

RISK MANAGEMENT

- TSIL shall identify, analyze, and mitigate risks which affect confidentiality, integrity and availability of information assets and information systems.
- TSIL may conduct a risk assessment annually for any changes in information systems, including applications, servers, networks and any process or procedure by which the systems are administered and / or maintained.

ORGANISATION OF INFORMATION TECHNOLOGY & SECURITY

Roles and Responsibilities

- Implementation of Information technology & security policy requires active involvement of all personnel within TSIL. Roles and responsibilities of various functionaries for Information Technology should, therefore, be clearly defined, reviewed, and updated.
- While defining roles and responsibilities, segregation of duties and the principle of least privilege should be employed, where applicable, so that incompatible roles are not assigned to the same individual.

IT Investments

- A formal budgeting process needs to be established and maintained to manage IT-related investment.
- The IT team shall prepare an annual IT budget based on the IT plans and shall submit it to management for review and approval.
- Approval for out of budget investment shall be taken from management as an exception.
- The IT leadership shall also monitor the actual budget spent against the planned budget.

IT Strategy

- IT Strategic planning aims at effectively managing & aligning the IT resources with TSIL's business strategy and priorities.
- IT team to develop a short-term plan for up to one year and a long-term plan for up to five years, incorporating technological upgrades and input from stakeholders. These plans will be presented to IT Committee & board for review and approval.
- Ensure that long-term IT plans are translated into actionable short-term plans to support organizational goals effectively.
- Allocate responsibilities and appropriate resources to ensure the successful implementation of IT plans.
- Communicate IT plans to business owners and relevant stakeholders as necessary to ensure

alignment and support.

- Monitor and evaluate the progress of IT plans on a quarterly basis. Report observations to IT committee and stakeholders.

ASSET MANAGEMENT

Control of Assets & Ownership

- Ownership of each asset should be assigned to a designated official / Department who will be the Asset Owner. Asset owners are responsible for maintaining the confidentiality, integrity and availability of the assets assigned to them.

Inventory of IT Assets

- A detailed inventory of all Assets relating to IT operations shall be maintained by the IT department including End of life or End of Support date, details of annual maintenance contract / subscription (AMC).
- An inventory of all software licenses shall be maintained and updated in the centralized database along with the expiry date.
- IT inventory should be labelled with corresponding application name, if any.
- The IT inventory should be reviewed periodically.
- Assets should be disposed of as per E-Waste Management Policy.

Information Classification

- All digital data generated, stored, and transferred should be classified in accordance with an approved classification scheme. The classification should be based on value, sensitivity, and criticality, as well as applicable statutory, regulatory, and legal requirements.
- Information should be labelled as per classification. The level of protection should be commensurate with the security classification of the information.

Business-Critical information Notification

- To ensure appropriate security controls are applied, all departments must proactively inform the IT team about any business-critical data they manage or generate. This includes data that is essential for operational continuity, regulatory compliance, financial reporting, or strategic decision-making. Timely notification will enable IT to assess risks and implement adequate protection measures such as access controls, encryption, backup, and monitoring.

PERSONNEL SECURITY

Background Checks

- All potential new employees and employees of a third party must be subjected to background checks.
- The procedures should be in conformity with relevant laws, regulations, and ethics. The background check related checks will be performed by TSIL's HR function.

Confidentiality/Non-Disclosure Agreements

- All employees (including temporary employees) and third-party users must sign a confidentiality or nondisclosure agreement prior to receiving physical or logical access to secure areas, IT Assets or any confidential or internal information.

User Training and Awareness

- All users of information assets should be suitably briefed on the Acceptable Usage Policy & TSIL may add a clause in the standard template of the employment contract employment offer letter on the acceptable use of IT assets of TSIL.
- TSIL may ensure that the security training sessions are provided to all new Joines at the time of induction about information and data security and their role to report any breaches immediately to their reporting manager and the IT team.
- Training in information security may also be imparted as refresher training to the existing employees at regular intervals.
- The training material related to information security and information technology may be periodically reviewed by IT team.
- Essential procedures to be followed in secure areas should be displayed in a prominent location.

Disciplinary Procedure

- Employees must perform their security responsibilities and comply with the requirements specified in the security policies with due diligence. Security violations may attract disciplinary and/or legal action.

