



DATA PROTECTION POLICY

Document No.: KSH/ISMS/DP/01

Version: 1.0

Effective Date: 01-04-2025

Review Date: Annual

Approved By: Managing Director

1. PURPOSE

KSH Automotive Pvt. Ltd. recognizes the importance of protecting personal, customer, supplier, employee, and third-party information from unauthorized access, disclosure, alteration, loss, misuse, or destruction.

This policy establishes the framework for safeguarding information assets and ensuring compliance with applicable data protection laws, customer requirements, contractual obligations, and information security best practices.

2. SCOPE

This policy applies to:

- All employees of KSH Automotive Pvt. Ltd.
- Directors and management personnel
- Contract workers and consultants
- Suppliers and service providers
- Business partners and third parties handling company data
- All information systems, applications, databases, records, and storage media used by the company

This policy covers both electronic and physical information assets.



Address: Plot No.11C, APIIC Industrial Park, Site A, Ammavaripalli Village, Penukonda, Anantapur, Andhra Pradesh, India-515164.

Email: kshhr@saehani.com

CIN -U28999AP2017FTC107297,

3. POLICY STATEMENT

KSH Automotive Pvt. Ltd. is committed to:

- Protecting the confidentiality, integrity, and availability of information.
- Complying with applicable legal, regulatory, contractual, and customer requirements.
- Preventing unauthorized access, disclosure, modification, or destruction of information.
- Implementing appropriate technical and organizational controls to safeguard data.
- Ensuring responsible handling of personal and business information throughout its lifecycle.

4. DATA PROTECTION PRINCIPLES

KSH Automotive Pvt. Ltd. shall ensure that information is:

4.1 Lawfully Processed

Data shall be collected, processed, stored, and shared only for legitimate business purposes and in accordance with applicable legal requirements.

4.2 Accurate and Complete

Reasonable steps shall be taken to maintain accurate and up-to-date information.

4.3 Protected Against Unauthorized Access

Appropriate controls shall be implemented to ensure information is accessible only to authorized individuals.

4.4 Retained Appropriately

Information shall be retained only for as long as necessary to meet legal, contractual, and business requirements.

4.5 Securely Disposed

Information that is no longer required shall be securely deleted, destroyed, or disposed of.



5. ACCESS CONTROL

5.1 Role-Based Access

Access to information systems and sensitive data shall be granted based on business need and job responsibilities.

5.2 User Authentication

- Unique user IDs shall be assigned to authorized users.
- Strong password requirements shall be enforced.
- Multi-Factor Authentication (MFA) shall be implemented for privileged and critical accounts.

5.3 Access Reviews

Periodic reviews shall be conducted to ensure access rights remain appropriate and necessary.

6. DATA ENCRYPTION

To protect sensitive information:

- Data shall be encrypted during transmission using secure protocols such as SSL/TLS.
- Sensitive information stored electronically shall be encrypted using industry-recognized standards such as AES-256 or equivalent.
- Backup media containing sensitive information shall be encrypted and securely protected.

7. VENDOR AND THIRD-PARTY SECURITY

KSH Automotive Pvt. Ltd. shall ensure that suppliers, contractors, and service providers handling company information maintain adequate security controls.

Requirements include:



Address: Plot No.11C, APIIC Industrial Park, Site A, Ammavaripalli Village, Penukonda, Anantapur, Andhra Pradesh, India-515164.

Email: kshhr@saehani.com

CIN -U28999AP2017FTC107297,

- Confidentiality obligations through contracts or Non-Disclosure Agreements (NDAs).
- Data protection clauses within supplier agreements.
- Periodic assessment of third-party security practices.
- Compliance with applicable customer and regulatory requirements.

8. EMPLOYEE RESPONSIBILITIES

All employees shall:

- Protect confidential and sensitive information.
- Follow company information security procedures.
- Use company systems responsibly.
- Report security incidents immediately.
- Participate in mandatory security awareness training.

Employees handling sensitive information must sign Confidentiality and Non-Disclosure Agreements.

Failure to comply with this policy may result in disciplinary action.

9. MONITORING AND INCIDENT MANAGEMENT

9.1 Monitoring

The company shall monitor and log:

- System access activities
- User authentication events
- Data processing activities
- Security-related events

Monitoring shall be conducted in accordance with legal and regulatory requirements.



Address: Plot No.11C, APIIC Industrial Park, Site A, Ammavaripalli Village, Penukonda, Anantapur, Andhra Pradesh, India-515164.

Email: kshhr@saehani.com

CIN -U28999AP2017FTC107297,

9.2 Incident Reporting

Any suspected:

- Data breach
- Unauthorized access
- Information leakage
- Cybersecurity incident
- Loss of sensitive information

must be reported immediately to the Compliance Officer or designated Information Security Representative.

9.3 Incident Response

KSH Automotive Pvt. Ltd. shall maintain an Incident Response Procedure (IRP) to:

- Investigate security incidents.
- Contain threats.
- Recover affected systems.
- Prevent recurrence.
- Notify affected stakeholders where required.

Customer and third-party data breaches shall be reported internally within 24 hours of discovery.

10. PHYSICAL SECURITY

The company shall implement appropriate physical security controls, including:

- Restricted access to server rooms and IT infrastructure.
- Controlled access to records storage areas.
- Visitor management procedures.
- Secure storage of confidential documents.
- Protection of portable devices and removable media.



11. NETWORK AND CYBER SECURITY

The organization shall maintain appropriate cybersecurity controls, including:

- Firewalls
- Anti-virus and anti-malware protection
- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- Secure network configurations
- Regular vulnerability assessments and patch management

These controls shall be periodically reviewed and updated.

12. DATA RETENTION AND SECURE DISPOSAL

12.1 Data Retention

Information shall be retained in accordance with:

- Legal requirements
- Regulatory obligations
- Customer requirements
- Business needs
- Company retention schedules

12.2 Secure Disposal

When information is no longer required:

- Electronic records shall be securely deleted.
- Physical documents shall be shredded or destroyed.
- Storage devices shall be sanitized or destroyed before disposal.



13. ROLES AND RESPONSIBILITIES

Management

- Provide leadership and resources for data protection activities.
- Ensure implementation of this policy.

IT Department

- Implement and maintain technical security controls.
- Monitor information security systems.
- Support incident management activities.

Compliance Officer

- Monitor compliance with this policy.
- Investigate reported incidents.
- Coordinate corrective actions.

Department Heads

- Ensure employees comply with policy requirements.
- Promote data protection awareness within their departments.

Employees

- Handle information responsibly.
- Follow security procedures.
- Report incidents and breaches immediately.

14. COMPLIANCE AND ENFORCEMENT

Failure to comply with this policy may result in:

- Corrective actions
- Disciplinary proceedings



KSH Automotive Pvt. Ltd.

Address: Plot No.11C, APIIC Industrial Park, Site A, Ammavaripalli Village, Penukonda, Anantapur, Andhra Pradesh, India-515164.

Email: kshhr@saehani.com

CIN -U28999AP2017FTC107297,

- Suspension of system access
- Termination of employment or contract
- Legal action where applicable

The company reserves the right to investigate any suspected violation of this policy.

15. POLICY REVIEW

This policy shall be reviewed annually or whenever there are significant changes relating to:

- Data protection legislation
- Information security threats
- Business operations
- Customer requirements
- Technology infrastructure

All revisions shall be communicated to affected personnel.

For KSH Automotive Private Limited

A handwritten signature in black ink, appearing to read 'Yongsung Kim', is positioned above the name of the Managing Director.

Mr. Yongsung Kim -Managing Director