MODERN TOOLING SOLUTION

INFORMATION SECURITY POLICY

1. Purpose and Scope

1.1 Purpose

This policy outlines the commitment of Modern Tooling Solution to protect its information assets—including operational data, customer information, employee records, and intellectual property—from unauthorized access, use, disclosure, modification, or destruction.

1.2 Scope : This policy applies to:

- All employees, contractors, and third-party service providers
- All systems, networks, devices, and platforms used to process or store company data
- All physical and digital forms of information

1.3 Objective:

- Ensure Confidentiality, Integrity, and Availability (CIA) of information
- Prevent unauthorized access and data breaches
- Ensure compliance with applicable legal, regulatory, and contractual obligations

2. Roles and Responsibilities

2.1: Management

- Approve and support the implementation of the policy
- Allocate necessary resources for security initiatives

2.2: Information Security Officer / IT Head

- Oversee enforcement and compliance
- Conduct risk assessments and audits
- Investigate security incidents

2.3: Employees

- Follow security procedures
- Protect passwords and access credentials
- Report suspicious activity or incidents promptly

3. Information Classification

All company information shall be classified into:

- **Confidential** (e.g., financial records, personal data)
- **Internal Use Only** (e.g., process documentation, shift schedules)
- **Public** (e.g., marketing materials)

Appropriate handling, storage, and transmission methods must be used based on classification.

4. Access Control

- Access to systems and information is granted on a **need-to-know** basis
- **Passwords must be strong**, changed regularly, and not shared
- Use of **multi-factor authentication (MFA)** is encouraged where applicable
- Access rights will be revoked immediately upon termination of employment

5. Data Protection

- Sensitive information must be **encrypted** during storage and transmission
- Use **licensed antivirus and firewall software** on all systems
- Regular **data backups** must be performed and stored securely
- Only authorized storage devices (e.g., company-approved USBs) may be used

6. Physical Security

- Entry to server rooms, control rooms, and storage areas is restricted
- Visitors must be logged and escorted
- All workstations should be **locked when unattended**

7. Use of IT Resources

- Company systems must be used for business purposes only
- **No unauthorized software** may be installed
- Internet and email use must comply with company guidelines

8. Incident Management

- All security breaches, data leaks, or unauthorized access must be reported to the Information Security Officer immediately
- An investigation and response process will be initiated as per the **Incident Response Plan**

9. Training and Awareness

- Employees will receive regular training on:
  - Phishing and social engineering risks
  - Secure password practices
  - Handling confidential information

10. Compliance Standards

- Information Technology Act, 2000 (India)
- ISO/IEC 27001:2013 – Information Security Management System
- GDPR (where applicable to international partners)
- Cybersecurity Guidelines from CERT-IN (Indian Computer Emergency Response Team)
- Industry-specific compliance like SEBI, RBI, or MSME guidelines if applicable

11. Time Frame and Deadline

- Risk Assessment: Conducted semi-annually.
- Policy Review and Update: Every 12 months or upon significant changes.
- Incident Response Testing: Twice per year.

12. Authorization and Approval

This policy has been prepared by the IT Department, reviewed by the Compliance Department, and approved by Senior Management.

Prepared by: Chief Information Security Officer (CISO)

Reviewed by: Legal and Compliance Head

Approved by: Managing Director / CEO

13. Documentation and Record

Mandatory Records:
- Risk Assessment Reports
- Access Logs and Audit Trails
- Incident Reports and Resolutions