Internal distribution SNN Group	
Code: SNN-POL-8.0.1	Revision: 0

TITLE **SPECIFIC CORPORATE POLICY ON IT&C AND CYBERSECURITY WITHIN THE SNN GROUP**

PURPOSE The purpose of the policy on IT&C and Cyber Security within the SNN Group is to establish the necessary framework for the implementation of process governance principles at SNN Group level that will ensure the efficient implementation, evaluation, prioritization and funding of IT and cybersecurity services, their monitoring and implementation and the evaluation of the results obtained. This policy also defines unitary principles applicable to the SNN group for IT services and cybersecurity.

APPLICATION All SNN Group officers

REQUIREMENTS

- IT&C governance and cybersecurity is an integral part of the SNN Group's code of governance and consists of principles to be adopted by each of the member organizations and ensures that IT&C and cybersecurity processes support the group's strategy and objectives;
- The goal of IT&C governance and cybersecurity is to coordinate efforts and ensure that the performance of these two areas meets the following objectives:
  - Alignment of digitization strategies and objectives and thus major projects;
  - Maximizing the added value of using IT&C solutions;
  - Responsible use of IT resources;
  - Proper cyber risk management.
- IT&C governance and cybersecurity at SNN group level ensure the fulfilment of common IT objectives and the mitigation of cyber risks so that the two areas deliver value to support the group's development. This governance policy drives the strategic alignment between IT&C and cybersecurity teams and processes across subsidiaries and SNN;
- The IT&C governance and cybersecurity policy defines a set of 7 SNN group core principles for the development and implementation of an IT&C governance and cybersecurity framework. These principles incorporate COBIT, ITIL and ISO standards and are based on the premise that IT must deliver the services the business needs to achieve its objectives;
- The seven core principles for SNN group governance are:
  - Linking IT&C and cybersecurity objectives with those of the SNN group and in particular with those of the subsidiaries;
  - Ensuring IT&C and cybersecurity performance through dedicated, properly sized and prepared organizational structures that can run the specific processes. They are constantly evaluated and deficiencies are responsibly addressed;
  - The contracting of IT&C and cybersecurity services and systems is done through rigorous needs assessment, selection and proper vetting of partners and suppliers;
  - Suppliers' performance management is realized based on contractual conditions;
  - Business continuity/disaster recovery is considered through requirements and practices implemented in technology and processes to address potential incidents that may affect both the SNN group and subsidiaries;
  - Ensuring the necessary measures for data confidentiality, integrity, availability and cybersecurity;
  - Compliance with the applicable legal and regulatory framework is ensured and compliance is continuously monitored.
- The IT&C governance and cybersecurity framework within the SNN group is defined as

follows:

- SNN has assumed responsibility for IT&C governance and cybersecurity by ensuring the necessary governance framework without affecting the specific objectives of the subsidiaries. The SNN group's IT&C governance and cybersecurity core principles have been adopted to ensure strategic alignment and common goals. Independent assessment of the effectiveness of the IT&C governance and cybersecurity framework is carried out by internal (group audit) and external auditors (if applicable);
- Group-wide IT strategy objectives are aligned with the group strategy and opportunities to improve IT&C and cybersecurity services;
- Optimal funding is provided for the operation of IT&C and cybersecurity services, the development of new projects and costs are efficiently managed and the return on investment is measured. Where appropriate, IT&C and cybersecurity projects and initiatives are aligned/coordinated/merged, including from a procurement perspective, so that they are in the best interest of the organization as a whole;
- IT risks are identified and adequately addressed in accordance with existing group risk management practices. The SNN group and its subsidiaries ensure that it has adequate resilience mechanisms in place for disaster recovery;
- IT&C and cybersecurity services are optimally contracted, keeping essential capabilities in-house;
- Processes and procedures are in place to ensure that SNN group IT&C and cybersecurity systems are managed, maintained, replaced and decommissioned effectively and in accordance with applicable procedures;
- Providing specific infrastructure, systems and processes for cyber and information security;
- IT&C and cybersecurity operations and processes are subject to specific audits, both internal and external, in terms of business continuity, cybersecurity, procurement, etc;
- The use of environmentally sustainable IT&C systems is promoted.

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