R SQUARE ENGINEERS
Giving the competitive edge

SECURITY POLICY

RSE'S SOP FOR SECURITY PROCESS

1ST APRIL 2024
DOC. NO. RSE/HRM/P/16
R SQUARE ENGINEERS

1 Purpose:

The purpose of this policy is to safeguard the organization's physical and intellectual assets, ensuring the security of employees, assets & stocks as well as protecting confidential information and maintaining the secrecy of production processes.

2 Scope:

This policy applies to all employees, visitors, vendors and third parties who enter the organization's premises and have access to its physical and digital assets.

3 Objective:

- Protect company assets, stocks, information, and intellectual property
- Safeguard employees and contractors
- Prevent unauthorized access to manufacturing facilities
- Ensure compliance with legal and regulatory requirements related to security

4 General Security Guidelines:

- **Access Control:** Employees and authorized personnel are the only ones allowed access to the manufacturing area and sensitive locations. No unauthorized personnel should enter restricted areas without explicit permission from a supervisor. Lock doors, gates, or storage areas when not in use.

- **Visitor Management**: All visitors are allowed to visit office area and meet RSE-PPM officials with prior appointment for matters relating to their business. Visitors are not allowed to enter restricted areas unless permitted and escorted by company's authorized personnel.

- **Physical Security Measures:** Doors, gates, windows and other entry points should be kept locked at all times when not in use. All windows and doors should be secured after working hours. CCTV cameras are installed at key locations (entrances, exits, production areas) and are monitored regularly and the surveillance footage are archived for a minimum of 30 days.

5 Physical Security:

- **Lighting**: Ensure the premises, especially external areas, shall be well-lit to deter unauthorized access after working hours.

- **Surveillance Systems**: CCTV surveillance cameras are installed in key areas such as entrances, exits, and the production floor for monitor activities on a regular basis and the surveillance footage shall be archived for a minimum of 30 days.

- **Locks & Alarm Systems**: All entrances and critical storage areas shall be guarded with appropriate locking arrangements to restrict unauthorized entry during working hours as well as after business hours.

6 Data Security:

- **Physical and Digital Data Protection**: Sensitive data, information & records (such as financial records, employee data, customer data and product designs) shall be secured by keeping in locked areas or encrypted digital systems. Authorized usage of laptops, mobile devices or USB drives containing sensitive information shall be ensured.

- **Password Management**: Authorized access & strong password policy for accessing company systems and networks shall be ensured. All employees shall strictly follow the code of conduct policy for ensuring confidentiality of critical data & information in line with the NDAs signed by the company with clients.

- **Protection from malware attack**: All computers & servers shall have licensed security software installed and updated regularly to prevent them from any external malware attack. Employees shall ensure these security software are always enabled and inform the IT person immediately in case they face / observe any problem to ensure security is never compromised.

- **Data Backup**: Data shall be backed up regularly (daily for critical systems and weekly for non-critical data).

7 Employee Responsibilities:

- **Workplace Behaviour**: Employees shall report any suspicious activity, unauthorized individuals, or security concerns to management immediately.

- **Confidentiality**: Employees must maintain confidentiality of sensitive company information both during and after employment.

- **Personal Items**: Personal items should be kept secure in designated lockers or areas; the organization is not liable for lost or stolen personal items.

8 Emergency Procedures:

- **Evacuation Plans:** Ensure all employees are familiar with evacuation routes and emergency procedures. Regular fire drills and safety training sessions shall be conducted to ensure effectiveness during such unlikely situations.

- **Incident Reporting:** All employees shall follow the process for immediately reporting security breaches, theft, accidents, or emergencies if any to the management team.

9 Maintenance and Audits:

- **Security System Maintenance:** Regularly check and maintain locks, cameras, alarms, and access control systems.
- **Internal Audits:** Conduct routine security audits to assess the effectiveness of the security measures and identify areas for improvement.

10 Compliance and Enforcement

- **Legal Compliance**: Ensure all security measures comply with local laws and regulations regarding privacy, data protection and workplace safety.
- **Consequences of Violating Security Policies**: Any employee or contractor found violating the security policy shall face disciplinary action, up to and including termination or legal action.

11 Policy Review and Updates:

This policy should be reviewed annually or when there are significant changes in operations or security threats to ensure it remains up to date. Updates will be communicated to all employees, and training sessions will be held if necessary.

________**s/d**__________
Mahesh Patel
(Proprietor)