Information Security Policy

Purpose

This information Security Policy establishes a binding framework for managing cybersecurity and information security within the company. It is issued in accordance with applicable legislation (the Business Corporations Act and related regulations, Act No 224/2015 Coll., on the Prevention of Major Accidents), the requirements for regulated services, and the normative requirements of TISAX at level 2.

Company Commitment

As a large enterprise, the company ensures that all information assets are protected in a manner appropriate to their importance. We ensure information security both as a supplier and as a service provider in the automotive industry.

The company´s management is committed to providing the necessary resources, supporting the effective operation of the Information Security Management System(ISMS), and actively contributing to its development.

Main Objectives of the ISMS

The purpose of the Information Security Management System(ISMS) is to:
- ensure **the availability**, **integrity**, **and confidentiality** of all information, both electronic and paper -based,
- ensure the secure and reliable operation of information technologies suppoerting the company´s activities,
- protect sensitive information of the company, its customers, partners, and suppliers,
- comply with the requirements of legislation, contractual obligations, and TISAX standarts.

Information Security Management Principles

The company is committed to:
I. Managing risks – continuously identify, assess, and minimize risks in the area of information security and data protection.
II. Training employees – ensure the professional competence of all employees through regular training and education accorrding to their roles.
III. Conducting audits – perform an information security audit annually and addres any identified deficiencies.
IV. Improving the ISMS – continuously enhance the effectiveness and efficiency of security measures and processes.
V. Monitoring and reviewing the system – regularly evaluate the effectiveness of the ISMS, implement necessary changes, and respond to new thretas and requirements.
VI. Respecting legal and contractual requirements – comply with applicable legislation, internal regulations contractual obligations, and stakeholder requirements.
VII. Ensuring information systém security – implement and document security measures, and manage access, technologies, and processes.

Responsibilities

The company supports the functioning of the ISMS through:
- establishing thios policy and related objectives,
- defining roles, duties, and responsibilities in the area of information security,
- systematic employee training and promoting security awareness,
- providing the necessary resources (personnel, technical, and financial),
- setting criteria for risk acceptance and their tolerated levels,
- conducting internal audits and security assessments,
- actively managing security events and incidents,
- supporting the continuous improvement of the ISMS.

This Information Security Policy is further elaborated into IMS objectives in TŽ-MS.