Clients and current laws impose strict compliance with the expressed requirements regarding Information Security (IS).

Vulcaflex considers it essential and ethical to ensure IS in both its operations and its supply chain.

Vulcaflex S.p.A. is aware that only what is allowed by agreements between the parties can be disclosed and that incidents in this regard (disclosures of confidential or personal information) can have negative consequences in terms of image, credibility, and industrial efficiency.

Therefore, Vulcaflex S.p.A. has adopted several measures, the main ones being:

- Based on laws and agreements with Clients, it has determined the requirements to be respected for the security of information (personal and confidential).
- It has established a system of rules and procedures that must be followed by its staff and industrial Partners.
- It has defined a structure for the prompt and effective management of Security Incidents.
- It has established emergency plans to be implemented in case of crises that could compromise operational continuity.

The **objectives** are as follows:

- Ensure the Confidentiality, Integrity, and Availability of all informational resources.
- Ensure the security of information from Clients, the supply chain, and managed within Vulcaflex S.p.A., in compliance with legal and Client requirements.
- Maintain operational continuity.
- Keep Security Incidents at ZERO.
- Ensure continuous compliance with the Automotive industry's TISAX standard and continuous performance improvement.

This Policy, desired by Management and periodically reviewed by the same, aims to create corporate awareness regarding information security to ensure full compliance; it is complemented and integrated by a series of detailed procedures.

The principles of this policy are understood and fully respected by all Vulcaflex S.p.A. personnel.

Below are the specific details for Data Protection or Privacy, to be considered an integral part of this Policy.

The **objectives** of the Information Security Policy, for this specific part related to personal data and Privacy, are:

- Compliance with current laws (see GDPR 679/2016 and Legislative Decree 30 June 2003 No. 196) for which the appropriate documentation has been prepared (see Privacy Master document).
- Ensure confidentiality and correctness in the use of personal data for clients, suppliers, and employees.

To achieve these objectives, the following **guidelines** have been identified:

- Adaptation and constant updating of the information system; the configuration of the corporate information system prevents unauthorized access and illegal processing as much as possible.
- Instructions on the lawful and correct use of personal data, collecting them for specified, explicit, and legitimate purposes. The data are:
    - Relevant, complete, and not excessive in relation to the purposes for which they are collected or subsequently processed.
    - Stored in a form that allows the identification of the subject for no longer than necessary for the purposes for which they are collected or subsequently processed.
- Personnel training (responsible and designated individuals) to ensure full implementation of the Instructions.

To implement the above, the following **Strategy** has been defined:

- Implement the Data Protection or Privacy management system concerning personal data to demonstrate and apply the principle of accountability as provided for by Article 24 of the GDPR; this system is integrated into the more general Information Security Management System with a TISAX perspective.
- Adopt a risk-based approach to the freedoms and fundamental rights of individuals concerning personal data processing, inspired by the principles of privacy by default and by design (Article 25 of the GDPR) and ensuring compliance with appropriate security measures (Article 32 of the GDPR).
- Establish appropriate processes for managing informed consent and respecting the fundamental rights of data subjects as provided by the first part of the GDPR and in primary respect of the following general principles:
    - Data are processed:
        - According to the principle of lawfulness, that is, in accordance with GDPR provisions and Civil Code provisions, ensuring that processing is not contrary to imperative norms, public order, and good morals.

        - According to the fundamental principle of fairness, which should inspire anyone handling something belonging to another's sphere.
    - Data are collected only for:
        - Specified purposes, meaning that collection as an end in itself is not permitted.
        - Explicit purposes, meaning that the data subject is informed about the processing purposes.
        - Legitimate purposes, meaning that the processing purpose must be lawful.
        - Compatible purposes with the initial processing basis, especially in communication and dissemination operations.
    - Data are also:
        - Accurate, precise, true, and updated if necessary.
        - Relevant, meaning processing is allowed only for institutional functions related to the activity carried out.
        - Complete: not in the sense of collecting as much information as possible, but considering specifically the concrete interest and right of the data subject.
        - Not excessive in a quantitative sense relative to the pursued purpose, meaning only the data necessary and sufficient to achieve the purpose are collected.
        - Stored for no longer than necessary for processing purposes and in accordance with provisions regarding the storage periods of administrative acts. After this period, data are anonymized or deleted, and their communication and dissemination are no longer permitted.
- Inform, train, and raise awareness among all internal and external parties using the company's data.
- Adopt appropriate processes and procedures for testing, verifying, and evaluating the effectiveness of the technical and organizational measures adopted and monitor the Data Protection or Privacy management system's update (Article 32 of the GDPR).
- Plan audits and periodic reviews to ensure the maintenance and adequacy of the adopted technical and organizational measures.

Cotignola, 30 May 2024
General Manager