IT- EU-POL-SEC-001

Information Security Policy

Contains the Nippon Gases Europe Information Security Policy

NIPPON GASES
The Gas Professionals

1. Document Information

Title**: Information Security Policy**	Author: **Diego Digitali**
Classification: **PUBLIC**	Area: **Nippon Gases Information Security**
Version: **1.4**	Version Date: **15/01/2024**

2. Document Control

	Version	Name	Date	Comments
Developed by:	1.0	Mauro Ruggeri	13/02/2019	Initial draft
	1.1	Diego Digitali	12/02/2021	Changed Policy Framework
	1.2	Jan Van den Bulck	19/02/2021	Included NSHD InfoSec principles
	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

	Version	Name	Role	Date	Comments
Reviewed by:	1.0	Jan Van den Bulck	Information Security Director	19/09/2019	
	1.1	Jan Van den Bulck	Information Security Director	12/02/2020	
	1.2	Jan Van den Bulck	Information Security Director	19/02/2021	
	1.3	Jan Van den Bulck	Information Security Director	26/09/2022	
	1.4	Ivo Karremans	Information Security Director	16/01/2024	

	Name	Role	Date	Signature
Version: 1.4 Approved by:	Cesar Callejo	CIO	16/01/2024	DocuSigned by: Cesar Callejo BEB88824BB5D4C0...
	Laura Zanotti	Legal Director	16/01/2024	DocuSigned by: B7D81E5BA4F342C...
	Eduardo Gil Elejoste	President	16/01/2024	DocuSigned by: Eduardo Gil 0D0AB22E47E0473...

3. Table of Contents

ISO 27001 References

Requirement 4 – Context of the organization

CLAUSE 5 - Information security policies

Category 5.1 - Management direction for information security
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

CLAUSE 6 – Organization of information security

Category 6.1 - Internal organization
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

Control 6.1.1 - Information security roles and responsibilities
Control 6.1.2 - Segregation of duties
Control 6.1.3 - Contact with authorities
Control 6.1.4 - Contact with special interest groups
Control 6.1.5 - Information security in project management

CLAUSE 7 - Support

Control 7.3 - Awareness

CLAUSE 9 - Performance Evaluation

Control 9.3 Management Review

CLAUSE 18 – Compliance

Category 18.2 - Information security review
Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

Control 18.2.2 - Compliance with security policies and standards

4. Introduction and scope

This Policy covers all Information risks, both technology and non-technology oriented, related to Nippon Gases Europe (NGE) Information Security Management System (ISMS). It focuses on all information assets (e.g., data, applications, data centers). This Policy is mandatory for all majority owned NGE companies (or business units) and businesses under NGE's management control.

Information is an asset which has value to an organization and needs to be suitably protected. Information security encompasses the preservation of the confidentiality, integrity, availability, traceability, and authenticity of information.
Information security is essential to:

- Ensure that the corporation's intellectual property assets are protected globally
- Establish and maintain the corporation's competitive advantage
- Assure the confidentiality and integrity of new and current business ventures and initiatives and that the related information is traceable and authentic
- Prevent inappropriate internal or external access to Confidential and/or Proprietary Information.

At the highest-level NGE defines this "Information Security Policy" to set out the organization's approach to manage its information security objectives.

This Policy addresses requirements created by:

a) NGE Code of Conduct;
b) NGE Business Strategy and Priorities:
    - Safety
    - Compliance
    - Sustainable Development
    - People Excellence
    - Customer Focus
    - Financial Results

c) regulations, legislation, and contracts.
d) the current and projected information security threat environment.

This Policy contains statements concerning:

a) definition of information security, objectives, and principles to guide all activities relating to information security.
b) assignment of general and specific responsibilities for information security management to defined roles.
c) processes for handling deviations and exceptions.

At a lower level, this Policy is supported by topic-specific policies, which further mandate the implementation of information security controls and are typically structured to address the needs of certain target groups within an organization or to cover certain topics.

These policies are communicated to employees and relevant external parties in a relevant, accessible, and understandable form to the intended reader in the context of the information security awareness, education, and training program.

This Information Security Policy is designed to provide guidance on the proper use and protection of NGE information, including information contained in its computers (including smartphones, tablets, and mobile devices), information systems, and networks, as well as in hard-copy format. This also includes third party information that NGE is legally obligated to protect.

The Information Security Team has developed detailed procedures and standards supporting this policy and additional policies on specific areas (see **ISMS Documents Framework** below).

This Policy applies to all 'Users' which is defined as all employees of NGE, and its majority-owned subsidiaries and affiliates, contractors, consultants, temporary workers, or anyone else granted the use of an ID for electronic access. Based on agreements, this policy may also apply to minority joint ventures.

Failure to comply with this policy and related information security procedures and standards can expose NGE to risks that might cause legal, financial, and reputational impact. All users are expected to abide by this policy.
Any violation of this policy can result in disciplinary actions, including termination of employment.

