



SAFETY POLICY INFORMATION

by Eurodies Italia S.r.l.

Approved by the Board of Directors on 28.11.2025



Table of Contents

1. Introduction	3
2. Purpose of the document	3
3. Scope	4
4. Information Security Roles and Responsibilities	4
5. Principles for responsible information handling	5
6. Objectives for the information security of Eurodies Italia S.r.l.	6
7. Reports	7
8. Updating, dissemination and communication	7



1. Foreword

Eurodies Italia S.r.l. (hereinafter “Eurodies”, “Company” or “Company”) is aware that it operates in a context characterized by high requirements of **confidentiality, reliability, protection of technical know-how** and **protection of information** shared with customers, partners and other stakeholders in the automotive supply chain.

In this document, the Company defines the principles, guidelines and commitments undertaken to ensure adequate management of information security, ensuring the confidentiality, integrity and availability of the data and information processed, regardless of the format, medium or system through which they are generated, received, stored, transmitted or processed.

In this perspective, Eurodies is committed to **providing products and services that comply with the requirements** established by customers and the specific needs of the automotive sector, adopting a **structured approach** to information security management consistent with the best reference practices and with the requirements of the **TISAX** scheme (Trusted Information Security Assessment Exchange). Adherence to the TISAX certification process is an essential tool for the Company to strengthen its governance system, demonstrate the reliability of its processes and respond transparently to customer expectations in terms of information protection.

Eurodies recognizes that, in the automotive sector, the secure management of information takes on a strategic value, with particular reference to the protection of technical data, drawings, design specifications, commercial information, prototypes, confidential documentation and any other element of the company’s information assets or received from third parties. The protection of this information is a fundamental prerequisite for preserving business continuity, corporate reputation, customer trust and the competitiveness of the company.

Eurodies is fully aware that threats to information security represent a growing **risk**, also due to the progressive digitalization, the interconnection of production and design processes and the increasing complexity of relationships along the automotive supply chain. For this reason, the Company undertakes to take appropriate organizational, technical and procedural measures to prevent unauthorized access, loss, alteration, unavailability or undue disclosure of information.

2. Purpose of the document

The Information Security Policy aims to define the principles and commitments undertaken by Eurodies Italia S.r.l. to ensure the protection of the information managed in the context of its operational, design, production and commercial activities, with particular reference to the needs of the automotive sector.

With this document, Eurodies intends to **protect the company’s information assets** and the information received from customers, partners, suppliers and other interested parties, ensuring its confidentiality, integrity and availability.



Eurodies recognizes information security as an essential element to ensure business continuity, customer trust, compliance with applicable requirements and the competitiveness of the Company. The Policy also guides the **behaviour and responsibilities of the people involved** in company processes, promoting risk awareness, accident prevention and continuous improvement, in line with the TESAX assessment and certification process.

3. Scope

The Policy contained in this document applies **to all information managed by Eurodies Italia S.r.l.**, regardless of the format, medium or method of processing, including information in electronic, paper, verbal or otherwise available format as part of the company's activities.

The field of application includes IT systems, network infrastructures, applications, devices, physical and digital archives, as well as human resources involved in business processes, with particular reference to operational, design, production, commercial and administrative activities.

The Policy is binding for all employees, collaborators, suppliers, partners and third parties who, for any reason, process, use or access company data, documents and information or received from customers and other interested parties. Appropriate security measures are required at every stage of the information lifecycle, including creating, receiving, classifying, using, storing, transmitting, sharing, preserving and, where applicable, deleting or destroying information.

4. Information Security Roles and Responsibilities

The overall responsibility for information security is entrusted to the **Board of Directors**, which defines the strategic guidelines, approves the text of the Policy, promotes a corporate culture oriented towards the protection of information assets and ensures the availability of the resources necessary for the implementation of adequate organizational, technical and procedural measures.

It also promotes information, training and awareness-raising initiatives aimed at personnel and other figures involved, so that everyone is aware of the risks associated with the management of information and the correct methods of use of IT tools, company systems and the documentation processed, with particular reference to technical, design and confidential information in the automotive sector.

The **IT Manager**, appointed by the Management, has the task of ensuring the proper functioning of the company's IT infrastructure, supporting the implementation of security measures, overseeing the management of access and authorizations, monitoring the adequacy of the systems and contributing to the identification of any vulnerabilities or needs for improvement. His responsibilities also include monitoring IT service providers, verifying compliance with contractual agreements and monitoring the use of authorized and regularly licensed software.



All corporate functions involved in the management of data, documents, information systems and digital tools are required to operate in compliance with applicable legislation, the *Organisation, Management and Control Model*, internal procedures and company provisions on the processing, protection and management of information. The activities must be carried out according to **the principles of correctness, transparency, accuracy, completeness and segregation of tasks**, also through a correct assignment and periodic verification of access profiles.

All employees, collaborators and third parties who access company information or systems are responsible, to the extent of their competence, for compliance with the rules defined by the Company. In particular, they are required to use IT tools exclusively for work purposes, diligently guard their credentials, not disclose them to third parties, not install unauthorized software, not circumvent security measures and not engage in conduct that may compromise the confidentiality, integrity or availability of information.