Termination of Employment

- Users of information systems should return all IT assets in their possession upon termination of their employment, contract, or agreement.
- The access rights of users of information systems should be revoked upon termination of their employment, contract, or agreement.

PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS

Physical Security and environmental controls

- All sites, which contain information and information processing facilities, should be protected from unauthorized physical access, damage, interference, and environmental threats such as damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster.
- Access will be provided at TSIL's premises on a need-to-use basis.
- All physical access and movement of information assets should be controlled, monitored, and reviewed.
- TSIL may review visitor logs on a periodic basis. Employees on long leave may be given restricted access to the system during their leave duration as authorized by CIO.

Data Center Management

- All critical IT processing facilities should be housed in a highly secure environment such as a Data Centre / Server room.
- The Data Centre / Server Room should have physical and logical protection for the information assets housed within it.
- The Head of IT should have the right to access the server room as and when needed, in case of any incident. Access by other employees should be logged in a register.
- The IT team should maintain a register for visitors' access to data center / server room & such logs should be reviewed on a periodic basis.
- Secure processes must be followed for hardware deployment, administration, and monitoring within the Data Centre.
- The Data Center / Server room with critical assets shall not be in the basement or the highest floor of the building.
- Smoking, eating, and drinking shall be prohibited in the data center / server room and other restricted areas. Appropriate signboards shall be displayed at all entry points.
- A contact list of essential resources and services shall be prepared and maintained up-to-date. The list shall be posted in clear view at the critical facilities. The list shall include the critical staff and support team members, Local police, Local fire department, Local hospital / emergency medical facility, Local electric, water, telephone emergency services
- A network and electrical diagram shall be maintained.
- All assets / cables shall be clearly marked / tagged.
- Asset movement register shall be maintained at the Data Center / Server Room
- Appropriate Annual maintenance contracts and preventive maintenance reports should be kept on record.

Telecommunication, Support and Power utilities

- Appropriate Uninterrupted Power Supplies (UPS) and power-conditioning equipment shall be implemented and maintained.
- Critical electronic equipment shall not be connected to raw power supply.

- Lightning protection shall be applied to all buildings and lightning protection filters shall be fitted to all incoming power and preferably all communication lines also.
- Power and telecommunication cables shall be separately laid with adequate protection against interception or damage.
- Wherever possible telecommunication cables shall be protected by using a conduit in public areas.
- All cables shall be clearly marked / tagged.
- Network cabling shall be structured, wherever possible.

Equipment Security

- All IT equipment including power and telecommunication cables should be protected against unauthorized access and environmental threats to prevent loss, damage, theft or compromise of assets and interruptions to activities.
- Users should ensure that unattended equipment has appropriate protection. This should be system enforced.

Removal of information assets

- Equipment, information, or software should not be taken off-site without prior authorization.

Secure disposal of retired IT hardware and equipment

- IT hardware and equipment shall be disposed of only after approval.
- Appropriate data and media destruction should be performed prior to disposal.
- Disposal of retired hardware and media should comply with prevalent environmental regulations.

ACCESS CONTROL

Access to Information

- All access to information and information systems shall be provided after due process of identification, authentication, and authorization.
- Authorization shall be granted on establishment of business needs and the principles of 'least privilege.'
- Controls should be implemented as necessary at the hardware, operating system, network, database, and application levels.
- All users of information and information systems shall be uniquely identified.
- Access control matrix for access to critical applications shall be defined.

User Access Management

- Access to information and information systems should be regulated using unique User IDs.
- The allocation and use of privileges should be restricted and controlled.
- Users' access to information assets should be reviewed at regular intervals to ensure they are maintained in line with business requirements and dormant accounts which are no longer required should be disabled.
- Formal Procedures for User management should be documented and communicated.
- Privileged user access shall be reviewed on half yearly basis.

Account lockout policy

- Any user account shall be locked after a maximum of five repeated failed attempts. The affected user shall submit a formal request for resetting the locked User ID.

Password Management

- The system should enforce complex passwords and force changes after a defined period. Password expiry should be set for a period of 90 days.
- First-time and reset passwords should be communicated to users through a secure process followed by a forced password change on logon.
- Where complex passwords cannot be enforced by the system, appropriate compensating controls should be ensured.
- Password complexity can be set / defined.
- Passwords should be encrypted when transmitted across any network.
- Multifactor authentication may be implemented for critical applications and administrators.

