1. Introduction

This Information Security Policy establishes the principles and guidelines to protect the confidentiality, integrity, and availability of information assets of the CEV Engineering Pvt Ltd. It supports compliance with legal, regulatory, and contractual obligations.

2. Scope

This policy applies to:

- All employees, contractors, and third-party users
- All information systems and data (digital and physical)
- All locations, including manufacturing plants, warehouses, and offices
- Suppliers, logistics partners, and service providers handling CEV Engineering data

3. Objectives

- Protect proprietary manufacturing data, designs, and customer data
- Prevent data breaches, cyberattacks, and industrial espionage
- Ensure operational continuity and compliance with ISO 27001 and IATF 16949

4. Roles & Responsibilities

Role	Responsibility
Top Management -	Approve ISMS policy, allocate resources, review risk posture
IT Department -	Implement controls, monitor systems, ensure technical compliance
Employees -	Adhere to security policies and report incidents
Third Parties -	Comply with contractual security requirements

5. Key Policy Statements

A. Access Control

- Access to information is granted based on role and need-to-know.
- Multifactor authentication (MFA) is enforced for critical systems (ERP).
- Regular access reviews are conducted (quarterly minimum).

B. Asset Management

- All information assets are inventoried.
- Asset owners are designated for each critical system.
- Sensitive customer or OEM data must be encrypted at rest and in transit.

C. Data Classification

- Information is classified as: Public, Internal, Confidential, and Restricted.
- Confidential data (e.g., OEM drawings, cost sheets) must be encrypted and access restricted.

D. Physical and Environmental Security

- Entry to production floors and server rooms is controlled via biometric access.
- CCTV surveillance is active 24/7 in critical infrastructure areas.
- Visitors are logged and accompanied.

E. Cybersecurity Controls

- Firewalls, antivirus, and endpoint protection systems are mandatory.
- USB ports are disabled on all workstations handling sensitive data.

F. Email and Internet Use

- Company-provided email is the only authorized communication channel for official use.
- Phishing protection tools and spam filters must be enabled.
- Social media access is restricted on shop floor devices.

G. Incident Management

- All employees must report suspected incidents (data loss, phishing, etc.) immediately.
- A formal Incident Response Plan (IRP) is maintained and tested annually.
- Major incidents are reviewed in Management Review Meetings.

H. Third Party & Supplier Security

- NDAs are mandatory for vendors with access to sensitive information.
- Cybersecurity posture of key suppliers is assessed annually.
- Data exchange with OEMs must follow secure protocols (e.g., VPN).

I. Backup & Disaster Recovery

- All critical business and production systems are backed up daily.
- Backups are stored securely, offsite or in cloud with versioning.
- DR drills are conducted yearly once.

J. Information Security Awareness

- Annual training on phishing, password security, and data handling is mandatory.
- Posters and newsletters reinforce best practices.
- Security induction is part of onboarding.

6. Compliance & Monitoring

- Regular internal audits will be conducted per ISO 27001 and IATF 16949 guidelines.
- Non-conformities are documented and corrective actions implemented.
- Violations may result in disciplinary action, up to termination.

7. Review & Maintenance

This policy will be reviewed annually or upon significant changes in operations, threats, or legal requirements.

Young Jin Kim
Managing Director

Effective Date: 02.01.2024