To the kind attention
of internal personnel, suppliers, clients and customers

The policy that Gen Set S.p.A. states about security of personal and business information is certainly aimed at achieving legislative compliance but not only; the strategic and evolutionary perspective of the Management is intended to overcome the strict regulatory aspects to meet the best existing security management information standards.
This policy is implemented through:

- technical and structural means;
- management means; manuals, procedures, agreements with customers, suppliers and other stakeholders;
- awareness and information to all stakeholders.

Applicability
Gen Set S.p.A. staff and third parties who, some way, interact with data processing have to fully comply with this policy.

Purpose
The Company considers that the protection of its own information assets and stakeholders is a strategic value; it applies adequate protection to personal data and information relating to suppliers, customers, employees, shareholders, public authorities and government; The aim is to protect them against any threat, either internal or external, intentional or accidental, that may put at risk the specific purposes the information assets were created for.

Management commitment

- The implementation of this policy is necessary to ensure that adequate protection is implemented **for personal and strategic** information and data, in particular linked to the requirements of GDPR. 679/2016 and that personal data security requirements are fulfilled.

Therefore, our Management expresses his commitment to ensure:

- **Confidentiality**: it means to ensure that unauthorized access and disclosure are avoided,
- **integrity** to maintain the accuracy and completeness of the information by ensuring that it has not been modified by unauthorized ones and,
- **availability,** to ensure that authorized users can actually access information assets on an ongoing basis.

Information security milestones and goals

- Keep Management risk at an acceptable level through design, implementation and management of a security system,
- Ensuring compliance with laws and regulations valid in our country or expressly requested by our foreign customers,
- Reach and maintain compliance with GDPR and subsequent changes and revisions.

EXPECTED BEHAVIOR

All staff and suppliers must conform their behaviors to the established procedures for information security and particularly become aware that:

- personal data, once made available by the data subject, remain his property and that every treatment must be based on laws remaining closely adhered to the legal basis and the purposes for which the data subjects made them available,
- personal data must be adequately protected to ensure its Confidentiality, Availability and Integrity
- any personal data exceeding the contractual purposes must not be required and, where made available with no use, immediately deleted,
- any personal data that has finished its purpose must be deleted (but in case of legal obligations or legitimate interests of its own or third parties).

Everyone is asked

- to comply with the internal regulations for using personal information,

- collaborate on improving data protection system,
- inform the person responsible of any data breach,
- report any vulnerability aspect identified,
- avoid any action, which, intentionally or negligently, can cause damage to The Company which, in any case, will be prosecuted as appropriate.

This invitation is also extended to customers.

IMPLEMENTATION STRATEGY

- **appropriate protection measures**

Company provides and implements appropriate protection measures, commensurate with the value of the information and the seriousness of the threat: it is guaranteed that all information security breaches and, if possible, its weaknesses are taken into consideration and mitigate.

- **Emergency preparation**

The Company is prepared to respond to any extraordinary reasonably expected event as prepares to respond promptly.

- **Training and awareness**

The risks of breach of data integrity, confidentiality and availability are often inherent in the unaware behavior of operators who expose the company's information assets to serious but avoidable risks with appropriate methods, subject to specific training sessions: on the other side where attacks arise from deliberate actions, the training focus on the seriousness of the consequences for those who cause a potentially harmful event of the company's assets.

- **Management and operational policies**

To support this policy, Top Management has defined procedures related to physical access security, control of access to information, training, employee code of practice, rule book for using company's computer network, *back up* and *restore* procedures , management, instrumentation use, malware control, firewall, network control, intrusion detection, business plans continuity.

- **Review**

This policy is regularly reviewed and upgraded to ensure that it keeps fitting the purposes of our company and the expectations of our users.

Conclusive note

This policy is communicated to all staff and made available to stakeholders through on the Company's website.

Gen Set Director
Luigi Foresti