Third-party Access

- Access by third parties to any Information Asset should be strictly restricted and controlled. Third party access risks should be assessed, and appropriate controls should be implemented.

Mobile Computing

- When using mobile computing and communication facilities, e.g. Notebooks, laptops, and mobile phones, appropriate controls should be implemented to protect against the security of risks arising out of mobile computing.

OPERATIONS MANAGEMENT

Change Management

- Changes to IT assets (including applications, servers, systems software, and network devices) should be performed in a controlled manner to ensure that the risks associated with such changes are managed to an acceptable level.
- Changes should be tested in a non-production environment before deployment and ineffective changes should be rolled-back.

Change Plan

- Manager IT shall identify the personnel who shall undertake the development of the change.
- The change Owner shall identify personnel from the User group to carry out the User Acceptance Tests (UATs). The UATs shall be conducted using carefully selected data, which shall be protected and controlled.
- The Owner shall submit the Change Request Documentation to the In-charge of Information Technology to carry out the change
- The In-charge of Information Technology shall be responsible for introducing the change and maintaining all relevant documentation pertaining to the changes to the information assets.

Changes in applications provided by application service provider

- TSIL should have a well-defined Service Level Agreement with application service provider that specify security controls, service levels and liability of Service Providers for violation of SLAs.
- TSIL shall obtain an integrity certificate / STQC or a written confirmation from the application developer or vendor stating that the application is free of known vulnerabilities / malware in the code. Such a certificate or a written confirmation shall also be obtained whenever material changes to the code, including upgrades, occur.
- TSIL shall obtain VAPT report from the vendor for such application.

Capacity management and system acceptance

- The initial requirements of critical infrastructure resources (including data center / server capacity) should be assessed and planned to ensure that the current and future business requirements can be met.
- The use of resources should be monitored and analyzed annually to ensure optimal performance and availability of systems.
- IT capacity planning across components, services, system resources, supporting infrastructure is consistent with past trends (peak usage), the current business requirements and projected future needs as per the IT strategy of TSIL.
- The assessment of IT capacity requirements and measures taken to address the issues shall be reviewed by ITC.

Configuration Management

- Standard Secure Configuration for providing high security, reliability and availability of systems deployed in TSIL should be developed and documented.
- Systems should be configured, as per applicable Secure Configuration Document (SCD).

Vulnerability Management

- Timely information about technical vulnerabilities of information systems deployed by TSIL should be obtained, TSIL's exposure to such vulnerabilities should be evaluated, and appropriate measures including application of patches should be taken to address the associated risk.
- Regular upgrades and patches must be applied to resolve software bugs and to ensure up-to-date versions of software.
- Upgrades and patches applied must be verified, tested, and authorized before they are used in the production environment.
- Systematic vulnerability assessment and penetration testing activities must be conducted by IT team for critical infrastructure to ensure technical vulnerabilities are recorded across TSIL's information systems and appropriately addressed. External consultants may be employed for such activities, and the program must be followed-up to ensure compliance.

Electronic messaging (email)

- Email applications should be protected against risks of unauthorised access, malicious code, spam. Email servers should be managed to ensure high availability.
- All official email messages and logs should be retained as per legal and regulatory requirements.
- Electronic mail access shall be assigned by the IT team only after obtaining a request from respective HR team.
- Each user shall be responsible for any activity performed through his / her electronic mail ID
- Size of Email box shall be defined by the IT team
- Attachment size restrictions shall be configured in email as per the user requirements.
- All incoming electronic mail shall be scanned for viruses as per TSIL's Malicious and Mobile Code (Anti-virus) management policy.
- Password policy should enforce a minimum of 8 characters for email accounts, disallow password reuse, and require password reset every 90 days.
- Two-factor authentication should be enabled for all the email accounts.
- Email accounts of employees who have departed the organization may remain active for up to two months following their last working day. Any extensions beyond this period should require prior approval from the respective HODs. The IT team must reset the email password on the employee's last working day.

