nCORE	**Information Security Policy** **(see Chapter 5.2 - ISO 27001:2017)**	**DOC002 - Rev 3.0** release 27-05-2022 Written by: Privacy Champion Approved by: Management Document Type: Public

Information security and protection are key requisites for the achievement of the business goals of our company. The requirements for information security are consistent with the company's objectives and the purpose of the Information Security Management System (ISMS) is to have information shared, operations correctly performed and any risks related to information reduced to acceptable levels. In consideration of this, the performance of company activities must always ensure adequate levels of availability, integrity and confidentiality of information through an established "Information Security Management System" (hereinafter also referred to as SGSI, i.e. the Italian acronym for ISMS) in line with the requirements expected by the company's stakeholders and in compliance with the applicable regulations in force from time to time.

In particular, the system is applied to "***Design, development and assistance of applications related to the automation of personnel selection***";

SGSI general objectives, pursued thanks to the management's commitment, are the following:

- demonstrate to stakeholders its ability to provide secure products/services on a regular basis, maximising business objectives;
- minimize the risk of loss and/or unavailability of customer data by planning and managing activities to ensure continuity of service;
- carry out a continuous and adequate risk analysis that constantly examines the vulnerabilities and threats associated with the activities to which the system applies;
- comply with applicable laws and regulations, contractual requirements, company rules and procedures;
- promote collaboration, understanding and awareness of the ISMS by strategic providers;
- comply with the principles and controls established by ISO 27001, ISO 27017 and ISO 27018, or other standards/regulations governing the business activities the company is involved in, including, in particular, regulations relating to Privacy and Personal Data Security (GDPR);
- Promoting continuous improvement by monitoring the functioning of the management system set up and through the achievement of set objectives.

In particular, for the implementation and delivery of cloud services, in accordance with ISO 27017, nCore is committed to adopting security requirements that take into account risks from internal staff, secure multi-tenancy (infrastructure sharing) management, access to cloud assets by service providers' staff, access control (in particular administrators), communications to stakeholders when infrastructure changes occur, security of virtualisation systems, data protection and access in the cloud, cloud account lifecycle management, data breach communication and information sharing guidelines to support investigation and forensic activities and ongoing security on the physical location of data in cloud servers.

Furthermore, the company is constantly engaged in the protection of personal data, especially with regard to data related to its customers. With reference to the latter and in accordance with ISO 27018 and applicable privacy legislation (GDPR), the company is a Data Processor, declaring its status and the resulting obligations in contracts with customers. These obligations are also set out in the appointment as Data Processor.

The company is involved in reporting any incidents found and any weaknesses identified in the SGSI and is engaged in supporting the implementation, performance, periodic review and continuous improvement of the SGSI.

The Management is committed to reach the goals set by this policy, using the necessary tools and resources.