Information Security Policy

The purpose of this Policy is to protect information at NIST Global in all forms—written, electronic, and verbal—from unauthorized access, disclosure, alteration, loss, or misuse.

Information may include, but is not limited to: emails, documents, training materials, plans, assessments, operational and audit data, analysis and findings, learner and employee records, client information, and disciplinary or grievance-related information. All information must be protected throughout its lifecycle, including collection, storage, use, sharing, transfer, retention, and secure disposal.

This Policy applies to all individuals who access, handle, or manage information on behalf of NIST Global, including but not limited to:

- All employees of NIST Global
- Management and department heads
- Freelancers, consultants, trainers, auditors, contractors, agents, and third parties associated with NIST Global

The Policy applies across all departments, business verticals, systems, applications, platforms, and locations, and covers information handled in physical, verbal, and digital formats.

Information Security Framework

NIST Global follows a structured Information Security Framework that safeguards information while enabling fully digital operations, cloud-based platforms, and remote collaboration. Information security is a shared responsibility across the organization. The framework is based on four core principles:

a) Know What Information We Have

NIST Global ensures awareness and accountability over information assets by:

- Identifying information handled across Zoho Business Operating System, LMS, websites, cloud platforms (AWS), and collaboration tools
- Recognizing information stored in paper form and information shared verbally during meetings, training, audits, and client interactions
- Ensuring departments and users understand their responsibility for the information they create, access, or manage

b) Assess Information Security Risks

NIST Global assesses information security risks by:

- Evaluating risks related to digital platforms, cloud hosting, applications, and third-party systems

- Considering threats such as unauthorized access, data leakage, cyberattacks, human error, and misuse of information
- Assessing risks before implementing new systems, applications, software, or vendors
- Considering legal, contractual, operational, and reputational impacts

c) Protect Information Appropriately

NIST Global protects information using layered controls covering people, process, physical security, technology, and cybersecurity, including:

- Role-based access to systems and applications
- Secure authentication and authorization mechanisms
- Controlled data sharing using approved platforms
- Protection of training materials and digital content from unauthorized access or distribution
- Secure handling of printed documents and sensitive verbal information
- Cybersecurity controls to protect networks, cloud infrastructure, applications, and endpoints from cyber threats

d) Govern, Monitor, and Continuously Improve

NIST Global ensures effective information security governance by:

- Establishing management oversight and accountability
- Monitoring compliance with this Policy
- Reviewing incidents, vulnerabilities, and emerging cybersecurity risks
- Continuously improving controls based on audits, incidents, and regulatory changes
- Aligning practices with **ISO/IEC 27001**, **DPDP Act 2023**, and **GDPR**

Digital Operations and Systems

NIST Global operates in a predominantly digital environment. Information security controls apply to:

- Zoho Business Operating System and department applications used for operations and delivery, including HR, finance, IT, project management, task monitoring, training operations, auditing and consulting workflows, and other business functions
- Digital platforms supporting training processes from enrolment to certificate issuance
- MS Teams used for training delivery and collaboration
- Google Slides used for controlled access to training materials without local downloads
- Learning content, animations, and digital deliverables shared with clients

- Websites, Learning Management Systems (LMS), and client platforms hosted on cloud infrastructure, including AWS
- EHS software applications developed using Zoho

Physical and Environmental Security

Physical security is an integral part of information security. NIST Global shall ensure:

- Authorized entry and exit controls for offices and sensitive areas
- Restricted and controlled access to server rooms and infrastructure areas
- Secure storage of physical documents and records
- Prevention of unauthorized removal, copying, or viewing of information

Information Security Incidents

Any actual or suspected information security incident, including data loss, unauthorized access, misuse of information, or system compromise, must be reported immediately to: **ict@nistglobal.com**

Upon receiving the incident report, the ICT team shall immediately notify Management for review and direction.

All incidents shall be:

- Investigated promptly
- Addressed with corrective and preventive actions
- Escalated to management where required

Compliance and Regulatory Alignment

NIST Global is committed to compliance with applicable information security and data protection requirements, including:

- **ISO/IEC 27001 – Information Security Management System (ISMS)**
- **Digital Personal Data Protection (DPDP) Act - 2023**
- **General Data Protection Regulation (GDPR)**

Data and information used or processed by NIST Global—including personal data and data used for Artificial Intelligence (AI) development, training, testing, or deployment—shall be protected from unauthorized access, misuse, alteration, loss, or disclosure and managed in line with the Data Protection Policy and AI Policy.

This Policy works alongside other organizational policies, including:

- Data Protection Policy
- Artificial Intelligence Policy

- Business Continuity Policy

Roles and Responsibilities

- **Management**
  - Provides oversight and resources for information security
- **Department Heads**
  - Ensure compliance within their functions
- **Employees and Associated Persons**
  - Protect information entrusted to them
  - Use systems responsibly
  - Report incidents promptly

Information security is a shared responsibility.

Awareness and Training

NIST Global shall promote information security awareness through:

- Employee induction programs
- Periodic communication and guidance
- Role-based awareness where required

Policy Compliance

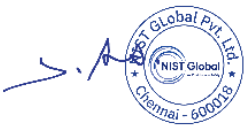
Failure to comply with this Policy may result in disciplinary action in accordance with organizational procedures.

Review and Continuous Improvement

This Policy shall be:

- Reviewed periodically or following significant incidents or changes
- Updated to reflect business, technological, or regulatory developments
- Approved by management and communicated across the organization

Signed by **Chairman & MD** Effective Date: 18th Dec 2025



Mr Antony Selvaraj