If local legislation and regulations are stricter than this Policy, then local legislation and regulations prevail.

5. 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 improvement of an effective Information Security Management System (ISMS) for the specific scope of certification.

6. Principles

NGE Code of Conduct is an integral part of this policy, including the principles and objectives, and with it, the following overarching Information Security principles must be adhered to protect NGE's reputation and assets:

1. Ensure the confidentiality and integrity of NGE's and customer assets i.e., keeping NGE's data, identity, and customers' assets safe.
2. Facilitate sustainable improvements of business processes and information processing – Information Security management is fully embedded in business processes.
3. Adopt a risk-based approach - Risks are treated in a consistent and effective manner:

- Prioritize scarce resources on protecting the business applications and underlying infrastructural components on the level of compliance to principles and objectives, where a security incident would have the greatest business impact.
- Analyze and assess the current and emerging Information Security threats so that informed, timely action can be taken to mitigate risks.

4. Provide timely and accurate information about Information Security management performance - Support business requirements and manage Information risks.
5. Foster a positive Information Security culture and promote continuous improvement in Information Security management.

7. Organizational Context

The ISMS put in place would consider coping with Internal and External issues that could mine its effectiveness.
Furthermore, the set of Interested Parties is defined.

7.1. Internal Issues

NGE considers relevant the following Internal Issues that could impact on ISMS effectiveness:

- **Distribution** on Europe: having different sites on different countries makes difficult sometimes to match business cultures, laws and regulations
- **M&A** (Merge and Acquisition) process: different companies with different sizes and histories have to agree and comply to a common objective on Information Security
- **OT** networks: having to manage Operational Technology networks on Production sites, needs to define precise and rigorous separations logical and physical to guarantee the correct level of protection for different sets of information with different objectives

7.2. External Issues

The most relevant External Issues are the following:

- **Supply Chain**: NGE Supply Chain is particularly critical because involves Suppliers of any size and of many kinds
- **Critical** Value Proposition: the core business is related to Gas Production and Delivery, from Human Health to Industrial Systems, and this renders the Information Security particularly critical and strategic
- **Market** Positioning: NGE confronts worldwide competitors and participates to a number of strategic agreements and contracts where Information Security is of paramount importance.

7.3. Interested Parties

The ISMS impacts many different Interested Parties that must be correctly informed about rules and guidelines.

- **Employees**, because they are the people who comply with the practices outlined in the ISMS.
- **Shareholders**, because effective information security influences the organization's financial success.
- **Regulators and the government**, because they create information security laws and ensure they are being met.
- **Suppliers and partners**, because NGE has contractual arrangements about the way sensitive information is protected.
- **The media**, because there is far more mainstream coverage of data breaches and a wider public interest in the way organization protects personal information.
- **Customers**, because they use NGE services and share sensitive information with NGE.

8. Information Security

'Confidential and/or Proprietary Information' refers to information related to the Company's business to which an employee has access to or generates while conducting their job responsibilities.
It is information the Company has not made public or authorized public disclosure of and is not available to persons outside the Company through proper means.
'Confidential and/or Proprietary Information' is considered a corporate asset, just like other "hard" assets, and is critical to NGE's competitiveness and success.

Confidential and/or Proprietary Information comes in various forms and relates to all aspects of NGE business. It includes both hard and electronic copies of emails, documents, agreements, spreadsheets, flow diagrams, PowerPoint presentations and the like and is often directed to NGE finance, legal, procurement, human resources, and technology functions. It also includes Confidential and/or Proprietary Information of others that NGE accepts under terms of confidentiality.

Every employee that views, handles, and generates such information is therefore responsible to safeguard these information assets from unauthorized use or disclosure.

This obligation extends even after employment with NGE ends, according to specific agreements signed by employees.
It is important that employees comply with NGE security Policies and Procedures when transmitting, in digital and/or paper format, Confidential and/or Proprietary Information to a third party.

9. Monitoring and Ownership

All communications, information, and other data (''information') created, sent, or retrieved over or stored in any NGE computer, information system or network, both through the Internet and internally, are treated as the property of NGE. Such computers, mobile devices, information systems, and networks may contain Confidential and/or Proprietary Information subject to legal protection and are subject to unannounced monitoring and inspection as necessary to assure their use for proper business purposes and to protect the Company's legal interests.
If a user has not received specific authorization to access an NGE computer, information system or network, the user must not do so.
Under appropriate circumstances, all communications, including text and image content, may be disclosed to law enforcement, government investigative agencies, or other third parties without prior

consent of the sender or receiver. Electronic information is legally discoverable and may be used as evidence in a court of law.

The use of NGE computers, information systems or networks will be deemed the user's irrevocable acknowledgment of and consent to these conditions. This includes NGE's rights to access all information on an NGE device or computer. Any doubt in connection with these matters must be resolved by contacting the Legal department.