Protection against Malicious (Anti-Virus)

- All servers, desktops, workstations, gateways, and any other access points to TSIL's network must be protected against malicious code.
- Anti-virus application and processes must ensure early detection, efficient containment, and eradication of malicious code. Adequate user awareness measures should be implemented for the same.
- The anti-virus and anti-malware software installed on all TSIL endpoints may be configured to scan all portable devices connected to them such as portable hard-drives, USB flash-drives, etc.
- Controls should be considered to prevent unauthorized mobile code execution.

Media handling

- All removable computer media (tapes or removable hard disks) should be protected from unauthorized disclosure, modification, removal, and destruction, with security measures commensurate with the information classification of the information held on the media.

Separation of development, testing and production

- Development, test, and production facilities and duties should be separated to reduce the risks of unauthorized changes to the production system.

Logging & Monitoring

- User activities, exceptions, and security events should be logged and monitored.
- The activities of users with high levels of access (privileged users such as system administrators and system operators) should be logged and independently reviewed on a regular basis.
- All access to critical applications and TSIL's network should be monitored for suspicious activities or security breaches. Adequate response mechanisms should be in place for containing security breaches.
- Application owner may ensure that the application is able to log the transactions and administrative actions, which are adequate to serve as a reference in case of any investigation for misuse of the application and/or debugging the errors in the application.
- The audit logs should be retained in accordance with below listed timelines:
- **Security & Access Logs:** Retain logs for **at least one year** for security purposes, with **critical logs** such as admin access, changes to critical systems, and incident logs retained for **three years**.
- **Financial and Transactional Logs:** These should be kept for **eight years**
- Logging facilities and log information should be protected against tampering and unauthorized access.

INFORMATION SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Information Systems Acquisition

- Procurement process for IT hardware, software and services should ensure that procurement is carried out on the best possible terms of business benefits, quality and cost in a transparent manner that makes economic and efficient use of TSIL's resources.
- Information security requirements in hardware, software and services being procured should be identified, and should be part of specifications provided during the procurement of assets.

Software Development and Control

- All software developed or customized for use by TSIL should follow a standard development process to ensure it meets functional, security and performance requirements.
- Adequate controls in the software development process should be built to address risks in meeting functional and security requirements of TSIL, in regulatory compliance, in timely completion and in meeting performance requirements.
- Appropriate controls for ensuring the confidentiality, authenticity and integrity of information passed between systems should be implemented.
- Access to program source code and other sensitive information should be restricted.
- Shadow IT - The use of unauthorized hardware, software, or cloud-based services, commonly referred to as Shadow IT, is strictly prohibited. All technology solutions must be requested, assessed, and approved by the HO IT committee to ensure compliance with organizational standards, data protection regulations, and security requirements. Employees must not bypass approval processes by installing or utilizing unapproved applications or devices. Any violations will be subject to review and may result in disciplinary action in accordance with company policy.

Cryptographic Controls

- Confidential information should be encrypted when stored in non-secure locations or transmitted over insecure networks. The type, strength and quality of encryption algorithm should be determined and implemented based on Risk Assessment and the corresponding level of protection required.
- All digital transmission of sensitive financial information (e.g. remittances, payment advice, etc.) should be digitally signed using digital certificates issued by a licensed Certifying Authority under a Public Key Infrastructure (PKI) or electronic signatures provided by approved providers of cryptographic support services.

BACKUP & RECOVERY MANAGEMENT

Backup Management

- All software and digital information essential to the continued operations of TSIL should be backed up and periodically tested for restoration.
- The security controls over the backup of information and media should correspond with the criticality of the information backed up.
- Backup should be retained in accordance with TSIL's Backup management standard.

Data Migration Controls

- Data migration policy shall be in place covering the systematic process for data migration, ensuring data integrity, completeness, and consistency.
- Proper sign offs from business users and application owners at each stage of migration should be obtained.

NETWORK MANAGEMENT

Network Management

- TSIL's internal network should be segregated from external networks.
- All connections to external networks (including Internet, networks of outsourced vendors) should be authorised and provided in a secure manner.
- All network devices in TSIL should be identified and documented.
- TSIL's network should be designed and maintained to meet the availability requirements of Information Owners and to provide for encryption of confidential and internal information
- Access Control Devices should be deployed to protect all critical resources on TSIL's network from both external and internal users.
- The devices should be configured and managed in such a manner that access to critical resources is allowed after due validation and restricted to authorized systems and services.
- All remote access to TSIL's network should be allowed based on business requirements. Remote access should be controlled by appropriate identification and authentication.

