HORIZON GROUP OF COMPANIES

INFORMATION SECURITY POLICY

PUBLIC DOCUMENT

Document Reference	ISP-001
Version	1.0
Classification	Public
Document Owner	Chief Operating Officer (COO)
Frameworks	ISO/IEC 27001:2022 (Clause 5.2) | TISAX® / VDA ISA 6.0

This document is approved for public release. It provides an overview of HORIZON GROUP's commitment to information security. Detailed controls and procedures are maintained in internal documentation.

1. Purpose

HORIZON GROUP provides logistics and supply chain services to original equipment manufacturers (OEMs), Tier-1 suppliers, and industry partners across the automotive value chain. In doing so, we process, transmit, and store confidential information belonging to our clients, business partners, employees, and our own operations.

This Information Security Policy ('the Policy') states HORIZON GROUP's commitment to protecting information assets and defines the high-level objectives and principles of our Information Security Management System (ISMS). It is the primary policy document under which all supporting information security policies, processes, and controls are established.

This Policy is issued to fulfil the requirements of:

- ISO/IEC 27001:2022, Clause 5.2 – Top management shall establish an information security policy
- TISAX® / VDA ISA 6.0 – Information Security control IS-01 (information security policy and organization)
- Applicable legal and regulatory obligations, including the EU General Data Protection Regulation (GDPR) and the NIS2 Directive

2. Scope

This Policy applies to:

- All HORIZON GROUP employees, managers, and directors, regardless of location or employment type
- All subsidiaries of HORIZON GROUP regardless of location or country.
- All contractors, temporary staff, consultants, and third parties who access or process HORIZON GROUP information assets
- All information assets – in any form (digital, physical, verbal) – owned, processed, or held on behalf of HORIZON GROUP or its clients
- All systems, applications, networks, and facilities within the defined ISMS boundary

The ISMS scope, which defines the specific organizational units, locations, and processes covered, is maintained in a separate Scope Statement, available to authorized stakeholders and TISAX audit providers upon request.

3. Information Security Objectives

HORIZON GROUP is committed to maintaining and continuously improving its ISMS in order to achieve the following information security objectives:

- Protect the confidentiality, integrity, and availability (CIA) of all information assets entrusted to HORIZON GROUP by its clients, OEM partners, employees, and suppliers
- Ensure all personnel, contractors, and relevant third parties understand their information security responsibilities and are equipped to fulfil them through adequate training and awareness
- Manage information security risks systematically through a risk-based approach, ensuring risks are identified, assessed, and treated in line with HORIZON GROUP's risk appetite
- Comply with all applicable legal, regulatory, and contractual obligations relating to information security, including GDPR, NIS2, and automotive supply chain requirements (TISAX® / VDA ISA)
- Protect sensitive automotive data, including vehicle development data, prototype information, and confidential OEM content, in accordance with TISAX® assessment requirements
- Preserve HORIZON GROUP's reputation and maintain the trust of customers, partners, and the wider automotive supply chain
- Detect, respond to, and recover from information security incidents in a timely and effective manner, minimizing impact on business operations and third parties
- Continually improve the ISMS through periodic reviews, internal audits, management assessments, and lessons learned from security incidents

4. Management Commitment

The Executive Management of HORIZON GROUP is fully committed to information security and to the effective operation of the ISMS. This commitment is expressed by:

- Establishing, communicating, and enforcing this Policy and the information security objectives throughout the organisation
- Ensuring that information security requirements are integrated into business processes, projects, and strategic decisions
- Allocating the financial, human, and technological resources required to implement, maintain, and continually improve the ISMS
- Promoting a culture in which all personnel actively support information security and are encouraged to report actual or suspected incidents without fear of retaliation
- Holding regular Management Reviews of the ISMS to assess its continuing suitability, adequacy, and effectiveness
- Ensuring that roles, responsibilities, and authorities for information security are clearly assigned and communicated

5. Information Security Principles

The following principles guide the design and operation of HORIZON GROUP's ISMS:

5.1 Risk-Based Approach

Information security decisions are based on a structured assessment of risk. Controls are implemented and maintained in proportion to the risk they address, considering the nature of information handled in the automotive supply chain, including classified OEM content and TISAX-protected data.

