PIS 009

POLICY FOR THE SECURITY OF THE INFORMATION IN RELATIONS WITH SUPPLIERS

ISSUED	08/02/2019	Ahanonu Chidi			
APPROVED BY THE DIRECTION	08/02/2019	Gianfranco ROATI			
CLASSIFICATION DOCUMENT		☒	PUBLIC	☐	CONFIDENTIAL
		☐	INTERNAL USE	☐	RESTRICTED

INDEX OF REVISIONS

REVISIONS	EMESSION'S DATE	MAJOR CHANGES
00	08/02/2019	First issue
01	09/10/2019	

SUMMARY

1 NORMATIVE REQUIREMENTS

- ISO 27001
- GDP Regulation (EU) No. 2016/679

2 AIM OF THE DOCUMENT

In order to mitigate the risks associated with access to the Insis Spa assets by its suppliers, it has been prepared this policy that defines the security requirements of the information.

3 POLICY

3.1 POLICY FOR INFORMATION SECURITY

Insis implements and maintains a quality management system of secure information by following the requirements specified in the UNI CEI EN ISO / IEC 27001: 2017, so as to ensure:

1. Confidentiality - Information only accessible to the persons and / or duly authorized processes;
2. Integrity - safeguarding the consistency of the information from unauthorized changes;
3. Availability - ensuring that the processes and tools for managing data are safe and tested;
4. Authenticity - reliable source of information;
5. Privacy - assurance of protection and control of personal data.

The lack of adequate levels of security of information can lead to damage of the INSIS, failure of customer satisfaction, the risk of incurring sanctions linked to violation of regulations as well as economic damages, financial and company image and the underlying chain.

The commitment of Insis direction, which is required by also applied by the supplier, is implemented through the definition of an adequate organizational structure to:

- establish corporate roles and responsibilities for the development and maintenance of Information Security;
- check that the policy for the Safety of Information is integrated in all business processes and procedures and controls are effectively and consistently developed;
- monitor the exposure to threats to information security;
- enable programs to spread awareness and culture on information security.
- The general objectives of Insis Spa, that providers Insis will in turn pursue, are thus:
- ensuring the highest standards, optimizing and rationing processes and business tools;
- ensure the effectiveness of the procedures and controls for Information Security;
- Insis guarantee of satisfaction in relation to the amount of information.

The supplier must ensure that all staff must work to achieve the security objectives in information management and should use the most appropriate technologies to ensure compliance with this policy

3.2 SECURITY REQUIREMENTS OF INFORMATION FOR SUPPLIERS

The supplier undertakes to comply with the guidelines of the previous policy for Information Security

The drawings exchange or other documents referred to in the PO must be:

- For source documents (drawings, specifications, etc.), or confidential documents protected by IPR, to FTP the Insis or by e-mail as attachments in encrypted folders with password; in both cases, it is up to Insis provide, through different channels, references and credentials to the person named in the NDA (or authorized to exchange data)
- Via e-mail for all other documents such as timelines, non-confidential information etc.

The people who will be able to receive information from Insis, except those public, are those indicated in the NDA if signed by both parties or otherwise authorized by both parties

The supplier undertakes to implement solutions to protect against fraudulent activity, contractual disputes, as disclosure and unauthorized modifications

In case you need to access to the assets of Insis by supplier, it will have to be authorized in advance and informed of the mode of utilization, which must strictly abide by and be subject to the control under Insis policies

For suppliers associated with the services and products in the supply chain for ICT, the supplier undertakes to comply with the requirements Insis to address the risks related to information security, requiring advance to Insis copy of the Policies and Procedures Applicable.