CIE Automotive

Policy on Information Technologies and Cybersecurity Risks

Contents

1. Purpose 3

2. Scope of application 3

3. Basic security principles 4

4. Measures to ensure information security 4

4.1. Prevention 4

4.2. Detection and response 5

4.3. Recovery 5

5. Organisational framework 5

6. Monitoring and control 6

The Board of Directors ("**Board**") of CIE Automotive, S.A. ("**CIE Automotive**" or the "**Company**", and collectively with its subsidiaries the "**Group**"), has approved this Policy on Information Technologies and Cybersecurity Risks. It is one of the policies on corporate governance and legal compliance, and it establishes the principles and guidelines used to support appropriate management of information security.

1. Purpose

The purpose of this Policy on Information Technologies and Cybersecurity Risks is to create a framework of principles and guidelines that will provide adequate support for proper management of information security, to ensure that the activities will be performed with appropriate oversight, rigour, and compliance.

CIE Automotive recognises that information security is an important part of performing its activities correctly.

It has therefore developed this policy, which establishes the basic security principles and integrates them with the operational requirements related to information confidentiality, authentication, traceability, integrity, availability, and storage.

The primary objective of this policy is to strengthen CIE Automotive's commitment to the employees, companies, clients, and suppliers, as part of its continual improvement in relation to the services offered, compliance with the applicable legislation, the internal processes, and protection of the information that CIE Automotive manages in the workplace.

This makes it necessary to ensure that all persons who interact with CIE Automotive, whether directly or indirectly, are aware of the contents of this policy and its corresponding rules for implementation, as well as the need to apply those contents when performing their own functions in relation to CIE Automotive.

This Policy on Information Technologies and Cybersecurity Risks has therefore been developed to ensure that CIE Automotive's information assets are protected, and it must be applied during all phases of the information lifecycle: generation, distribution, storage, processing, transport, viewing, and destruction.

To ensure effective application of this policy and its corresponding rules for implementation, CIE Automotive must allocate the resources necessary to allow its proper development, in terms of the policy's implementation and maintenance, and also including the security controls and measures established in each workplace.

2. Scope of application

This policy applies to:

- ✓ All of CIE Automotive's companies, the Group.
- ✓ All contractors and external parties acting under CIE Automotive's responsibility, or that have access to its assets.
- ✓ All information managed, processed, or stored by any of the Group's areas.
- ✓ All facilities, systems, resources, and processes used to provide internal services or services connected with external parties via agreements or contracts.

This policy has also been established to allow monitoring of the supply chain, to ensure that all its participants have commitments in line with those of the company; and to manage information security when the products sold are being developed and manufactured.

This policy is part of the legal framework defined by the laws and regulations in force, as directly or indirectly related to information security and to the use of automated means of information processing.

This policy is designed to be practical and dynamic, which means that new rules for its implementation can be incorporated after its initial entry into force.

In addition, all legislation and regulations in force on the subject of personal data protection, intellectual property, and use of online tools must be understood as applicable, with the following sources and standards used as references:

- ✓ GDPR: The European Union's General Data Protection Regulation (Regulation (EU) 2016/679).
- ✓ TISAX: Trusted Information Security Assessment Exchange.
- ✓ ISO/IEC 27001: a standard that outlines the requirements for establishing an Information Security Management System (ISMS).
- ✓ ISO/IEC 27002: a standard that provides guidance on controls for implementing an ISMS, such as those relating to access to information, encryption of confidential data, and password management.
- ✓ Other standards required by stakeholders, especially the clients.

3. Basic security principles

- ✓ Agreeing that information and the systems used to process and store it are strategic assets, with a commitment to achieving the levels of security necessary to ensure protection of those assets and, therefore, improve the quality of the services offered to employees and clients.
- ✓ Ensuring the confidentiality of the information managed for appropriate provision of the services, with the security measures adapted to the level of confidentiality required for the information managed.
- ✓ Ensuring the availability of the information and the systems used to process and store it, establishing the necessary organisational, physical, and technological measures needed for prevention, detection, and recovery.
- ✓ Managing the risks to which the information may be exposed by identifying potential threats and implementing appropriate security measures to address them.
- ✓ Maintaining a security environment that ensures compliance with the legal requirements that apply to information and to the systems.

