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: **1.6**	Version Date: **02/12/2025**

Document Control

	Version	Name	Date	Comments
Developed by:	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.
	1.6	Diego Digitali	02/12/2025	Updated CIO’s name; added references to NIS2 directive

	Version	Name	Role	Date	Comments
Reviewed by:	1.4	Ivo Karremans	Information Security Director	16/01/2024	
	1.5	Ivo Karremans	Information Security Director	02/09/2024	
	1.6	Ivo Karremans	Information Security Director	30/01/2026	

	Name	Role	Date	Signature
Version: 1.6 Approved by:	Javier Alvarez	CIO	17/02/2026	Firmado por: Javier Alvarez D1E6FE01E90C431...
	Laura Zanotti	Legal Director	17/02/2026	DocuSigned by: B7D81E5BA4F342C...
	Raoul Giudici	President	17/02/2026	Firmato da: Raoul Giudici 68D5CDC8D8D240D...

Introduction and scope

This Policy defines Nippon Gases Europe's (NGE) commitment to safeguarding the confidentiality, integrity, and availability of its information assets, including data, applications, infrastructures, and data centers. It is integrated with the company Code of Conduct and establishes the governance framework and principles for a structured management of information security.

The Policy also reflects the principles introduced by Directive (EU) 2022/2555 (NIS2), including its various National transposition, which requires subject organizations to adopt technical, operational, and organizational measures proportionate to the risks associated with the services they provide.

This Policy applies to:
- all employees of NGE and its majority-owned subsidiaries and affiliates;
- consultants, contractors, temporary workers, and third parties authorized to access information assets;
- IT, OT, cloud, application, physical and logical infrastructures that process or support corporate information;
- minority joint ventures, where specified by contractual agreements.

Security Principles

The organization adopts a set of security principles aligned with ISO/IEC 27001 standard, international best practices and Directive NIS2. These principles form the foundation of the Information Security Management System.

Technical details (also related to National transposition of Directive NIS2), operational measures, and specific controls are defined in lower-level procedures, standards, and work instructions, which describe the practical implementation of this Policy.

The principles include:

- **Risk management** – identifying, assessing, and treating risks related to assets, processes, suppliers, and critical services.
- **Roles and responsibilities** – clearly defining and communicating security responsibilities.
- **Human resource reliability** – ensuring personnel have appropriate skills and are bound by confidentiality and proper conduct.
- **Compliance and security audit** – periodic verification of compliance with policies, regulatory requirements, and contractual obligations.
- **Supply chain cybersecurity risk management** – assessing and controlling risks introduced by suppliers and partners.
- **Asset management** – identifying, classifying, and protecting information and infrastructure assets.
- **Vulnerability management** – detecting, analyzing, and mitigating vulnerabilities through structured processes.
- **Business continuity, disaster recovery, and crisis management** – maintaining and testing plans that ensure resilience of critical services.
- **Authentication, digital identity, and access control** – protecting logical and physical access based on least privilege.

- **Physical security** – protecting facilities and environments against unauthorized access and environmental threats.
- **Personnel training and awareness** – ongoing education on security practices and expected behaviors.
- **Data security** – protecting data throughout its lifecycle via appropriate measures.
- **Secure development, configuration, maintenance, and decommissioning of information and network systems** – applying security criteria across system lifecycles.
- **Network and communications protection** – preventing unauthorized access and protecting information flows.
- **Security event monitoring** – continuously monitoring events, anomalies, and potential threats.
- **Incident response and recovery** – structured processes for detection, response, recovery, and post-event improvement.

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, including Directive NIS2 and its National transposition laws where NGE operates;
- 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;
- support structured models for incident response and reporting, in line with NIS2 requirements;
- 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.

Top Management Commitment

Top management:

- promotes a culture of security;
- ensures adequate resources to achieve the above objectives;
- supervises and approves risks and protection strategies;

- ensures adoption of measures proportionate to cybersecurity risks, as outlined in NIS2.

Roles and Responsibilities

Board of Directors:
- approves the Policies required by NIS2 transposition laws;
- oversees and approves cybersecurity risks and the organization's security maturity.

Chief Information Officer:
- ensures implementation of the Policy and achievement of security objectives.

Information Security Director (ISD):
- maintains and improves the Policy;
- leads the security program;
- coordinates risk management, incident management, supply chain security, and monitoring.

Service Owners and Process Owners:
- identify and classify services and assets;
- implement operational measures defined in lower-level procedures.

All Personnel:
- comply with policies and procedures;
- report anomalies and security incidents.

Reporting and Monitoring

- The ISD provides periodic reports to the Board on security posture, emerging risks, and improvement activities.
- Internal audits and independent reviews ensure continuous compliance with the Policy and NIS2 expectations.

Policy Violations

Non-compliance with this Policy may result in:
- disciplinary measures;
- revocation of access rights;
- contractual actions against non-compliant third parties.