Network Redundancy

- Adequate redundancy should be built into the network links, critical network equipment's.
- Redundant links should have the same level of security as the primary links.

Network Monitoring

- The IT team, along with the third-party service provider, shall monitor all network resources, services, access, and their usage, as well as all traffic through the gateways for possible misuse and intrusions.
- **NOC (Network Operations Center):** The NOC, which is outsourced, will oversee the health and performance of the network infrastructure. This includes monitoring network uptime, managing incidents, troubleshooting issues, and ensuring optimal network performance.
- **SOC (Security Operations Center):** The SOC is responsible for monitoring security events across the organization's IT environment. This includes identifying and responding to security threats, analysing suspicious activities, and ensuring that all security incidents are handled in a timely and compliant manner. The SOC team shall also provide continuous threat intelligence and vulnerability assessments to enhance the overall security posture.

INFORMATION SECURITY INCIDENT MANAGEMENT

Incident Reporting

- All users of information systems including third parties must report any security breach or attempt to breach and security weakness in information systems, immediately, to the designated official / IT team. IT team will report all incidents to the CIO and Infra Head immediately.
- Authorized officials only will report Information security incidents to outside authorities, when such reporting is required to comply with legal, statutory, and regulatory requirements.

Incident Management

- TSIL should establish an incident management process, which includes incident detection, recording, response, and escalation procedure, to ensure quick, effective, and orderly response to security incidents.
- The details of the incidents are along with the date of the incident, incident description, incident root cause, preventive and corrective action taken may be maintained and preventive actions may be initiated.

BUSINESS CONTINUITY AND DISASTER RECOVERY

- Business Continuity and Disaster Recovery Plans should be developed to address threats to continuity of operations and information systems that are critical to TSIL's business.
- Recovery plan should be designed to meet the expected time of recovery and the level of availability. The plans should include information security requirements and appropriate safeguards to minimize the risk, duration, and cost of disruption to the business.
- Business Continuity and Disaster Recovery Plans should be implemented, tested periodically, and updated. Based on the business need and nature of changes undergone, a documented drill, or an actual test may be initiated of all business continuity plan/ disaster recovery plans will be

- conducted by the IT/ business team on an annual basis.
- Cyber Crisis management plan should be appropriately documented.

OUTSOURCING / THIRD PARTY MANAGEMENT

Outsourcing / Third Party Security

- The risks associated with outsourcing of IT services, software development and IT supported business processes to third parties should be assessed and managed at an acceptable level and adequate controls implemented.
- All outsourcing arrangements should have a well-defined Service Level Agreement that specify security controls, service levels and liability of Service Providers for violation of SLAs.
- All contracts and SLAs relating to outsourced services should detail security requirements in compliance with ISP and supporting Standards & Procedures.
- Outsourcing contracts should be reviewed for compliance with legal, regulatory, and statutory requirements, contractual obligations, and ISP, prior to being approved.
- An acknowledgement in writing may be obtained from the third parties for acceptance of ISP and contract / SLA may suitable be modified to include non-disclosure clauses.
- Subcontracting clause may be suitably included in the contracts / SLA.
- TSIL shall obtain the source codes for all critical applications from their vendors. Where obtaining of the source code is not possible, TSIL shall put in place a source code escrow arrangement or other arrangements to adequately mitigate the risk of default by the vendor. REs shall ensure that all product updates and programme fixes are included in the source code escrow arrangement.
- TSIL shall obtain a certificate or a written confirmation from the application developer or vendor stating that the application is free of known vulnerabilities, malware, and any covert channels in the code. Such a certificate or a written confirmation shall also be obtained whenever material changes to the code, including upgrades, occur.

Monitoring and Review of Third-party services

- TSIL may review the performance of the third-party based on the agreed service levels.
- Security controls and service levels associated reports and records of third-party service providers may be independently assessed, reviewed, and monitored. Consultants/third parties audits may be performed periodically to review the services offered by the third party.
- TSIL may conduct annual review meetings to ensure that the desired performance levels are maintained by the third parties.

