NOVARES

IS (INFORMATION SECURITY) POLICY-FOR PARTNERS

Author: CISO
Owner: Group CFO
Reference: PM-IT-C00FP-A
Last Update: 2024.05.23
Application: NOVARES

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) is applicable to all NOVARES companies worldwide. The ISP applies to all information assets owned, contracted, leased, or operated for or by NOVARES.

Table of contents

Directory Structure

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

1 Information Security Policies (TISAX 1.1.1 information security policies availability)

This policy has been created by CISO and approved by CEO, the CISO is responsible for the implementation at group level and each site manager is responsible for the local deployment.

The information security policy is available on SMART (INTRANET) for all Novares employees.

An extract of this ISP is available for our business partner.

Recipients of the policies should be required to acknowledge they understand and agree to comply with the policies where applicable.

The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide integrity, confidentiality, and availability. The purpose of this Information Security Policy is to provide the necessary controls for the protection of information and information systems and to allow the use, access, and disclosure of NOVARES information in accordance with company interests, business strategy, applicable laws, regulations, contracts, the current and projected information threat security environment.

This applies to all information.

NOVARES expects their employees or anyone who has access to its information and resources (hereafter the user or users) to perform their duties in a responsible, professional, and ethical manner and in accordance with the law and terms of this policy as well as the IT Charter (PM-IT-D00).

All NOVARES information must have an identifiable owner responsible for the classification (public, internal, confidential, SECRET), management and protection of information. All employees are required to safeguard NOVARES information according to this policy. Employees are trained, entrusted with, and continuously responsible for, the proper use and protection of all NOVARES assets.

in case of violation of this ISP or IT Charter (PM-IT-D00), NOVARES management can temporarily or permanently disconnect any user, any company, or any establishment, to prevent any unauthorized activity in the future.
NOVARES is entitled to report any violation of the law to the competent authorities.
The attention of every user is drawn to the fact that failure to comply with the rules of this ISP may lead to disciplinary action up to and including termination of contract and/or civil or criminal penalties and that the author may be held responsible as soon as it is determined that the facts are imputable to them.

Suspected abuse of NOVARES networks and communication resources must be reported to your immediate manager. Serious abuses must be immediately reported to NOVARES CISO. If warranted, the incident will be investigated. NOVARES Human Resources must be consulted to ensure that appropriate and consistent disciplinary action is applied.

The ISP is reviewed once a year and each time if it is required by the CISO see last page for details.

2 Organization of Information Security (TISAX 1 2 1)

Information in any form processed within the organization, including, whatever their form: oral, visual, paper, digital, physical, whether this information is created by NOVARES employees or non-permanent staff (trainees, temporary workers, eg.), created for NOVARES by service providers or transmitted to NOVARES by customers or partners. Like video, and audio representations, drawing, contract, customer data, business secrets, critical business processes, know-how, patents, personal data, Prototype – product development is designated as information assets.

The supporting information assets is also included in this scope.

- The computing hardware and software systems which access and manipulate information.
- The network systems which transport information.

To guarantee CIA (confidentiality, integrity and availability) Novares define the following policies:

- Confidentiality – information classification and handling
  - PM-LI-D00 confidentiality management (for employees, suppliers and visitors)
  - SO-QS-E00 Control internal documentation.
    - SO-QS-E05 Assets list and classification
  - SO-QS-F00 Control external documentation.
  - SO-QS-G00 Maintain records.
    - SO-QS-G01 Maintain records template.

- PM-IT-D00 IT Charter
- PM-IT-AE00 Hardening [EN]

- IT Accounts and privileges
  - PM-IT-E00 IT Accounts management (AD, third party) [EN], [FR], [CN], [CZ], [DE], [ES], [IT], [RS], [TR], [RO]
  - PM-IT-N00 Password Policy
  - PM-IT-M00 IT Accounts and privilege review
  - PM-IT-E02 SAP Financial consolidation FC user access - INTERNAL [EN]
  - PM-IT-F00 User SAP access management [EN]
  - PM-IT-B00 IT Software applications change request [EN]

- IT service provider management
  - PM-IT-AF00 IT Safety insurance plan [EN]

- Supporting assets Lifecycle
  - PM-IT-H00 Assets lifecycle management [EN]

- Network Security
  - PM-IT-X00 Network management [EN]
  - PM-IT-AG00 Remote access [EN]

- information security incident management
  - PM-IT-A00-1 Incident Management [EN], [FR], [CN], [CZ], [DE], [ES], [IT], [RS], [TR], [RO]
  - PM-IT-A00-2 Incident Management (IS Security) [EN]
  - PM-IT-A00-3 Event logging [EN]
  - PM-IT-G00 IT Backups policy [EN], [ES]

- Cryptography
  - PM-IT-Z00 Cryptography management [EN]

- Mobiles devices
  - PM-IT-AA00 Mobile device management [EN]
  - PM-IT-AB00 BYOD (Bring Your Own Device) charter.

- Patch Management
  - PM-IT-AC00 Vulnerability and patch management [EN]

- Regulatory
  - PM-LI-A00 Manage legal matter and regulatory.

