Borgaro Torinese, 18/06/2025

INFORMATION SECURITY POLICY

VIGEL Spa, in order to implement its **Information Security Policy**, has developed and undertakes to keep constantly updated an **Information Security Management System** (**ISMS**) compliant with the requirements of the technical standard ISO/IEC 27001:2022, the TISAX® framework and the relevant binding legal standards.

In particular, as part of the management of its information, VIGEL ensures:

1) The compliance with current legal and technical regulations and international safety standards that impact its technological and organizational infrastructure;
2) The observance of proper security levels through the implementation and maintenance of an **Information Security Management System** (**ISMS**);
3) The compliance of the ISMS with the requirements set out in the reference standards or frameworks mentioned above and the management of any non-conformities or incidents through appropriate corrective actions, also considered as a tool for the control and improvement of processes, and if the conditions exist, also through disciplinary actions pursuant to the workers national collective agreements;
4) The selection of reliable partners concerning the secure management of information and the protection of personal data, according to the Regulation (EU) 2016/679;
5) The protection and enhancement of the environment, minimizing the impact of company activities on it, with particular attention to the effects on climate change.

This **Information Security Policy**, distributed in a digital edition on the institutional website and in a paper edition by posting it on company noticeboards, applies to all internal and third-party personnel who in various capacities processes, archives and transmits information in carrying out company processes and concretely represents the organisation's commitment towards its employees and collaborators, customers and third parties, aimed at guaranteeing the safe management of information and the physical, logical and organizational tools suitable for processing the information itself, in all its activities and processes.

In summary, this **Information Security Policy** is aimed at pursuing the following objectives:

1) The organization has full knowledge of the information managed and evaluates its respective criticality, in order to design and implement adequate levels of protection;
2) Access to information occurs in a secure and adequate manner to prevent any unauthorized processing or processing carried out without the necessary access rights;
3) The internal staff and those of third parties who contribute to the processing of the information are aware and adequately trained with respect to the problems relating to the security of the same and adopt procedures aimed at observing adequate levels of protection;
4) Any anomalies, incidents or vulnerabilities having repercussions on the information system, services and corporate security levels are promptly detected and adequately treated, through efficient prevention, communication and reaction systems, in order to minimize the impact on the business, and in particular on the security and availability of services and information;
5) Corporate "business continuity" and "disaster recovery", through the application of defined and periodically tested security procedures;
6) Physical access to company premises occurs exclusively by authorized personnel, to guarantee the safety of the areas and the assets stored therein;
7) Compliance with legal requirements and compliance with security commitments set out in contracts with third parties;
8) The processing of personal data, both in cases in which Vigel operates as Data Controller and in cases in which it operates on behalf of third parties as Data Processor, takes place in compliance with the European Regulation on the Protection of Personal Data (GDPR 679/2016).

This **Information Security Policy** is periodically subjected to monitoring and possible revision through a review process by the Management, to ensure its adequacy and promote its continuous improvement, and is shared with the organization, third parties and customers, through the methods described above.

To achieve the principles and objectives identified above, Vigel undertakes to implement organizational and operational measures aimed at guaranteeing:

1) The **confidentiality** of the information processed, archived and transmitted, through the timely definition of internal responsibilities and operational procedures for the management of the services and information connected to them and by implementing timely control of physical and logical access to electronic and paper archives, limited exclusively to authorized personnel only;
2) The **integrity** of the information, applying backup and "disaster recovery" procedures and restricting physical and logical access to the information to authorized personnel only;

3) The **availability** of information through the timely identification of roles, company functions and related access rights to the information and assets necessary for carrying out internal and external company processes;

4) That in general all access, whether physical or digital, is authorised, controlled and monitored on the basis of the following criteria:
   a) access is authorized to authorized personnel only for the information strictly necessary for carrying out their activities (principle of minimum knowledge or need to know);
   b) access is authorized to authorized personnel only for information relating to the specific activities carried out;
   c) access to the ICT infrastructure and physical spaces is permitted only to authorized personnel in line with the company policy;

5) That employees, suppliers, partners, contractors and any other third party involved in the processing of information falling within the scope of the Information Security Management System are aware of their role and the impact of their actions on information security, and consequently accept the obligations and responsibilities pertaining to them, in order to protect the information, assets and resources of the organisation;

6) That human resources are informed about the principles set out in this Policy and adequately trained and trained with respect to the work procedures that impact the secure management of information;

7) That the processing of information, activities, resources and solutions relating to the protection of the organization's own information or managed by the same on behalf of its customers comply with the applicable legal, technical or regulatory standards of a mandatory, contractual or voluntary nature;

8) That every activity and resource of the organization or entrusted by it to third parties, as well as every information pertaining to the scope of the ISMS, is protected against threats relating to confidentiality, integrity and availability, in proportion to their value and in compliance with current regulations;

9) That all Vigel staff are responsible for the obligation to:
   (a) comply with the legal and regulatory provisions in force, of a mandatory, contractual and voluntary nature applicable within the scope of the ISMS; (b) protect the intellectual property, confidentiality, integrity and availability of information managed directly by Vigel or entrusted to third parties; (c) take care of Vigel's physical assets, systems and resources; (d) safeguard and appropriately manage all information and data relating to the activities within its competence; (e) contact the Management, the Information Security Management Committee and/or other competent authorities in the event of actual or suspected security breaches; (f) report any need for changes or additions to the procedures relating to information security management.

Compatibly with their roles and related responsibilities relating to information security management, each person must also:
(g) ensure compliance with this Policy, requirements, standards and/or established procedures; (h) identify and define access rights to assets according to their specific activities and responsibilities; (i) formally request third parties to comply with confidentiality agreements; (l) operate in compliance with the risk levels that have been defined for your area of relevance.

All personnel assigned specific responsibilities in information security management also have the duty to: (m) implement security based on Vigel policies; (n) ensure and monitor compliance with this Policy, the relevant requirements, standards and procedures within the scope of the ISMS; (o) monitor company assets and adequately protect them according to applicable technical and legal regulations; (p) apply rules, functions, tools, objects and controls that are consistent and functional to the purposes of the organization and which guarantee compliance with the requirements of the ISMS; (q) ensure that Vigel personnel and third parties are informed and trained on the Policy, requirements, standards and/or procedures for managing information security, as well as made aware of the consequences of failure to comply with the Policy and the requirements established in these areas; (r) adopt adequate measures to ensure control over aspects that impact information security; (s) contain the level of risk in the relevant areas; (t) keep active the measures to be adopted in the event of accidents resulting from the occurrence of anomalous and emergency conditions, and activate the business continuity plans envisaged by the ISMS.

Furthermore, third parties who directly or indirectly manage the sensitive assets of Vigel and its customers are obliged, in carrying out these processes and activities, to:
(u) formalize its commitment to confidentiality and non-disclosure of information processed in the areas of competence; (v) protect the physical and intellectual resources and information they may access in carrying out assigned activities; (z) guarantee full compliance with the provisions of the ISMS.

The President of the Board of Directors