4. Measures to ensure information security

In order to ensure the existence of an overall information security framework that provides as much protection as possible against those threats, CIE Automotive's Security Committee must implement a series of measures to prevent and detect possible incidents affecting information, as well as measures for reaction and recovery.

Information security must be understood as a comprehensive process that includes all technical, human, material, and organisational elements related to the system.

A variety of initiatives must be implemented to support the efforts already made, with the aim of providing a general overview on information security for all parties involved; defining adequate controls for protecting the assets; and complying with the requirements established by the legislation in force.

In relation to this, adequate mechanisms must be put in place to prevent and detect incidents that could potentially affect information security, along with mechanisms for reaction and recovery. These mechanisms include the following measures, among others:

4.1. Prevention

Efforts must be made to prevent and avoid incidents that could affect information security and the services provided. This must be done by implementing the necessary security measures and controls, which must be defined using a formal process of risk analysis and management.

Those measures and controls, along with the responsibilities related to information security, must be clearly and formally defined and documented in the corresponding Information Security Policy and Information Security Rules.

In addition, to ensure compliance with the Information Security Policy, the following must occur through each of the departments:

- Active participation in the development lifecycle for the systems, especially their authorisation before going into operation.
- Periodic evaluations of the information security situation, with external reviews requested in order to obtain an independent assessment.

4.2. Detection and response

Prevention measures are not always sufficient to entirely prevent security incidents, which means that there must be ongoing monitoring of the information systems to identify any anomalies during their operation.

Whenever an information security incident is detected, the corresponding verification, analysis, and communication mechanisms must be activated.

4.3. Recovery

Continuity plans must be established for the systems, to prepare for any situations where incidents have a significant impact, and those plans must be integrated with the general business continuity plans and recovery activities.

5. Organisational framework

Ensuring the security of the information assets is a responsibility that corresponds to all the company's departments, and to each and every one of the people who interact with those assets.

However, the Company's Board has been delegated responsibility, to the extent permitted by law, for coordinating the Group's general management strategies and guidelines, while operating in the interest of each and every one of the companies belonging to the Group. In turn, the Chair of the Board and the Company's CEO and senior managers are responsible for the function of organising and coordinating the Group by distributing, implementing, and monitoring the general strategy and policies that the Board has established.

As part of that delegation of responsibilities, the Company's Board, via its Audit and Compliance Committee, must perform oversight to ensure that the companies belonging to the Group are monitoring the principles and best practices contained in this corporate policy.

In turn, the Audit and Compliance Committee must delegate oversight of this policy and compliance with it to the Security Committee. In order to ensure the security of the information and related assets, that committee must perform the following functions:

- ✓ Review this policy at least once each year, and approve the rules used to implement it.
- ✓ Establish the means necessary to ensure that all persons subject to this policy understand its contents and the rules used to implement it.

The membership of the Security Committee must consist of the corporate representatives from the following departments: Information Systems, Engineering, Human Resources, and Compliance. Also, in addition to its permanent members, that committee must have invited members, determined on the basis of the information security situation and other conditioning factors.

That committee must appoint a Head of Information Security, with the following functions delegated to that person:

- ✓ Establishing the information security requirements, with responsibility for the use and protection of information within that position's scope of activity.
- ✓ Designating one or more people with authority to exercise the functions related to the information security requirements.
- ✓ Taking appropriate decisions to ensure that the security requirements for the information and services are being met, verifying that the established security measures are adequate for protecting the information and services and for maintaining the level of information security, within that position's scope of activity.
- ✓ Ensuring that periodic reviews are performed to verify compliance with the obligations related to information security, and ensuring that the appropriate training and awareness-raising is taking place at the company.

6. Monitoring and control

CIE Automotive must implement the control mechanisms necessary to ensure compliance with the legislation and the principles and best practices established in this policy, as part of an appropriate business management system. The Group must also dedicate adequate material resources and a suitable number of sufficiently qualified human resources for those purposes. It must approve and periodically review guidelines used to assess and manage the related risks, applicable to all the Group, which must include some objective criteria for classifying the operations based on their risks, along with specific procedures for their approval.