Managing Changes to Third Party Services

- TSIL may ensure that changes to third party services including maintaining and improving existing information security policies, procedures, and controls, are appropriately managed taking account of the criticality of business systems and processes involved and re-assessment of risks.

AUDIT & COMPLIANCE

Audit & Compliance

- All relevant legal, statutory, regulatory, and contractual requirements related to Information Technology should be identified, documented, and incorporated in the Information Technology Standards & Procedures document.
- Information systems, processes and operations should be checked periodically for compliance with ITP.
- The Information system audit conducted by TSIL should address the IT risk exposure throughout TSIL including areas of corporate governance of information systems and security controls.
- The information system audit may be done in line with the risk-based methodology as may be prescribed. TSIL shall conduct information system audits on a periodic basis, or, as and when required.
- Data protection and privacy should be ensured as required by relevant legislation, regulations, and, if applicable, contractual clauses.

Audit Trail

- Every IT application which can access or affect critical or sensitive information, shall have necessary audit and system logging capability, and should provide audit trails.
- The audit trails shall satisfy TSIL's business requirements apart from regulatory and legal requirements.
- The audit trails must be detailed enough to facilitate the conduct of audit, serve as forensic evidence when required and assist in dispute resolution, including for non-repudiation purposes.
- TSIL shall put in place a system for regularly monitoring the audit trails and system logs to detect any unauthorized activity.

E-WASTE MANAGEMENT

- The Policy covers handling of all electrical and electronic assets which are obsolete or broken and considered as having no more useful / serviceable life in TSIL and hence are intended to be sold, donated, or discarded.
- The Policy also aims at generating awareness amongst all the working staff for proper

maintenance of electrical and electronic equipment and proper disposal at the end of their useful life.

- TSIL shall identify as per Disposal policy the electronic equipment's to be considered as e-waste
- The electrical goods identified for disposal can be sold to certified e-Waste vendor on as is where is basis.
- The necessary certificate as per the norms of the Central Pollution Control Board shall be obtained from the said e-Waste vendor and kept on record for future use.
- Records of E-waste shall be properly maintained by the Admin Team.

ACCEPTABLE USAGE

- IT assets of TSIL are provided for business purposes and authorized users should adhere to safe usage practices that do not disrupt business or bring disrepute to TSIL.
- All employees and third parties with access to information systems and assets must comply with the Acceptable Usage Policy and applicable legal, statutory, regulatory, and contractual requirements.
- Any breach in this regard may result in disciplinary and/or legal action.

IT Strategy Committee (ITSC)

An IT Strategy Committee is a governance body within an organization responsible for overseeing and guiding the alignment of information technology (IT) initiatives with the organization's overall business objectives.

Constitution

The IT Strategy committee shall include following members

Sr.No	Name	Designation
1	Mr. V.K. Taparia, Executive Director	Chairman
2	Mr. P.C. Somani, CFO	Member
3	Mr. Sudhir Kanvinde, CIO	Member
4	Mr. Yogesh Sawant, Head of IT Infra	Member

Quorum – At least 3 members

Meeting Frequency – At Least Half yearly basis

Roles & Responsibilities-

- Ensure that the company puts in place an effective IT strategic planning process
- Guide in preparation of IT Strategy and ensure that the IT Strategy aligns with the overall strategy of the company towards accomplishment of its business objectives
- Satisfy itself that the IT Governance and Information Security Governance structure fosters accountability, is effective and efficient, has adequate skilled resources, well defined objectives and unambiguous responsibilities for each level in the organization
- Ensure that the processes are in place for assessing and managing IT and cybersecurity risks
- Ensure that the budgetary allocations for the IT function (including for IT security), cyber security that commensurate with the company's IT maturity, digital depth, threat environment.
- Ensure implementation of a robust IT architecture meeting statutory and regulatory compliance
- Review on annual basis, the adequacy and effectiveness of the Business Continuity Planning and Disaster Recovery Management of the company
- Review of existing IT projects and assessing the cyber security aspect of the projects
- Conducting cyber security assessment / review for the new technology / business implementation and its changes
- Review of cyber security projects such as implementation of new security tool
- Update the management periodically on the activities of IT Strategy Committee.