5.2 Confidentiality, Integrity, and Availability

All controls are designed to protect the three core attributes of information: confidentiality (preventing unauthorized disclosure), integrity (preventing unauthorized modification), and availability (ensuring information is accessible when legitimately required).

5.3 Least Privilege and Need-to-Know

Access to information and systems is granted based on the minimum level of privilege necessary to perform a defined business role. Access to confidential information – including data classified at TISAX protection levels – is restricted to those with a documented need to know.

5.4 Legal and Contractual Compliance

HORIZON GROUP complies with all applicable laws, regulations, and contractual requirements relating to information security, including GDPR, NIS2, and the information security obligations imposed by OEM and Tier-1 customer contracts, including TISAX® assessment requirements.

5.5 People, Process, and Technology

Effective information security requires a combination of capable people, well-defined processes, and appropriate technology. HORIZON GROUP invests in all three dimensions and ensures that its workforce is competent and aware of their information security obligations.

5.6 Continual Improvement

The ISMS is not static. HORIZON GROUP commits to continually reviewing and improving its information security practices in response to changes in the threat landscape, business environment, and applicable requirements.

6. Roles and Responsibilities

Accountability for information security is distributed across all levels of the organisation:

- Executive Management bears ultimate accountability for the ISMS and for ensuring adequate resources are available to meet the information security objectives
- The Chief Technology Officer (CTO) is responsible for the development, implementation, maintenance, and oversight of the ISMS, including compliance with ISO 27001:2022 and TISAX® / VDA ISA 6.0 requirements
- Managers and team leaders are responsible for ensuring this Policy and all supporting controls are understood and implemented within their areas
- All employees and contractors are responsible for complying with this Policy and all supporting information security policies, completing mandatory security awareness training, and reporting actual or suspected information security incidents promptly
- Third parties (suppliers, service providers, partners) who process HORIZON GROUP information are required to comply with contractually agreed information security requirements commensurate with the sensitivity of the data they handle

7. Supporting Policy Framework

This Policy is supported by topic-specific policies, processes, and procedures that provide detailed guidance for employees and form the documented body of the ISMS. These include policies covering:

- Information classification and handling
- Access control and identity management
- Physical and Environmental Security
- Acceptable use of information assets

- Cryptography and data protection
- Incident management and response
- Business continuity and disaster recovery
- Supplier and third-party security
- Human resource security (pre-employment, during employment, and termination)
- Risk management and treatment

These documents are maintained in HORIZON GROUP's ISMS documentation system and are available to personnel with appropriate access rights. Summaries of relevant obligations are communicated to employees through security awareness training.

8. Policy Compliance

Compliance with this Policy and all supporting information security policies is mandatory for all persons within the scope defined in Section 2.

Actual or suspected breaches of this Policy must be reported immediately to the HORIZON GROUP Information Security team at info@horizonautologistics.com or through the incident reporting channel. HORIZON GROUP guarantees that good-faith reports of suspected breaches will not result in retaliation.

Breaches of this Policy may result in disciplinary action, up to and including termination of employment or contract, and may be referred to law enforcement authorities where criminal conduct is suspected.

Compliance with this Policy is monitored through internal audits conducted by the ISMS team, management reviews, and third-party assessments including ISO 27001 certification audits and TISAX® assessments by ENX-accredited audit providers.

9. Exception Process

Every effort must be made to comply with this Policy. Exceptions may only be granted in exceptional, documented circumstances. Any request for an exception must:

- Be submitted in writing to the CTO, including full business justification and proposed compensating controls
- Be risk-assessed and documented in the risk register
- Receive written approval from the CTO (and from Executive Management for high-risk exceptions)
- Be time-limited, with a defined expiry and review date

No permanent exceptions to this Policy will be granted. Unapproved non-compliance is treated as a policy violation.

10. Review and Revision

This Policy shall be reviewed at least annually by the CTO and re-approved by Executive Management. Additional reviews shall be triggered by:

- Significant changes to the business, technology environment, or applicable regulations
- The occurrence of a major information security incident
- Changes to TISAX® / VDA ISA requirements or ISO 27001 standard
- Results of internal audits or external assessments indicating the Policy requires update

Per Folkesson
Chief Executive Officer
Per Folkesson

— END OF DOCUMENT —

ISP-001 v1.0 · HORIZON GROUP · ISO/IEC 27001:2022 Cl. 5.2 · TISAX® / VDA ISA 6.0 · PUBLIC