**Policy**

**Information Security Management (standard ISO 27001 and ISO 27701)**

Dear Customer,

Dear Collaborator,

Dear Supplier,

Dear Business Partner,

Dear Consortium Member,

We have built our success on our ability to meet and exceed our customers' expectations by helping them in the difficult task of ensuring the compliance of their business with complex and delicate binding, regulatory, technical and contractual requirements.

Protecting the information of our customers is mandatory for us. We therefore ask the same commitment to all our stakeholders (suppliers, collaborators, business partners, consortium members).

**Our business context**

We are a joint stock cooperative consortium. Our consortium members (shareholders) are represented by micro and small medium enterprises, each of which represents a Subject Matter Expert.

Our mission is to provide professional services to businesses (consultancy, training, audit and business assurance). We support our customers in the delicate task of ensuring compliance of their business with mandatory and regulatory, technical, contractual and internal requirements.

In the provision of our services, we therefore treat various information owned by our customers, some of which are classified as confidential. We also process personal data of natural persons who operate on behalf of our clients' Organizations.

**Our commitment for Information Security**

We are committed to ensuring the full and systematic compliance of all the services provided to our customers with the mandatory, regulatory, contractual and technical requirements applicable for information security.

We are committed to ensuring the full and systematic compliance of all services provided to our customers with the mandatory, regulatory, contractual, technical requirements applicable to information security, including information classified as personal data in accordance with the GDPR.

We have adopted a specific policy for the protection of personal data in accordance with the GDPR. This policy is an integral part of this policy and is available on our website www.minervagroupservice.com

This policy is communicated to all our stakeholders and is available on our website [www.minervagroupservice.com](http://www.minervagroupservice.com)

**Our Information Security Objectives**

**Our commitment**

We are committed to pursuing information security and personal data protection objectives in accordance with the applicable mandatory requirements.

**Our confidentiality, integrity, availability objectives**

Our objectives for information security are expressed in objectives of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

Confidentiality objectives: the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity objectives: the property of safeguarding the accuracy and completeness of assets.

Availability objectives: the property of being accessible and usable upon demand by an authorized entity. Availability objectives include resilience objectives. We have adopted a specific policy for business continuity. This policy is an integral part of this policy and is available on our website www.minervagroupservice.com

**Our control objectives**

In order to pursue our information security objectives, we plan and pursue operational control objectives for the treatment of information security risks.

**Our Information Security Management System**

In order to pursue our information security objectives, we have adopted an information security management system compliant with the ISO 27001 standard.

Our Information Security Management System has been integrated into the more general corporate management system and has been planned in order to consider aspects of Governance and Internal Control System, Risk Management aspects (with reference to the guidelines of the ISO 31000 standard) and Compliance aspects (with reference to the guidelines of the ISO 19600 standard).

We are committed to adapting and continuously improving our Information Security Management System and to make aware and train our stakeholders on its correct application.

**The penalties**

Violations of this policy and of the Information Security Management System imply the application of disciplinary measures, including the termination of existing contractual relationships and the forfeiture of the status of consortium member.

**Our contact channels**

For any report of vulnerability, threat, improvement, non-conformities, incident, violation, data breach you can contact our Information Security Manager at the following email address: pmo@minervagroupservice.it

We are committed to ensuring the confidentiality of reports and to prohibit any form of retaliation against reporting agents.

*Minerva Group Service*