NSG GROUP INFORMATION SECURITY POLICY

Approved by: Group CEO

_____

Date: 23 December 2025

_____

Policy Objective	This document defines the Information Security Policy for NSG Group. This policy is the overarching Information Security policy for the organisation. Information Security is achieved through the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction. This is done in order to provide confidentiality, integrity, and availability of the Group's assets and all information it collects, stores, transfers or processes for clients and employees or people acting on behalf of NSG, in accordance with relevant legislation, regulation and contractual obligations. This document applies to information in all its forms, including electronic, physical or intangible, e.g. knowledge

Scope	**The NSG Group Information Policy applies to:** • All NSG Group companies (including JVs and Associates) and their employees, at all locations, across all countries within the Group, where NSG has management control. • Third party organisations who support NSG Group must align to this policy.

Definitions	OT (Operational Technology) - refers to systems used to control and monitor physical processes, like machines and equipment in factories or logistics operations. ICS (Industrial Control Systems) - are a type of OT used to manage and automate industrial tasks, such as production lines or energy systems. **Enterprise Risk Management (ERM) -** is a structured, organization-wide approach to identifying, assessing, managing, and monitoring risks that could affect the achievement of an organization's strategic and business objectives, integrating risk considerations into governance, strategy, and decision-making processes at all levels.

Detail	**Information Security Objective** Information security objectives help implement an organisation's strategic business goals in accordance with its information security policy and help determine whether it is functioning as expected. The Information Security Objectives are:

- **Business Alignment –** Ensure that information security supports NSG Group's Vision, Mission, and strategic priorities by enabling secure business growth, digital transformation, and sustainability initiatives, and by implementing an appropriate workflow to evaluate and integrate information security requirements during the design phase of all NSG Group initiatives.
- **Compliance and Obligations –** Comply with all applicable laws, regulations, contractual requirements, and internal standards related to information security, data protection and data privacy, where compliance will be assessed by those responsible for the processes, by the compliance functions and by the NSG Group's Internal Audit, in accordance with the review cycle required by each standard.
- **Information Security Policies and Organization -** NSG will ensure that all documents supporting NSG's information security stance are kept up to date and compliant.
- **Human Resources -** NSG will provide employees or people acting on behalf of NSG with information security training and regularly monitor quality and compliance by tracking the training completion rate. NSG will follow up with employees or people acting on behalf of NSG/report to governance forums, where appropriate, if the rate does not meet the agreed minimum set by the business.
- **Identity & Access Management -** Ensure the confidentiality, integrity and availability of NSG Group information assets, including intellectual property, operational data and personal information, against unauthorised access, disclosure, alteration or destruction by implementing processes and controls to ensure that legitimate parties have the right access to the right resources at the right time.
- **Risk and Audit –** Manage information security through a risk-oriented approach, identifying and assessing risks to critical assets and applying proportionate controls to mitigate them, in accordance with NSG Enterprise Risk, confirmed that any information security non-conformities raised by customers, internal or external auditors are addressed in a defined risk treatment and mitigation plan in place.
- **Data Classification -** Implement and maintain a structured process to identify, classify, and label all information assets according to their sensitivity and business value. This ensures appropriate protection measures are applied throughout the information lifecycle, supporting confidentiality, integrity, and availability in line with legal, regulatory, and contractual requirements.
- **Industrial Security -** Establish and maintain a minimum baseline of security controls for all manufacturing and logistics sites to protect OT/ICS environments, strengthen supply chain security, and support business continuity.

Top Management Commitment

The NSG Group is committed to maintaining a high level of Information Security and has established an Information Security Framework which is endorsed by the Group's Management Committee.

The CDIO is responsible for the creation of Digital policies, Standards and Controls that when followed will maintain regulatory compliance and risk across the IT Landscape.

Compliance with this Policy

Adherence to this policy is mandatory. All employees or people acting on behalf of NSG have an individual responsibility to ensure their personal compliance with this policy and must seek guidance for further clarification if required. Any deviation from this policy is prohibited, unless an exception approved, and will maintain a register of all approved exemptions from the Security Policy.

Compliance with this policy may be monitored through inspections, audits and/or requests for written confirmations of compliance.

Policy Reviewers and Approvers are responsible for regularly assessing the compliance of this policy within their area of responsibility. Any employees or people acting on behalf of NSG found to have violated this policy may be subject to disciplinary action as per the processes included in the Disciplinary Policy.

Employees or people acting on behalf of NSG Responsibilities

Employees or people acting on behalf of NSG must ensure that their day-to-day activities are compliant with the Group's information security policies, standards and procedures, and must confirm their compliance with the Group's information security policy on an annual basis.

Continuous improvement for Information Security

Information security critical documents used to Information Security policy must be reviewed at least annually, to ensure they continue to meet the needs of NSG.

Reviews must consider changes in the organisation or systems of the group and relevant changes to legislation and regulation.

Independent reviews of the Group's information security policies, standards and procedures must be conducted at least annually.

Security Policy

NSG Group Digital must approve, publish and communicate the information security policies, standards and procedures to all employees or people acting on behalf of NSG and relevant external parties.

Third Party Security

There must be a defined Third-Party security assurance programme in place to define the Group's Information Security management process for Third Parties that have access to collect, handle, process and/or store NSG or Customer Information. Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets shall be agreed with the supplier and documented.

NSG Group Digital must support the Third-Party assurance programme on behalf of the

	contracting business units.

Revision History	• Approved by CEO on 31st March 2023 • Approved by CEO on 17th March 2024 • Approved by CEO on 23rd December 2025