

EVO IMS Policy

1. Purpose and Aims

The purpose of this Integrated Management System (IMS) policy, encompassing the Information Security Management System (ISMS), Quality Management System (QMS), and Environmental Management Systems (EMS) at Évolution Synergétique Automotive S.L. (ÉVO), is to establish a strategic framework for further development of topic and target-specific guidelines for the IMS.

This document signifies the management's commitment and serves as the foundation for planning, executing, operating, measuring, and continuously improving the IMS. Our requirements are derived from normative, contractual, and self-imposed specifications.

1.1. Normative Requirements

Our IMS certification requirements are derived from:

- ISO/IEC 27001
- ISO 9001
- ISO 14001
- TISAX - VDA ISA

1.2. Contractual Requirements

Our contractual obligations for the IMS stem from agreements with customers and partners, including non-disclosure agreements and supply contracts, where information security and quality are of importance.

1.3. Self-imposed Requirements

We use an Integrated Management System (IMS) to provide our customers with the highest possible quality of products and services while ensuring the protection of our applications and processes, taking into account environmental considerations.

2. Scope and Responsibilities

The IMS at ÉVO applies to all internal and external employees within the organization.

3. Guideline Contents

3.1. Corporate Strategy/ Mission

Mission: We provide services and support for the development of integral and customized solutions in the field of electromobility, while developing in-house and innovative mobility solutions to drive and accelerate the transition to a sustainable future.

Vision: Our vision is to be a benchmark in the transformation of the future mobility, driven by an unquestionable commitment to the satisfaction of our customers and an exceptional organizational culture. We aim to be recognized as a model of innovation, quality, and excellence, where the customer experience and the well-being of our employees are fundamental. We aspire to be the preferred workplace in our industry, through the promotion of an inclusive, positive, and constantly growing environment for our team.

3.2. Policy of the Integrated Management System

We commit to implementing information security and quality in business operations, while also considering environmental factors. This involves the planning, execution, operation, measurement, and continuous improvement of the IMS. Our information security and quality guidelines, processes, and resources form the foundation for our daily operations. We use these for suitable, appropriate and state-of-the-art measures to protect centralized and decentralized applications, systems and components that are necessary for secure business operations and to meet our quality standards.

The management of ÉVO is the highest authority for the IMS.

3.2.1. General Threat Scenario and Information Security

The business operations of ÉVO increasingly depend on Information and Communication Technologies (ICT), with the human factor playing a crucial role as a regulatory component. In these human-machine systems, information

security is paramount to guarantee the smooth functioning of the technology. The goal is to ensure the availability, integrity, and confidentiality of information processed by ICT.

3.2.2. Quality

Our objective is to ensure compliance to, and correct implementation of, all quality management requirements. All activities and processes within the scope of the IMS are evaluated for compliance with the quality objectives set by the company.

3.2.3. Environmental Commitment

Our commitment to the environment includes effective environmental management, setting and achieving environmental objectives compatible with our strategic direction, integrating environmental management system requirements into our business processes, ensuring available resources for environmental management, and promoting continuous improvement.

3.3. Objectives of the Integrated Management System

The top management defines the strategic framework objectives within the scope of the IMS, aligned with the strategic direction of ÉVO.

Our IMS objectives include:

- I. The protection goals of information security in terms of confidentiality, integrity and availability are a central component of our policy.
- II. We protect applications, systems and components that are necessary for secure business operations.
- III. We ensure compliance with legal, regulatory, contractual and self-imposed obligations regarding information security and quality.
- IV. We consider information security, quality and environment as an integral part of our corporate culture.
- V. The management is a promoter of information security, quality and environment and a role model to our internal and external employees.
- VI. We implement an information security, quality and environmental organization with clear responsibilities and authorities to effectively design

and operate information security, quality and environment, assess performance and continuously improve it.

- VII. We consider existing information security, quality and environment as a success factor of our IMS. We therefore create an appropriate awareness of information security, quality and environment among our employees and regularly promote the application of our guidelines.
- VIII. We consider efficient and forward-looking risk management as an integral part of our IMS. In principle, we strive for a low level of risk, but also take on appropriate risks when opportunities arise. However, we do not enter into any risks that could endanger our existence.
- IX. We align measures in information security, quality and environment with our business objectives. They must be appropriate and in an economically justifiable proportion to possible damage.
- X. We promote constructive handling of information security, quality and environmental events and weaknesses among our employees in order to be able to react quickly and effectively and to derive possibilities for improvement.
- XI. We consider information security as an integral part of our emergency and crisis organization.
- XII. We strive to constantly improve our information security, quality and environment with our service and outsourcing partners.
- XIII. We submit our documented regulations on information security, quality and environment to continuous quality control, especially with regard to effectiveness, comprehensibility and implementation.
- XIV. We monitor, measure, analyse and evaluate the effectiveness of our Integrated Management System through external and internal audits. The management is regularly and appropriately informed in order to be able to make decisions to improve information security quality an environment. Quantitative indicators are used to the extent necessary to manage our information security and quality performance.

