Information Security Policy Statement

1. Purpose

This Information Security Policy Statement summarises our commitment to protecting customer, company and personal information. It is intended for customers and business partners and provides a high-level overview of our information security principles without disclosing internal operational details.

2. Information security commitment

Information security is a management priority and an integral part of our business operations. Our Information Security Management System is based on TISAX AL 3 and the VDA Information Security Assessment (ISA) 2027 and is designed to protect information throughout its life cycle.

3. Scope and applicability

Our information security requirements apply to employees, relevant external service providers, business processes, IT systems, and information assets involved in handling customer, company or personal information. Relevant suppliers and partners are required to meet applicable security requirements where contractually agreed.

4. Protection objectives

We protect information based on the principles of **confidentiality**, **integrity** and **availability**. Customer and company information is protected against unauthorised access, disclosure, loss, manipulation and disruption according to its protection needs and applicable legal, contractual and business requirements.

5. Governance and responsibilities

Information security responsibilities are defined, communicated and reviewed. Management provides oversight and resources, while information security functions coordinate the implementation, monitoring and continual improvement of security measures. Employees are required to comply with applicable information security requirements and report suspected incidents or weaknesses.

6. Security controls

We maintain appropriate organisational, personnel, physical and technical controls to protect information. These include access management, secure information handling, employee awareness, physical protection, secure IT operations, vulnerability and patch management, backup and recovery measures, network protection, malware protection, logging, monitoring and supplier security controls.

7. Legal and contractual compliance

Applicable legal, regulatory and contractual requirements are identified, assessed and considered in our information security policies, risk management, supplier management and management reviews. This includes requirements related to confidentiality, data protection, customer agreements, service obligations and other binding commitments.

8. Incident response and continuity

We maintain processes to identify, report, assess and respond to information security incidents. Lessons learned from incidents are used to improve the ISMS. Business continuity and recovery arrangements are maintained to support timely response and restoration of important business operations in crisis situations.

9. Supplier and partner security

When selecting suppliers and partners, preference is given to those with relevant information security certifications or comparable evidence of security maturity. Where applicable, security requirements are contractually agreed and monitored during the business relationship. Suppliers, contractors and external service providers are assessed according to the nature of their services, their access to information and the protection needs of the information involved. We ask our supplier to pass relevant security requirements on to sub-suppliers where necessary to maintain a secure supply chain.

10. Review and continual improvement

This policy statement and the underlying information security framework are reviewed periodically and updated when relevant legal, contractual, organisational or technical changes occur. Management reviews the effectiveness of the ISMS and supports continual improvement of information security.