- audit Management
  - PM-IT-AI IT audit Management
  - SO-AU-B00 Integrated management system audit - Internal auditor guideline

3 information security responsibilities (TISAX 1.2.2)

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.

NOVARES INFORMATION Owners (Data owner)

All information must have an identifiable owner, the process pilot is the information owner.

They have the responsibility to establish the following information security controls:

- Define the level of confidentiality (public, internal, confidential, SECRET)
- Conduct periodic reviews of access authorization and privileges to ensure that access is based on the "need to know" concept
- Review and reconcile access security violations, both physical and electronic, and ensure appropriate corrective action
- If the information is produced as part of a project, the producers of the information and the project manager are jointly responsible for monitoring the classification of the information.

NOVARES Manager must:

- Ensure that all employees understand their obligation to protect NOVARES information and information systems.
- Ensure that information security awareness training is part of the ongoing employee education process, and that any special employment agreements for the protection of that information are signed as required.
- Communicate the NOVARES ISP to business partners, joint ventures, and service providers.
- Identify and report information security issues through helpdesk platform.
- Identify and support the development of Disaster Recovery plans DRP for all NOVARES critical systems.
- Act upon any violations of this policy.

Novares employees
The recipient of information must guarantee the protection of the information entrusted to him.

For information at the CONFIDENTIAL and SECRET level, intended for a nominally identified population, the recipient must first obtain the agreement of the issuer of the information in the event of dissemination beyond the perimeter indicated by the notice.

The fact that the sender of an item of information has not mentioned its sensitive nature does not mean that the recipient, who is subject to the obligation of discretion can disseminate it widely. He may also ask the sender of the information about any precautions he should take about the information he has received from the sender. In particular, the public dissemination of information must be the result of a voluntary and controlled process.

All users accessing NOVARES computing, and communication networks must follow the NOVARES IT CHARTER PM-IT-D00 and confidentiality.

4 Project and information security (TISAX 1.2.3)

When implementing projects (HR moving, organizational structure change, location change, changes to regulations, software change, IT department moving, new prototype facility, new prototype storage area ….) it is important, that the information security requirements are considered.

Site manager must classify Projects at the beginning of the project (public, internal, confidential, or SECRET) considering their information security requirements, the criteria for the classification of projects are linked to the level of confidentiality of the information and the information security risk.

For each new project, the site manager must assess the information security risks with SP MC E00, such as security of internal and external communication aspects.

The information security requirements are addressed in the early stages of projects.

The risk assessment is reviewed during the project.

A list of all projects, with status must be manage by the site manager.

Information security requirements for products or services to be delivered by the project see BD PM A00.

5 Information Security Risk Management (TISAX 1.4.1)

Risk assessments are conducted once a year and in response to events by the CISO at Group Level and by local Information Security responsible (Plant director/SC/TC

use PM-IT-AAH to summarize the IS Risk

CISO assign a responsible person (risk owner) to each information security risk.

risk owners specify the vulnerability (root cause) for each risk, define and follow the action plan.

- ⇨ The following risks are considered in the Global IS risk assessment:
  - Project
  - External IT service
  - User authentication
  - Separation into development, testing and operational systems /segmentation.
  - operation of external software within the shared environment
  - contractors and cooperation partners

In case of changes to the environment (e.g., organizational structure, location, changes to regulations), reassessment is conducted in a timely manner by the CISO.

6 Assessments (TISAX 1.5.1 and 1.5.2)

It is mandatory to annually review the effectiveness of the Information Security.

- An annual internal audit is performed following the ISO 27001 appendices, the planification is made by system quality leader.
- Information security policies and procedures PM-IT are reviewed annually by the CISO according to procedure SO-QS-E00 Control internal documentation.

This review should include assessing opportunities for improvement of the organization's information security policy and managing information security in response to changes.

to:

a) the organization's business strategy.

b) the organization's technical environment.

c) regulations, statutes, legislation and contracts.

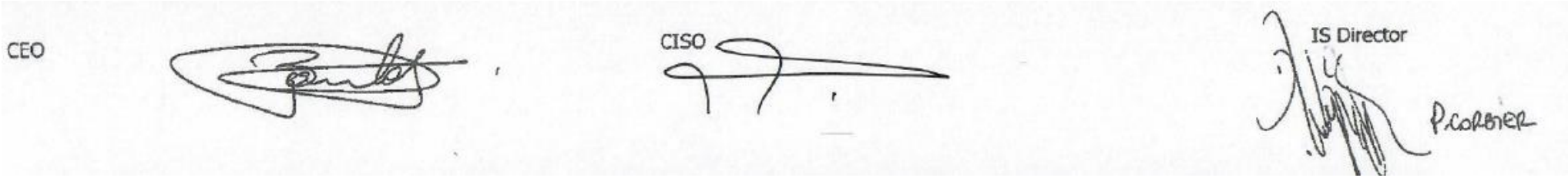
d) information security risks.

e) the current and projected information security threat environment.

f) lessons learned from information security events and incidents.

As essential control mechanism Information security reviews are conducted by an independent body at regular intervals and in case of significant changes. The planification is made by system quality leader.

7 Approval



8 Updates

Index	Date	Author / Contact	Modification
A	2024/05/23	F. SORDET	Creation