The **COMPANY POLICY** requires that, in line with the company mission, the management of all business processes is set up with the rules of the application of the **TISAX Management System Version 6.0.3** developed taking into account the **ISO/IEC 27001:2022 standard and the controls provided for in Annex A.**

PURPOSE AND OBJECTIVES

The management of **COMET SUD & COMET SVK** has defined, disseminated and undertakes to maintain this policy for Information Security Management at all levels of its organization.

The purpose of this policy is to ensure **maximum customer satisfaction** in the use of our services and the **protection and protection from all threats, internal or external, intentional or accidental, of information in the context of our activities** in accordance with the indications provided by the ISO/IEC 27001 standard and the guidelines contained in the ISO/IEC 27002 standard in their latest versions.

SCOPE OF APPLICATION

This policy applies without distinction to all bodies and levels of the Company.

The implementation of this policy is mandatory for all personnel and must be included in the regulation of agreements with any external party who, for any reason, may be involved with the processing of information that falls within the scope of the TISAX Management System.

The information assets to be protected consist of all the information managed through the services provided and located in all the company's offices.

You must ensure:

- the **confidentiality** of information: i.e. the information must be accessible only by those who are authorized.
- Information **integrity**: i.e. protecting the accuracy and completeness of information and the methods for processing it.
- The **availability** of information: i.e. that authorised users can effectively access the information and related assets when they request it.

The lack of adequate levels of security can lead to damage to the corporate image, lack of customer satisfaction, the risk of incurring penalties related to the violation of current regulations as well as economic and financial damage.

An adequate level of security is also fundamental for information sharing.

The company identifies all security needs through the analysis of the risks that loom over its company assets which allows it to acquire appropriate awareness of the level of exposure to threats. The risk assessment makes it possible to assess the potential consequences and damages that may result from the failure to apply security measures to the information system and what is the realistic probability of implementation of the identified threats.

The results of this assessment determine the actions needed to manage the identified risks and the most appropriate security measures.

Our principles of information security management cover the following aspects:

1- ASSET INVENTORY ALWAYS UP-TO-DATE - Ensure a constantly updated catalog of company assets relevant to information management and a manager must be identified for each one. Information

must be classified according to its level of criticality, so as to be managed with consistent and appropriate levels of confidentiality and integrity.

2- UPDATED INFORMATION RISK ASSESSMENT – The information risk assessment is updated at least annually when management reviews or in the event of adverse events or in the event of an asset inventory adjustment.

3- SECURE ACCESS TO SYSTEMS - To ensure the security of information, any access to systems must be subject to an identification and authentication procedure. Information access permissions must be differentiated according to the role and positions held by individuals, so that each user can access only the information he or she needs, and must be periodically reviewed.

4- SAFE USE OF COMPANY ASSETS - Procedures must be defined for the safe use of company assets and information and their management systems.

5- CONTINUOUS TRAINING OF PERSONNEL - Full awareness of information security issues must be encouraged in all personnel (employees and collaborators) starting from the moment of selection and for the entire duration of the employment relationship.

6- TIMELY MANAGEMENT OF ADVERSE EVENTS - In order to be able to manage incidents in a timely manner, everyone must report any safety-related issues. Each incident must be handled as outlined in the procedures.

7- ADEQUATE PHYSICAL PROTECTION OF COMPANY PREMISES - It is necessary to prevent unauthorized access to the offices and individual company premises where information is managed and the security of the equipment must be guaranteed.

8- MANAGEMENT OF CONTRACTUAL COMPLIANCE WITH THIRD PARTIES - Compliance with legal requirements and information security principles in contracts with third parties must be ensured.

9- SIMULATIONS OF THE BUSINESS CONTINUITY PLAN - A continuity plan must be prepared that allows the company to effectively deal with an unforeseen event, ensuring the restoration of critical services in a time and manner that limits the negative consequences on the company mission.

