1.0 OBJECTIVES

We, LDS committed to establish and define procedures for the effective management, security, maintenance, and availability of Information Systems used across the organization, including ERP, HRMS, email, network infrastructure, and manufacturing related IT systems.

2.0 SCOPE

This policy applies to all information systems, users, hardware, software, and IT infrastructure owned or managed by the Company, including:

- IT assets (servers, desktops, networks, applications)
- Locations (Plant sites, U-1, U-2 & U3)
- Third-party services/ Cloud-based platforms (cloud, ERP, remote access)
- Applications used in manufacturing, supply chain, HR, and finance

3.0 ROLES AND RESPONSIBILITIES

Frequency	Reviewer	Communication to
Once in three Years	Managing Director	IT

IT

- Oversee system availability, performance, and compliance

System Administrators

- Backup, patching, updates, and access controls

Network Admin

- Firewall, internet, VPN, and LAN/WAN management

Application Owner

- Ensures uptime and functionality of specific apps (e.g., ERP)

End User

- Use systems responsibly and report issues immediately

4.0 PROCEDURES

I. Establishment of internal regulations and policies related to information security

- Employees are required to adhere to the NDA executed at the time of employment with LDS, Need to check with HR.
- LDS information must be used for appropriate business purposes only.

- Disclosing proprietary or confidential information internally and externally must be done with proper safeguards in accordance with applicable laws.

II. Education for the prevention of information security breaches (Internal regulations training, etc.)

- Employees who have been assigned access credentials to work with systems that generate, store, or manage confidential information bear the responsibility for preserving the complete confidentiality of such access credentials to ensure against unauthorized use by any other person.
- Employees who have any reason to believe or suspect that someone else is using their access credentials must immediately notify their supervisor.
- Employee misuse of confidential information and/or the systems in which the information is stored is a serious breach of job responsibilities and will result in discipline up to and including termination of employment

III. Audit of control procedures to prevent information security violations

- Implementation of ISMS as per ISO 27001 : 2022 requirements
- Internal Audit to be conducted on yearly basis by Qualified Internal Auditors
- NCR to be closed within 10 days time period

IV. Incident Response Plan (IRP) for managing breaches of confidential information

- Incident Response Plan (IRP) to be prepared and implemented

V. Conducting information security risk assessments

- *Risk Identification*
- *Risk Estimation & Evaluation*
- *Risk Control*
- *Monitoring Effectiveness of Risk Control*

VI. Measures to protect customer / third-party data from unauthorized access or disclosure

Employee misuse of confidential information and/or the systems in which the information is stored is a serious breach of job responsibilities and will result in discipline up to and including termination of employment

A. System Installation & Configuration

- Install only approved hardware and licensed software.
- Use hardened configurations aligned with IT policy.

B. User Access Management

- Provision access via formal request (HR Department Head approval).
- Assign access rights based on job role (least privilege principle).
- Disable/remove access on resignation, transfer, or suspension.
- Use multi-factor authentication for sensitive systems.

C. Backup and Restore

- Daily/weekly automated backups for critical systems (ERP, MES, server files).
- Store backups both on-site and off-site/cloud.

D. Patch Management

- Removing root cause (malware, compromised accounts, etc.).

E. Monitoring and Logging

- Use monitoring tools for server health, uptime, CPU, memory, and disk usage.
- Monitor logs for unauthorized access or anomalies.
- Retain logs for minimum 90 days or as per audit requirement.

F. Incident Response

- Report system failures, breaches, or anomalies to IT Helpdesk.
- Follow defined Incident Response Procedure (see IRP document).
- Document root cause analysis and corrective actions.

G. Asset Management

- Maintain a register of all IT assets with owner, location, and serial numbers.
- Conduct physical and logical asset audits annually.

H. System Decommissioning

- Wipe data using secure erasure tools.
- Remove access from all systems and update asset register.
- Recycle or dispose of hardware as per e-waste policy.

5.0 Information Security Controls

- *Wipe data using secure erasure tools.*
- Remove access from all systems and update asset register.
- Recycle or dispose of hardware as per e-waste policy
- Failure to protect customer and third-party information may damage relations with customers, suppliers, or others and may result in legal liability.

6.0 Password policy

- All employees are required to use this system to store passwords for all LDS related content requiring a password.

6.0 TOOLS AND SYSTEMS USED

- ERP (e.g., SAP / Oracle / Tally)
- MES (Manufacturing Execution System)
- Firewall (e.g., Fortinet / SonicWall)
- Antivirus (e.g., Quick Heal / Sophos / McAfee)
- Backup Software (e.g., Veeam / Acronis)
- Server

7.0 REVIEW FREQUENCY

Frequency	Reviewer	Communication to
Once in three Years	MD / Directors	Respective employees

Prepared by	Approved by
M. Dinesh	
ESG Coordinator	Director / MD

L.D.S. RUBBER TECH (CHENNAI) PVT. LTD. CHENNAI