Author: CISO
Owner: Group CFO
Reference: PM-IT-C00FP-B
Last Update: 2025.11.25
Application: NOVARES

IS (INFORMATION SECURITY) POLICY FOR PARTNERS - PUBLIC

Purpose

The objective of this information security policy is to provide the necessary controls to ensure the integrity, confidentiality and availability of information assets (CIA).

NOVARES implements an information security management system that complies with TISAX requirements, NOVARES uses the standard scope for the assessment. The scope of TISAX defines the scope of the evaluation. The assessment includes all processes, procedures and resources under the responsibility of NOVARES that are relevant to the security of protection objects and their protection objectives as defined in the assessment objectives listed on the listed sites.

All evaluation criteria listed in the listed evaluation objectives are subject to evaluation.

Confidentiality measures are designed to prevent attempts at unauthorized access to sensitive information. Data is classified according to the importance and type of damage it could suffer if it fell into the wrong hands. More or less stringent measures are implemented depending on the level of confidentiality.

For NOVARES, integrity means maintaining the consistency, accuracy and reliability of data throughout its lifecycle. Data must not be altered in transit and measures must be taken to ensure that it cannot be modified by unauthorized persons (for example, in the event of a breach of confidentiality).

Availability means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

This NOVARES Information Security Policy (ISP) for partners applies to all information

Table of contents

Directory Structure

- PM Performance Monitoring
  - ↳ PM-IT Information System
    - ↳ PM-IT-C00 ISP

1 Information Security Policies availability

This policy has been created by the CISO and approved by the CEO.
The CISO is responsible for implementation at the group level. The information security policy is available on internet for all our business partners.

Recipients of the policies should acknowledge they understand and agree to comply with the policies where applicable. NOVARES managers must communicate the ISP to business partners, joint ventures, and service providers. Information security policies must be available and communicated to business partners and suppliers, and they must be informed of any relevant updates.

2 Information

"Information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to ensure integrity, confidentiality, and availability. This Information Security Policy aims to provide the necessary controls to protect NOVARES information and information systems, and to allow their use, access, and disclosure in accordance with company interests, business strategy, applicable laws, regulations, contracts, and the current and projected information threat environment.

This applies to all information processed within the organization, regardless of its form: oral, visual, paper, digital, or physical. This includes information created by NOVARES employees or non-permanent staff (trainees, temporary workers, etc.), by service providers for NOVARES, or transmitted to NOVARES by customers or partners. Videos, audio representations, drawings, contracts, customer data, business secrets, critical business processes, know-how, patents, personal data, prototypes, and product developments are designated as information assets.

3 Security Incident

In the event of a security incident within a partner organization that could negatively impact Novares, the partner must without undue delay inform their main Novares business contact @NOVARESTEAM.COM.

Incident Management

- Security Incident Handling: Security incidents must be addressed promptly and appropriately.
- Incident Reporting: Security incidents must be reported without delay.
- Lessons Learned: Insights gained from incidents should be integrated into the continuous improvement of security practices.

Continuity Plan
The supplier must establish a continuity plan for critical IT services, including alternative communication strategies and redundancy solutions.

4 information security – Novares responsibilities

NOVARES has established an internal architecture and assigned the following levels of responsibilities to ensure the security and integrity of its information assets.

CISO Chief information security officer (contact person for information security topic)

- Write the ISP
- Define the scope of the ISP.
- Define the organization's requirements for the ISP.
- Conduct ISA Questionary, review the effectiveness of the ISP and include conclusion in the performance review.
- is charged with the design and implementation of controls to secure all information and resources in a manner acceptable to NOVARES management.
- Assess the information security risk and conduct action plan.
- ensure compliance with corporate security policies. Segregation of duties should be maintained for the performance of network and security administration activities.

5 Confidentiality Non-Disclosure Agreements (NDA) – Partners responsabilites

Responsibilities for information security must be clearly defined, documented, and assigned to business partners and suppliers.

As part of its relationships and project development, Novares requires business partners and suppliers to sign Non-Disclosure Agreements (NDAs) to protect sensitive information exchanged.

NDAs should include the parties involved, the type of information covered, the validity period, and the responsibilities of the obligated parties.

Additionally, employees of partners must be qualified and trained for their tasks in information security.

6 IT Security Measures

Novares uses encryption, firewalls, and intrusion detection systems to protect its information.

Novares has an access control and identity management policy to ensure that only authorized personnel can access sensitive information.

7 Prototype Protection

Physical and Environmental Security: supplier must implement measures such as perimeter security, intrusion monitoring, and visitor management to protect prototypes.

Awareness and Training: suppliers must implement a program on prototype protection.

8 Information Security Risk Assessment and audit

As part of its supplier panel management, Novares conducts a risk assessment regarding information security.

Risks related to external IT service providers and cooperation partners are considered in the overall information security risk assessment

In case of changes to the environment (e.g., organizational structure, location, changes to regulations), the supplier must inform Novares

Information security audits must be conducted by an independent and competent entity at regular intervals for IT partners.
Additionally, contractual obligations regarding information security must be passed on and enforced with subcontractors and cooperation partners.

9 Updates

Index	Date	Author / Contact	Modification
A	2025/04/04	X. COTHENET	Creation
B	2025.11.25	P. BIGOT	Correct confidentiality status of this document