Title: IT Policy	Doc. No.: L3-PUR
	Rev. No.: 00
	Effective Date: 01/03/ 2020
	Date : 01/03/2020

1. Purpose

This policy outlines the acceptable use, security, and management of IT resources at Oriental Rubber Industries to ensure data integrity, operational efficiency, and protection against cyber threats.

2. Scope

Applies to all employees, contractors, consultants, temporary staff, and other workers at Oriental Rubber Industries who use IT systems, including hardware, software, networks, and data.

3. Acceptable Use

- IT resources must be used for business purposes only.
- Personal use of company devices should be minimal and not interfere with work.
- Users must not install unauthorized software or access inappropriate content.

4. Data Security

- All sensitive data must be stored on secure servers or approved cloud platforms.
- Regular backups must be performed and stored securely.
- Access to data should be role-based and reviewed periodically.

5. Password Policy

- Passwords must be strong (minimum 8 characters, mix of letters, numbers, symbols).
- Passwords must be changed every 90 days.
- Sharing passwords is strictly prohibited.

6. Email and Communication

- Company email should be used for official communication only.
- Phishing awareness training will be conducted annually.
- Suspicious emails must be reported to IT immediately.

7. Hardware and Software Management

- All hardware and software must be procured through the IT department.
- Unauthorized devices are not allowed on the company network.
- Software updates and patches must be applied regularly.

8. Internet Usage

- Internet access is monitored and filtered.
- Streaming, downloading, or accessing non-business-related content is discouraged.
- VPN must be used when accessing company resources remotely.

9. Mobile Device Policy

- Mobile devices accessing company data must be encrypted and password-protected.
- Lost or stolen devices must be reported immediately.
- Remote wipe capability must be enabled on all company-issued mobile devices.

10. Incident Response

- All IT incidents (e.g., data breaches, malware infections) must be reported to the IT team immediately.
- The IT team will investigate and document incidents and take corrective actions.

11. Compliance

- Employees must comply with applicable laws and regulations (e.g., GDPR, IT Act).
- Non-compliance may result in disciplinary action, including termination.

12. Review and Updates

- This policy will be reviewed annually or as needed.
- Updates will be communicated to all employees.

13. ERP System Guidelines

- ERP access is role-based and granted only upon approval.
- Users must ensure accuracy of data entered.
- Unauthorized modifications are prohibited.
- Training is mandatory before access.
- Daily backups and audits are required.
- Vendor updates must be managed by IT.

14. Cybersecurity Policy

- IT department manages cybersecurity controls.
- Firewalls, antivirus, and VPNs must be used.
- Email filtering and phishing training are mandatory.
- Sensitive data must be encrypted.
- Incident response plan must be followed.
- Annual cybersecurity training is required.
- Compliance with standards like ISO 27001 is mandatory.