TRANSFORMERS & RECTIFIERS [INDIA] LTD.

	Document No. IT/ITSP/01	Issue No. 1	Date 08/04/25
	INFORMATION TECHNOLOGY SECURITY POLICY AND PROCESS	Page	1 OF 3

1.0 Purpose:

The purpose of this Information Technology Security Policy is to protect TARIL's information assets, manufacturing systems, and business applications from unauthorized access, misuse, disclosure, alteration, or disruption, ensuring the **confidentiality, integrity, and availability** of information.

2.0 Scope:

This policy applies to:

- All IT systems, Production-supporting systems, networks, applications, and data.
- Corporate office, manufacturing plants, warehouses, and remote locations.
- All employees, contractors, consultants, vendors, and third parties.
- On-premises, clouds, and remote access environments.

3.0 Information Security Objectives:

- Protect business, customer, supplier, and employee information
- Ensure reliability of manufacturing and operational systems
- Preventing cyber threats, data breaches, and unauthorized access
- Support business continuity and regulatory compliance

4.0 Governance and Responsibilities:

TARIL's IT Department / Information Security Team

- Implement and maintain security controls
- Monitor systems, vulnerabilities, and incidents
- Report on security posture to management

Department Heads / System Owners of TARIL

- Classify data and approve user access
- Ensure systems comply with security requirements

Users

- Follow information security policies and procedures
- Protect login credentials and IT assets
- Report security incidents immediately

5.0 Information Technology Security Policy and Processes

5.1 Access Control

Policy:

Access to TARIL's systems and data shall be granted strictly on a **need-to-know and least privilege basis**.

Process:

1. User access request submitted and approved by department head/system owner
2. IT provisions access based on approved role
3. Privileged access requires additional approval
4. User access reviewed at least quarterly
5. Access revoked immediately upon resignation, termination, or role change

5.2 Data Classification and Protection

Policy:

Information must be classified and protected according to its sensitivity.

Data Classification:

- Public
- Internal
- Confidential
- Restricted

Process:

1. System owners classify information
2. Confidential/Restricted data encrypted where applicable
3. Access restricted based on classification
4. Secure disposal of data when no longer required

5.3 Network and Infrastructure Security

Policy:

TARIL's network and infrastructure must be protected against internal and external threats.

Process:

1. Firewalls and network security devices implemented
2. Network segmentation between office IT and production systems
3. Security logs monitored regularly
4. Remote access controlled and secured
5. Periodic review of firewall and network rules

5.4 Endpoint and Device Security

Policy:

All endpoints accessing TARIL systems must meet security standards.

Process:

1. Anti-virus/anti-malware installed and updated
2. Operating system and application patches applied regularly
3. USB and external media usage controlled
4. Laptops and portable devices secured and encrypted where required

5.5 Incident Management

Policy:

Information security incidents must be identified, reported, and resolved promptly.

Process:

1. Users report incidents immediately to IT
2. Incident logged and categorized
3. Containment and mitigation actions taken
4. Root-cause analysis conducted
5. Corrective actions implemented and documented
6. Significant incidents reported to management

5.6 Vulnerability and Patch Management

Policy:

System vulnerabilities must be identified and addressed in a timely manner.

Process:

1. Periodic vulnerability scans conducted
2. Vulnerabilities assessed based on risk
3. Patches applied as per defined timelines
4. Patch status tracked and reviewed

5.7 Backup, Recovery, and Business Continuity

Policy:

Critical systems and data must be protected against loss and disruption.

Process:

1. Regular backups of critical systems and production data
2. Secure storage of backups
3. Periodic backup restoration testing
4. Disaster Recovery (DR) and Business Continuity Plans maintained

5.8 Third-Party and Vendor Security

Policy:

Third parties accessing TARIL systems must comply with information security requirements.

Process:

1. Security requirements included in contracts
2. Vendor access limited, monitored, and time-bound
3. Access revoked upon contract completion

5.9 Security Awareness and Training

Policy:

All users must be aware of their information security responsibilities.

Process:

1. Security awareness training onboarding
2. Periodic refresher training
3. Communication of security threats and best practices

6.0 Monitoring and Compliance:

- Compliance with this policy is mandatory
- Security controls are monitored periodically
- Non-compliance may result in disciplinary action

7.0 Exceptions:

Any exception to this policy must be:

- Documented
- Risk-assessed
- Approved by IT and Management

8.0 Review and Maintenance:

This policy should be reviewed **annually** or upon significant changes to TARIL's IT or business environment.

PREPARED BY	REVIEWED & APPROVED BY	DATE OF APPROVAL
MITUL PATEL	CHANCHAL RAJORA	08/04/2025