Each party involved is also required to **promptly report any anomalies**, incidents, unauthorized access, vulnerabilities, non-compliant behavior or situations potentially detrimental to information security, actively contributing to the prevention of IT risks, the protection of company know-how and the continuous improvement of the information security management system.

5. Principles for responsible information handling

Eurodies adopts a systemic approach to information security management, based on the following key principles:

- **Confidentiality**
Access to information must be granted only to authorized persons, depending on the role held, the activities carried out and the actual operational needs.
- **Integrity**
Information must be complete, accurate, up-to-date, and protected from unauthorized modification, alteration, or deletion to ensure its reliability over time.
- **Availability**
Company information, systems and tools must be accessible in the time and manner necessary to carry out activities and business continuity.
- **Eurodies**
is committed to complying with applicable laws, regulations, contractual requirements and standards, including those relating to personal data protection, information security and the TESAX assessment and certification pathway.
- **Risk management**
Information security risks are identified, assessed and treated through a structured approach, aimed at preventing or reducing possible negative impacts on business operations, customers and other stakeholders.



- **Responsibilities**

All parties involved in the management, use or access to information are responsible for the proper protection of the information, in accordance with their role, activities and applicable business procedures.

- **Continuous improvement**

The information security management system is monitored, evaluated and updated over time to improve its effectiveness, strengthen existing safeguards and respond to the evolution of risks, technologies and applicable requirements.

6. Objectives for the information security of Eurodies Italia S.r.l.

Eurodies is committed to ensuring the protection of company information and confidential information received from customers, partners, suppliers and other interested parties, through the adoption of organizational, technical and procedural measures appropriate to the context in which it operates and consistent with the applicable requirements, including those provided for by the TESAX assessment and certification process.

To this end, Eurodies defines the following objectives for effective information security management:

- adopt, maintain and improve over time an **Information Security Management System** that is appropriate to the company's activities and the related risks;
- identify and periodically assess **risks relating to information security**, defining and implementing appropriate prevention, mitigation and control measures;
- **formalize and apply procedures and operating instructions** for access management, physical and logical protection of information, security of IT systems, backup management and business continuity;
- **promote staff awareness and training**, to spread a culture of safety and ensure that each person is aware of the risks and protection measures applicable to their role;
- **assess and monitor** relevant suppliers and subcontractors, so that an adequate level of protection of the information shared is ensured;
- **prevent** accidents, unauthorized access, loss, alteration, unavailability or improper disclosure of information;
- **monitor** the effectiveness of the measures taken and periodically update the objectives according to the evolution of risks, technologies, regulatory requirements and customer expectations.

To make its commitment measurable, Eurodies also defines these quantitative objectives:



- ensure that by 2027 at least 90% of staff receive **regular training on information security**;
- ensure that 100% of corporate users have **personal access credentials** and **system authorizations strictly limited to the tasks performed**.

7. Referrals

Eurodies promotes a business environment based on **integrity, responsibility and transparency**, encouraging the timely reporting of any unlawful conduct, violations of the *Organisation, Management and Control Model* pursuant to Legislative Decree 231/2001, non-compliance with company procedures or behaviour that may compromise information security.

The Company has made available to the Recipients an **internal channel** for reporting significant unlawful conduct pursuant to Legislative Decree 231/2001; violations of the Model or other situations potentially detrimental to the Company, including any violations or critical issues related to the management, protection and security of information.

This channel operates in compliance with D.lgs. no. 24/2023 on *Whistleblowing*.

Reports can be made, even anonymously, in the following ways:

- In **written form through the Whistleblowing platform**, which can be reached at the dedicated link on the company website and at the address <https://eurodies.integrity.complylog.com/>.
- In **oral form** by registration, according to the procedures provided for by the company procedure.

Reports are transmitted and managed in accordance with the procedures described in the paragraph "Reports" and in the paragraph "Measures in application of the discipline referred to in D.lgs. 24/2023" of the general part of the Model itself and, in particular, on the basis of the "Procedure for the management of reports pursuant to D.lgs. 24/2023" adopted by the Company.

Eurodies guarantees the **confidentiality of the identity of the whistleblower**, the persons involved and the content of the report, in compliance with the applicable regulations. The **protection of the whistleblower from any form of retaliation**, discrimination or penalization related to the report made in good faith is also ensured, without prejudice to the possibility of making anonymous reports in accordance with the procedures provided for by the company procedure.

8. Updating, dissemination and communication

The Board of Directors of Eurodies ensures the dissemination of the Information Security Policy to all employees, collaborators and, where applicable, to third parties involved in the management of or access to company information, in a manner suitable for ensuring its knowledge and effective application.



The Policy is **reviewed at least annually** and, in any case, whenever updates are necessary due to regulatory changes, evolution of applicable requirements, updates of the best practices of reference, needs related to the TISAX assessment and certification process or significant organizational, technological and operational changes.

Any updates to this document are approved by the Chairman and **promptly communicated to the relevant recipients** through the channels deemed most appropriate, including:

- emails to employees;
- posting or publication on the company bulletin board;
- delivery or sharing when hiring new staff;
- sharing when entering into or renewing contracts with suppliers, partners or other relevant third parties.

Eurodies is also committed to promoting understanding of the contents of the Policy through appropriate communication, information and awareness-raising initiatives, so that all the people involved are aware of the principles, commitments and responsibilities related to information security.

Avigliana (TO), 28.11.2025

The Management