IT Security Policy

Our approach to Information Technology (IT) Security

The F.I.L.A. Group is one of the leading global enterprises devoted to the research, design, manufacture, and sale of tools for creative expression. The Group designs, makes and packages tools and supports for drawing, colouring and painting, modelling, for use by children, youths and adults. Our product range includes more than 25 well-known brands and thousands of products sold on all continents.

We are engaged to a responsible behavior towards all our relevant stakeholders in operating business, combining respect of people, natural environment, and communities, and sustainability is therefore embedded with our Purpose, Vision, Mission, Values set out in our Ethics Code, and day-to-day operations.

This policy, together with our Ethics Code and the Corporate Governance Model, should be adopted by all Group companies and form part of the Group Organization, Management and Control Model, in accordance with the principles and objectives of the Organization, Management and Control Model as per Italian Legislative Decree 231/2001.

The Group protects its corporate assets at the highest level of its technical capabilities and available resources, broken down into the following fundamental elements: people, assets (assets) and information. The necessary condition for the performance of all activities of the F.I.LA. Group is the protection of the information managed by means of criteria, measures and security controls proportional to the risks and value of the information itself.

The IT Security of the F.I.L.A. Group is a fundamental requirement to ensure the reliability of the information processed, as well as the effectiveness and efficiency of the services provided by the Group. The IT Security has as its primary objective the protection of information, personal data and digital preservation and the elements through which the data are managed from all threats, be they organizational or technological, internal or external, accidental or intentional, guaranteeing their confidentiality, integrity and availability. and compliance with current applicable legislation.

We are committed to IT Security, which means both to protecting “assets” such as a site, a computer or a car, against cyber threats, and at the same time to minimizing the impact in the case of vulnerabilities that exceed the defenses implemented.

At F.I.L.A. Group the IT Security objectives can be summarized as follows:

- Confidentiality, i.e. ensuring the prevention of abusive or unauthorized access to information, services and systems
- Integrity, meaning ensuring that information has not been altered by accident or abuse
- **Security**: the information must be maintained and kept secure from any possible external threat, either perpetrated physically or logically.
- Availability, or ensuring access to information and network services by the staff in charge in relation to work needs
- Consistency, i.e. to check that there are tools that allow us to understand if what we expect really happens
- Control, i.e. having the ability to regulate access to the data system and to limit access and partition users by groups, functionalities, etc.
- Supervision of the operations that are carried out, i.e. checks or audits.

The lack of an adequate level of data security, in terms of Confidentiality, Availability and Integrity, can have as consequences the loss of competitive advantage, image, customers, turnover and a consequent significant financial loss. To all this we must also add the risk of incurring penalties linked to violations of the regulations in force.

Therefore, the security of the information system is obtained by implementing a series of adequate security measures, or procedures, technical mechanisms or practices that reduce the risks to which the information assets are exposed.

We direct our activities to comply with current legislation, with particular reference to applicable Codes regarding the protection of personal data in all the countries where we operate, not only in order to avoid the risk of company involvement, but above all to guarantee an adequate level of security of personal data of the Group and its information system.

We are committed to maintaining the highest possible ethical standards and to complying with all applicable laws in all countries in which we do business. We firmly believe to have the responsibility to operate in compliance with the rules

of the countries where we have a presence, distinguishing ourselves as an enterprise capable of exporting the values that permeate our actions, by promoting them in the communities where we operate.

Scope of this Policy

This Policy applies to F.I.L.A. S.p.A., its subsidiaries, the entities in which it holds a majority interest, and the facilities that it manages. We are committed to working with and encouraging our business partners to uphold the principles in this Policy and to adopt similar policies within their businesses.

Locally each company should adopt more stringent rules and procedures, as needed and in accordance with local laws and regulations. While conducting its management, coordination and supervision activities, F.I.L.A. S.p.A. respects management autonomy of each affiliate within its Group, managing and controlling the overall business, as per legitimate interests of majority and minority shareholders, considering confidentiality requirements and local applicable laws.

We firmly believe to have the responsibility to operate in compliance with the rules of the countries where we have a presence, distinguishing ourselves as an enterprise capable of exporting the Values that permeate our actions, by promoting them in the communities where we operate. The purpose of this Policy is to provide guidance to F.I.L.A.'s directors, officers, employees, agents, consultants, intermediaries, controlled joint ventures, and other third-party representatives to ensure compliance with applicable regulation and our Values and Policies.

The F.I.L.A. Group is committed to a continuous improvement of its policies and its programs, facilitating the adoption at local level of all procedures, rules, and instructions needed to have the principles set in this Policy applicable and monitored, in order to make an impact. By adopting this Policy, we believe to contribute to a better condition of existing and of next generations, providing tools for a better quality of life.

