Address: Plot No.11C, Industrial Park, Site – A, Ammavaripalli Village, Penukonda Mandal, Anantapur, Andhra Pradesh, India-515164
Email: govind@saehani.com CIN -U28999AP2017FTC107297, Tel: +91-9133442003

DATA PROTECTION POLICY

Version: 1.0
Effective Date: 11-11-2024
Approved By: P.Govindarajulu

---

1. Purpose

The purpose of this policy is to ensure that all customer and third-party data handled by KSH Automotive Pvt Ltd is protected from unauthorized access, use, disclosure, alteration, or destruction.

---

2. Scope

This policy applies to all employees, contractors, suppliers, service providers, and third parties who handle or have access to customer or third-party data in the course of business with KSH Automotive Pvt Ltd.

---

3. Policy Statement

KSH Automotive Pvt Ltd is committed to:

- Ensuring confidentiality, integrity, and availability of personal and third-party data.
- Complying with applicable data protection laws, regulations, and customer requirements.
- Implementing appropriate technical and organizational measures to prevent data breaches.

Address: Plot No.11C, Industrial Park, Site – A, Ammavaripalli Village, Penukonda Mandal, Anantapur, Andhra Pradesh, India-515164
Email: govind@saehani.com CIN -U28999AP2017FTC107297, Tel: +91-9133442003

4. Key Data Protection Measures

4.1 Access Control

- Role-based access is implemented across systems handling sensitive data.
- Multi-factor authentication (MFA) is mandatory for privileged users.
- Regular access reviews are conducted.

4.2 Data Encryption

- Data is encrypted during transmission (e.g., SSL/TLS) and at rest (AES 256-bit or equivalent).
- Encrypted backups are maintained as per the retention policy.

4.3 Vendor and Third-Party Controls

- Data protection clauses are included in all supplier and service agreements.
- Third-party security assessments are conducted periodically.

4.4 Employee Responsibilities

- Mandatory training on data privacy and security awareness.
- All employees must sign confidentiality and non-disclosure agreements.
- Internal disciplinary action for non-compliance with this policy.

4.5 Monitoring and Incident Response

- All access and data processing activities are logged and monitored.
- An Incident Response Procedure (IRP) is in place for managing security breaches.
- Any breach involving customer/third-party data must be reported within 24 hours to the Compliance Officer.

4.6 Physical and Network Security

- Secure access controls in place for server rooms, storage facilities, and data centers.
- Firewalls, anti-virus software, and intrusion detection/prevention systems are implemented.

Address: Plot No.11C, Industrial Park, Site – A, Ammavaripalli Village, Penukonda Mandal, Anantapur, Andhra Pradesh, India-515164
Email: govind@saehani.com CIN -U28999AP2017FTC107297, Tel: +91-9133442003

4.7 Data Retention and Secure Disposal

- Data is retained as per the company's **Data Retention Policy**.
- Data is securely deleted or destroyed when no longer required.

---

5. Roles and Responsibilities

Role	Responsibility
IT Department	Implement and maintain technical security measures
Compliance Officer	Monitor compliance and investigate incidents
Department Heads	Ensure staff adhere to this policy
All Employees	Handle data responsibly and report any breaches

---

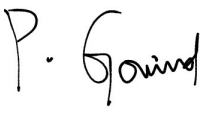
6. Enforcement

Any violation of this policy will result in disciplinary action, up to and including termination of employment or contract, and may include legal action.

---

7. Review and Updates

This policy will be reviewed annually or when there are significant changes to laws, technology, or organizational structure.



Compliance Officer
Approved on: 11-11-2024
Next Review Date: 11-11-2025