Milan, March 24th, 2022

Subject: System management policy

The Information Security Management System has as its primary objective the protection of SupplHi's information assets and the maintenance of the requirements of confidentiality, integrity and availability of information.

The achievement of adequate levels of security allows the company to mitigate and counteract losses and damages that may have an impact on people, on the company's image and reputation, on economic and financial aspects, as well as allowing compliance with the contractual and legislative context in force regarding the protection of information.

In this context, the Company identifies the following objectives for this manual:

- To adopt and implement recognized principles and best practices to ensure Information Security and promote the acquisition of certifications of compliance with reference standards;
- To identify roles and responsibilities to be assigned to its staff, regardless of the hierarchical level occupied, also involving third parties who perform key tasks if present;
- To assign the resources necessary to ensure the use of suitable measures for aspects concerning physical, logical and organizational security;
- To identify, document and apply rules governing how information, goods and tools are used;
- To develop an awareness program for staff, through periodic information and training sessions;
- To prepare adequate reaction and management measures in case of the occurrence of incidents that may compromise information security and normal operation;
- To commit to carrying out a continuous process of improvement and evolution of the Information Security Management System, planning, executing, verifying and continuously implementing measures and expedients to combat potential events that may compromise the company's information assets

Security is seen as a set of cyclical processes at every level and the ISO/IEC 27001:2013 standard focuses on safety management aspects, defining a catalog of security countermeasures at a level that can be applied to different environments, systems and procedures within any type of company.

The Company has also decided to extend its ISMS to ISO/IEC 27017 and ISO/IEC 27018 with regard to the protection of information in Cloud. The need arises from the need to respond to the multiple requests coming from outside and inside the organization, including the need to respond to what is defined by the GDPR regarding the protection of personal data of customers and employees.

The main steps to manage information security according to the standard can be effectively summarized through the PDCA (Plan, Do, Check, Act) cyclical paradigm.