3.4. Documentation, Updating, and Review of the Regulations on Information Security and Quality

We apply comprehensive documented regulations to achieve our information security, quality and environmental goals.

In particular, we have derived topic and target group-specific guidelines from the strategic framework objectives (see section 5.3),

The guidelines are reviewed for their suitability, appropriateness and effectiveness at scheduled intervals or on special occasions.

The Management is involved in any changes of outstanding importance.

All employees are made aware of the regulations that apply to them in our IMS portal or repositories.

For certain interested parties, such as suppliers, authorities, partners and customers, these are made available in an appropriate manner to the extent necessary.

4. Management Responsibilities for the IMS Policy and Objectives

The management:

- is committed to the policy described in this document and ensures that the strategic information security and quality objectives defined in this guideline are translated into concrete guidelines and that they are adhered to within the scope of the IMS.
- is committed to the continuous improvement of the IMS and, to this end, makes decisions in the context of regular management reviews by examining its continued suitability, appropriateness and effectiveness. This includes this IMS Guideline.
- commits itself to implement applicable requirements with regard to information security and quality appropriately.
- ensures that this IMS guideline is communicated to all internal and external staff within the scope of the IMS and, where necessary, to interested parties.
- has overall responsibility for the IMS and ensures that the normative requirements for obtaining the corresponding certificates are met.

- has created an IMS organisation with roles and committees, assigned responsibilities and provided it with the necessary authority to optimally perform all IMS-related tasks.

5. Committees and Roles of the IMS Organization

Different bodies and roles have been defined for the operation of the IMS. These roles include Integrated Management System Officer (IMS-O), Information Security Officer (ISO), Information Security and Quality Coordinators or Managers, and the IMS Control Committee.

5.1. Integrated Management System Officer (IMS-O)

The IMS-O is responsible for the establishment, operation and continuous development of the IMS in accordance with legal, regulatory, contractual and self-imposed obligations.

IMS-O supports the Top Management, who retains overall responsibility for the IMS.

In principle, it coordinates measures for the maintenance and improvement of necessary documentation for the IMS and promotes their implementation.

The IMS-O is responsible for establishing a continuous improvement of environmental actions of all EVO staff, although care for the environment depend on responsibility of each employee.

The IMS-O is in charge of providing awareness to guarantee that EVO staff know the company IMS policy considering environmental aspects.

Its specific tasks are described in various directives and procedures of the IMS documentation.

5.2. Information Security Officer (ISO)

The ISO supports the IMS-O in setting up, operating and continuously developing the ISMS in accordance with legal, regulatory, contractual and self-imposed obligations.

ISO implements defined technical and organizational measures to maintain and improve the information security of ÉVO.

The concrete tasks are described in various directives and procedures for information security.

5.3. Information security and quality coordinators or managers

They promote the implementation of information security, quality and environmental specifications in their area, e.g. a specialist department, and thus contribute to the multiplication of information security and quality in ÉVO.

5.4. IMS Control Committee

The IMS Control Committee monitors and controls information security, quality and environment in the company. It decides on guidelines and specifications that are valid throughout the company. It meets at least once a year.

Members are the Managing Directors as well as the IMS-O, ISO and, as required, others such as information and Quality Coordinators.

6. Responsibilities of the Employees

Directives and procedures for information security, environment and quality must be observed by all employees. Violations of this guideline and the additional regulations, processes and procedures for information security, environment and quality can result in consequences under criminal, civil or labor law.

The design and application of our specifications use the following formulations:

- Mandatory requirements: commit to a certain behaviour.
- Target specifications: obligatory like a mandatory specification, but allow exceptions in atypical cases, which must be objectively justified.
- Optional requirements: are at the individual discretion of the individual, in relation to a specific decision situation. No justification necessary.

6.2. Incident reporting

Safety-relevant events, which particularly affect safe business operations, must be reported (also in case of suspicious cases!). The disclosure of confidential and data protection-relevant information to unauthorised third parties or observed or suspected weaknesses in telecommunications and electronic data processing systems must be reported. Examples are, for example, the loss of hardware, inexplicable system behaviour, loss or modification of data and programs,

suspicion of misuse of the own user ID. Events that endanger the quality of processes, services or products must also be reported.

In individual cases, it may be necessary to involve the direct superior before reporting, but this is not mandatory. Reports can also be made verbally.


Further information:

- User Manual
- Security Incident Management Manual

7. Signatures

Signed on behalf of ÉVO by the Management.

28/04/2023



José Juan Mellado Troncoso