10. Intellectual Property - Copyrights & Trademarks

NGE and its employees are subject to all European and country laws relating to intellectual property, such as patents, trademark, copyright, and trade secret usage, and to privacy, security, and social media. Employees are also subject to the terms of all agreements signed by NG, and the terms and conditions of all software licensing, development, and hosting agreements.
This policy applies to all software and all copyrightable or trademarked materials or content that are owned or licensed by NGE or are developed, authored, or created by employees, contractors, or vendors at NGE's expense or using NGE's resources. It includes compliance with obligations for safeguarding personal protectable information. Failure to observe and comply with the intellectual property, licensing, or privacy terms of these agreements may result in legal action and is a serious violation of this policy.

11. ISMS Documents Framework

The diagram below outlines the framework and hierarchy for Information Security policies, standards, and guidelines. For any questions or clarifications regarding these documents contact the Information Security Team.
This Policy applies the principles expressed in NGE Code of Conduct, known by all employees, and extends them with ISO 27001 Requirements.
Furthermore, a set of other Policies are specific for different part of the ISO 27001 Standard and they are implemented through a series of Procedures and Standards, specified in detail.

All the ISMS documents are contained and accessible, with different Access Levels according to their Information Classification level, in ITS Information Security NGE intranet site, and they could refer or recall, whenever fit and necessary, documents external to the ISMS Documents set because belonging to other NGE Departments involved in the ISMS perimeter, like Infrastructure, Legal, Procurement and HR. In this way, ownerships, roles, and responsibilities are clearer and the maintenance and development of the documents are better managed.

12. Roles and Responsibilities

NGE's risk management governance is based on several lines of defense model. Additionally, the following roles and responsibilities, and Policy governance are defined for Information Security management areas.
Business Management is ultimately accountable for managing risks in their business, including those in the case of outsourcing.

12.1. European President

European President promotes the definition and the implementation of an adequate system of information protection and management.

NGE European President operates to deliver the needed resources for the implementation of ISMS and delegates the definition, implementation and monitoring of the information security system to Information Security Director, ISMS Manager and Users based on their roles.
NGE European President approves and signs this Policy, together with CIO and Legal Director.
All other Policies could be approved by interested Directors and/or M (see below).

12.2. Chief Information Officer (CIO)

The Chief Information Officer has an overall ownership of the Information Technology function and leads its activities. This includes development, implementation, operation and maintenance of an IT Control Framework.

12.3. Legal Director

The Legal Director has an overall ownership of the Legal and Compliance issues.

12.4. Information Security Director (ISD)

NGE ISD is appointed, has an overall ownership of the IT security and leads its activities and reports to CIO.
The role includes IT security vision, tactical translation and the coordination, monitoring and reporting of global implementation.
The ISD develops the global IT Security Control Frameworks.
The Information Security Team (IST) supporting the ISD is also responsible for pro-actively monitoring, analyzing and reporting risk trends and new or changing regulatory requirements that have or will have an impact on NG's Information Security management.

12.5. Information Security Management System Manager

NGE Information Security Management System Manager (ISMS Manager) reports to NGE ISD.
NGE ISMS Manager has the following responsibilities:

- defining and updating of the Information Security policy based on NGE Information Security policy and guidelines, NGE business needs and relevant legal requirements;
- designing the information security system and preparing plans for its implementation;
- coordinating the information security system implementation;
- monitoring the implementation of information security systems and of protection measures on information system assets;
- promoting training, awareness and communication initiatives and programs on Information Security;
- promoting audit and assessment activities for the continuous monitoring of the adequacy and effectiveness of the information protection system;
- reporting to NGE ISD the status of information security system, plans, actions and issues.

NGE ISMS Manager operates in collaboration with NGE Human Resources and Legal departments.

13. Segregation of duties

Care must be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event must be separated from its authorization. The possibility of collusion must be considered in designing the controls. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision must be considered.

14. Contact with authorities

NGE has procedures in place that specify when and by whom the authorities (e.g., law enforcement, regulatory bodies, supervisory authorities) must be contacted and how identified information security incidents must be reported in a timely manner (e.g., if it is suspected that laws may have been broken).

15. Contact with special interest groups

Appropriate contacts with special interest groups or other specialist security forums, mailing lists and professional associations are maintained.

16. Information security in project management

Information security must be integrated into the organization's project management method(s) to ensure that information security risks are identified and addressed as part of a project. This applies to any project regardless of its type, e.g., a project for a core business process, IT, facility management and other supporting processes.

17. Exceptions

If one or more of the requirements detailed in this or in the supporting policies is not being met, it must be brought immediately to the attention of the IST and a specific Risk Treatment Plan must be kicked off.

18. Review Cycle

Each Information Security Management System' Policy must have an owner who has approved management responsibility for the development, review, and evaluation of the policies. The owner is responsible also for reviewing the owned policy at least annually, eventually supported by specific stakeholders. The review includes assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions, or technical environment.
The review of information security policies must consider the results of ISMS's Management Reviews.