10- COMPUTER SECURITY BY DESIGN - Security aspects must be included in all phases of design, development, operation, maintenance, assistance and decommissioning of IT systems and services.

11- CONTINUOUS LEGISLATIVE UPDATING - Compliance with legal provisions, statutes, regulations or contractual obligations and any requirements relating to information security must be ensured, minimizing the risk of legal or administrative sanctions, significant losses or damage to reputation.

12- PERIODIC PENETRATION TESTS – Periodic penetration tests must be carried out in infrastructures and applications to assess the resilience of systems to external attacks and identify any vulnerabilities and allow them to be subsequently fixed.

RESPONSIBILITY FOR COMPLIANCE AND IMPLEMENTATION

Compliance with and implementation of the policies are the responsibility of:
1- All personnel who, in any capacity, collaborate with the company and are in some way involved with the processing of data and information that fall within the scope of the Management System. All personnel are also responsible for reporting all anomalies and violations of which they become aware.

2- All external parties who maintain relationships and collaborate with the company. They must ensure compliance with the requirements contained in this policy.

The Head of the Management System who, within the framework of the Management System and through appropriate rules and procedures, must:
- Conduct risk analysis with appropriate methodologies and take all measures for risk management
- Establish all the rules necessary for the safe conduct of all business activities
- Verify security breaches and take necessary countermeasures and control the company's exposure to major threats and risks
- Organise training and promote staff awareness of all matters related to information security.
- periodically verify the effectiveness and efficiency of the Management System.

Anyone who, employees, consultants and/or external collaborators of the Company, intentionally or negligently, disregards the established safety rules and in this way causes damage to the Company, may be prosecuted in the appropriate places and in full compliance with legal and contractual obligations.

REVIEW

The Management will periodically and regularly verify the effectiveness and efficiency of the Management System or in conjunction with significant changes, in order to ensure adequate support for the introduction of all necessary improvements and to encourage the activation of a continuous process, with which control and adaptation of the policy is maintained in response to changes in the corporate environment. of the business, of the legal conditions.
The Head of the Management System is responsible for reviewing the policy.
The review will have to verify the status of improvement and corrective actions and adherence to the policy.
It will have to take into account all changes that may affect the company's approach to information security management, including organizational changes, the technical environment, the availability of resources, legal, regulatory or contractual conditions and the results of previous reviews.
The outcome of the review should include all decisions and actions related to improving the company's approach to information quality and security management.

MANAGEMENT COMMITMENT

Management actively supports information security in the company through clear direction, clear commitment, explicit assignments and recognition of information security responsibilities.
The management's commitment is implemented through a structure whose tasks are:
- Ensure that all information security objectives are identified and that they meet business requirements;
- Establish corporate roles and responsibilities for the development and maintenance of the TISAX Management System;
- provide sufficient resources for the planning, implementation, organization, control, review, management and continuous improvement of the TISAX Management System;
- check that the TISAX Management System is integrated into all business processes and that procedures and controls are developed effectively;
- Approve and support all initiatives aimed at improving the quality and security of information;
- activate programs for the dissemination of awareness and culture of information security.

30/06/2026

C.E.O. _____

IMPEGNO DELLA DIREZIONE

La direzione sostiene attivamente la sicurezza delle informazioni in azienda tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.
L'impegno della direzione si attua tramite una struttura i cui compiti sono:
- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e che questi incontrino i requisiti aziendali;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del Sistema di gestione TISAX;
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del Sistema di gestione TISAX;
- controllare che il Sistema di gestione TISAX sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- approvare e sostenere tutte le iniziative volte al miglioramento della qualità e sicurezza delle informazioni;
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.

31/03/2026

Amm.re Delegato

COMET SUD s.r.l.
Sede Legale e Stabilimento: S.S. 265 Km. 27,550
81025 Marcianise (CE)
UFFICIO COMMERCIALE
N. ORDINE N..... DATA.....
"APPROVATO"