Internal distribution SNN Group	
Code: SNN-POL-9.0.1	Revision: 0

TITLE **SPECIFIC CORPORATE POLICY ON PHYSICAL PROTECTION AND THE PROTECTION OF CLASSIFIED INFORMATION WITHIN THE SNN GROUP**

PURPOSE The goal of the physical protection and the protection of classified information policy within the SNN group is to implement and maintain an unified system of coordination of physical protection, classified information and critical infrastructure processes, integrating the subsidiaries by ensuring consistent adherence to international norms and recommendations, national legislation, regulatory requirements, internal policies and single group-wide standards. The policy sets the standards and accountability for meeting the commitment.

APPLICATION All SNN Group officers

REQUIREMENTS **Physical Protection**

- Development and implementation of security, guarding and physical protection framework policies, in a coherent and consolidated structure at the level of SNN Group's companies (as regulated by Law no. 111/1996 and Law no. 333/2003) by:
  - elaboration of Physical Protection Risk Analyses;
  - elaboration of the Security Plan;
  - integrated management of the physical protection system regarding controlled access, burglar alarm and video system;
  - physical protection of classified information.
- Implementing, maintaining and analysing the physical protection system at SNN group level by:
  - Developing and issuing policies, programs, procedures, guidelines and work instructions with uniform requirements at group level;
  - Advice on aligning access procedures with the organizational structure;
  - Compliance with legal compliance requirements regarding personnel access to sites or premises, vital, protected or security areas (security rooms);
  - Approval of changes or updates of specific procedures, methodologies and forms.
- Providing the function by supplying resources and methodological advice in the realization of missions for the implementation of technical systems for new projects, elaboration and implementation of specific working procedures;
- Ensuring a training and education program on the areas under coordination as well as providing and endorsing support materials for mandatory and periodic training in the field of physical protection;
- Implementing physical protection policy and procedures and work methodologies, in defining objectives and identifying risks;
- Coordinating the planning of activities for the implementation of the strategic projects, the set of common objectives as well as the implementation of the measures provided in the Investment Plan adopted according to the development strategy of SNN;
- Consolidation of objectives, data and activity specific information required for group reporting (MRM) or required by legislation;
- Coordinating maintenance plans and programs and monitoring their implementation;
- Obtaining/renewing competences, certifications, endorsements and authorizations of PP staff;
- Equipment/investment plans/programs to maintain the physical protection system at the projected level of operation.

Classified Information - requirements for Group companies

- Security Structure Assurance;
- Implementation of the guidelines on the protection of classified information in SNN;
- Ensuring the protection of classified information by updating the measures laid down in the PPLCI (Program to Prevent the Leakage of Classified Information);
- Providing measures to counter leaks of classified information;
- Obtaining / renewing certificates and authorizations for access to state secret information;
- Maintaining and upgrading the INFOSEC system;
- Ensuring compliance with legal compliance requirements regarding personnel access to security areas (security rooms);
- Providing training through CI protection courses and questionnaires;
- Human Resources Management (Classified Information Offices);
- Organization of Classified Information Offices;
- Management of classified information;
- Protection of classified information;
- Granting the right of access to classified information;
- Industrial safety;
- Protection of sources generating classified information -INFOSEC.

Critical infrastructure - requirements for Group companies

- Identification and designation of NCI/ECI (National Critical Infrastructure/European Critical Infrastructure);
- Appointing the SLO (Critical Infrastructure Security Liaison Officer) - the contact person for reporting security incidents regarding the Critical Infrastructure SLO ME and completing the incident reporting forms.
- At SNN GROUP level there is a pyramidal reporting structure for the NCI/ECI: Central level SLO (liaises with the relevant authorities), SLO NPP and SLO NFP - through SLO SNN;
- Preparation of the OSP (Operator Security Plan) - where NCI/ECI are designated;
- Drafting the Exercise Plan according to the OSP;
- Drafting Exercise Analysis Reports;
- Drafting Security Incident Sheets;

Special Issues (preparing the Company for Mobilization)

- Drawing up function-specific documents.

General

- Governance structure: The group's Physical Protection, Classified Information Protection, Critical Infrastructure Protection and Special Issues programs shall have a centralized governance structure with a group-wide coordinating function responsible for establishing policies, standards and guidelines. This central oversight ensures coherence and coordination between the different entities;
- Communication and training: The group's Physical Protection, Classified Information Protection, Critical Infrastructure Protection, and Special Issues programs require effective communication and training mechanisms to disseminate policies and compliance guidelines to as many entities within the group as possible. These programs involve developing training materials, conducting workshops and implementing communication channels that reach

employees and stakeholders;

- Risk assessment: Risk assessment approaches are different for each group security program and also different and tailored for each branch or subsidiary. Group security programs usually require a comprehensive risk assessment process that takes into account the risks associated with each entity and the overall risks faced by the group as a whole, with legal requirements for each. This complicates "group policy" efforts and the efficient allocation of resources, but at the same time puts order into the wording and approach to these processes;
- Reporting and monitoring: Reporting and monitoring mechanisms within group security programs often involve the consolidation of data and information to provide a holistic view of compliance performance at the group level. This facilitates oversight, tracking key values and identifying emerging trends or issues.

ASSOCIATED PROCEDURES	N/A		
EFFECTIVE DATE	On the date of approval	APPROVAL	SNN Board of Directors