

IT- EU-POL-SEC-001

NGE Information Security Policy

Contains the Nippon Gases Europe Information Security Policy



**NIPPON
GASES**
The Gas Professionals




Document Information

Title: NGE Information Security Policy	Author: Diego Digitali
Classification: PUBLIC	Area: Nippon Gases Information Security
Version: 1.5	Version Date: 02/09/2024

Document Control

	Version	Name	Date	Comments
Developed by:	1.3	Diego Digitali	26/09/2022	Added References to Traceability and Authenticity, introduced ISMS, applied general simplification, and fixed some minor typos
	1.4	Diego Digitali	15/01/2024	Fixed the Review Cycle part, substituted "should" with "must" or indicative form, fixed the Classification level footer, added the new ISD as reviewer
	1.5	Diego Digitali	02/09/2024	Updated President's name; Policy reviewed and simplified.

	Version	Name	Role	Date	Comments
Reviewed by:	1.3	Jan Van den Bulck	Information Security Director	26/09/2022	
	1.4	Ivo Karremans	Information Security Director	16/01/2024	
	1.5	Ivo Karremans	Information Security Director	02/09/2024	

	Name	Role	Date	Signature
Version: 1.5 Approved by:	Cesar Callejo	CIO	26/11/2024	Firmado por: 
	Laura Zanotti	Legal Director	26/11/2024	BEB88824BB5D4C0... DocuSigned by: 
	Raoul Giudici	President	26/11/2024	B7D81E5BA4F342C... Firmato da: 

3B8AE19BBF714FA...

Introduction and scope

This Policy defines Nippon Gases Europe (NGE) commitment to safeguard the confidentiality, integrity, and availability of its information assets (e.g., data, applications, data centers), and it's integrated by *NGE Code of Conduct*.

This Policy applies to all Users, defined as all employees of NGE, and its majority-owned subsidiaries and affiliates, contractors, consultants, temporary workers, or anyone else granted the access of NGE's information assets. Based on specific agreements, this Policy may also apply to minority joint ventures.

Objectives

NGE Information Security System is designed to achieve the following objectives:

- protect the interest of shareholders, employees and third-parties;
- ensure compliance with applicable laws and regulations;
- ensure a standard model for corporate information protection and the management of related risks;
- guarantee a proper corporate information protection and the continuity of business processes, based on the level of confidentiality, integrity and availability requested;
- minimize the business risk by preventing and minimizing the impact of information security incidents;
- retain documentation of the designed and implemented systems;
- retain evidence of the authorization processes and of the performed activities as required by business functions.

Those objectives are pursued through:

- the application to systems design and implementation of the best standard currently available to protect information assets to ensure compliance to relevant legislation on information processing and the required level of:
 - Confidentiality (information is accessible only to authorized individuals or systems);
 - Integrity (information and processing methods must be accurate and complete);
 - Availability (information must be available and usable as required by business processes).
- the establishment, implementation, operation, monitoring, review, maintenance and continuous improvement of an effective Information Security Management System (ISMS), compliant to the ISO/IEC 27001 Standard, on version that is current at the date of this Policy;
- a strong commitment of the top management that guarantees the needed resources to achieve these objectives.