General principles

In our strategies and operations, we consider the following principles relating to IT Security

- **Business information systems**: employees and internal collaborators are provided with all the tools necessary to carry out the tasks assigned. Tools and software applications provided are work tools and must be used for these purposes: the data present within the work tools (including e-mail systems and local/network file systems, as well as data storage locations in the Cloud) are considered corporate data and as such owned by the Company. Consequently, the company can have complete access to them and users will not be able to have expectations of privacy with respect to the information sent, received or stored. Improper uses of Company systems include processing, transmission, retrieval, access, display, storage, printing and in general the dissemination of fraudulent, harassing, threatening, illegal materials and data. , racist, of sexual orientation, obscene, intimidating, defamatory or otherwise not congruent with professional behavior. Therefore, no data of this kind must be present on the F.I.L.A. network, on Personal Computers, within the applications (such as e-mail, Intranet portals, etc.). Furthermore, users of company systems must not use the infrastructures to do business, sell products, or for any other commercial activity other than those expressly envisaged by the company management
- **Access to information:** Access to information by each individual user must be limited to only the information they need for the performance of their duties (“need to know” principle). The disclosure and transmission of information internally, as well as externally, must be based on the same principle. FILA Group will enforce this policy setting up proper user profiles and rights, to restrict the ability to access information accordingly with the principle stated above. Sharing user access information, such as accounts and password, with other employees or individuals, not keeping them properly and safely stored or not updating access information regularly and accordingly with IT Security Operational Guidelines, are considered improper use of Company Systems and Information and, as such, sanctioned.
- **Personnel and security**: The F.I.L.A. Group plans and carries out training and information activities aimed at personnel, with a focus on information security and the correct use of Company equipment. Personnel must be required to ensure a minimum level of safety for assigned equipment. The theft, damage or loss of work tools must be promptly reported. The staff (including consultants and external collaborators) must sign confidentiality clauses.
- **Cyber incidents and anomalies**: All employees are required to detect and notify whoever is responsible for any problems related to Group and Company safety. All employees are required and expected to carry on daily business and use Company Systems (with special reference, but not limited to Collaboration Tools like E-Mail, Microsoft Teams, Microsoft Sharepoint) with proper care and attention to suspicious messages, attachments,

requests for contact.

- **Physical security**: Access to buildings and premises relevant to the protection of assets must take place only after identification of the authorized parties. The identification and design of physical security countermeasures must consider both the possibility of physical threats and the applicable legislation. The maintenance of the equipment must be performed in accordance with the manufacturer's instructions or with documented procedures to ensure service availability and integrity
- **IT Security**: The identification and design of IT Security countermeasures must consider both the possibility of internal and external unauthorized access attempts, as well as the applicable legislation and any other relevant constraints. Users must not exploit any weaknesses or deficiencies of the IT Security system to damage systems or data, obtain resources for which they are not authorized, steal resources from other users or have access to systems for which they do not have the necessary authorizations. On the contrary, users must take care to communicate to the system administrator, in writing, any malfunction of the system that may suggest the possible loss of stability or reliability of the same
- **Checks**: The information systems must be periodically checked as well as the application of operating procedures. The personnel in charge who work in the IT division is authorized to carry out interventions in the Group IT system aimed at guaranteeing the safety and protection of the system itself, as well as for further technical and / or maintenance reasons (e.g. updating / replacement / implementation of programs, hardware maintenance etc.).

The security checks to be carried out to protect the IT resources that make up its assets are achieved through:

- implementation and compliance with policies in all organizational, procedural and technological areas in a homogeneous way with respect to the defined objectives
- the adequate assignment of tasks and responsibilities within the Group for the implementation of policies
- verification (as part of the IT risk analysis) of the level of effectiveness of the measures implemented, also resorting to periodic vulnerability assessment run by external, independent parties.

Failure to comply with the provisions of this IT Security Policy will be subject to disciplinary sanctions as appropriate.

F.I.L.A.'s Top Management has a strategic role in the full implementation of this Policy ensuring the involvement of all personnel and of those who collaborate with F.I.L.A. and the consistency of their behavior with the values embodied in this Policy.

This Policy is communicated within the organization and made available online to all stakeholders on the web site www.filagroup.it.

F.I.L.A. encourages anyone who becomes aware of facts or behaviors contrary to the Company's Code of Ethics, policies and internal rules, laws or regulations, to make a report in the utmost confidentiality. Assuring confidentiality of the whistleblower's identity, F.I.L.A. offers the following channels to file a report:

- E-mail: whistleblowing.fila@gmail.com
- Mail to: odv@fila.it Organismo di Vigilanza, F.I.L.A. Fabbrica Italiana Lapis ed Affini S.p.A. Via XXV Aprile, 5 20016 Pero (MI).

October 2021

GROUP CEO – Massimo Candela