Data Protection Policy

NIST Global handles data from employees, learners, clients, vendors, suppliers, regulators and international boards. This policy explains how we protect that data and comply with the **Digital Personal Data Protection (DPDP) Act 2023** and, where applicable, **General Data Protection Regulation (GDPR)** requirements for our international and UK/EU-related activities.

It applies to:

- All NIST Global employees, consultants, freelancers, interns, contractors, partners, subsidiaries and third parties who have access to or handle NIST Global official data
- All data stored or processed in Zoho WorkDrive, Google Drive, email and official systems

What Data we Handle

- **Personal Data:** Information that identifies a person, including:
  - Name, contact details, employment details
  - Login IDs, passwords
  - Financial or payroll information
  - Identification records, photos, training records
  - Sensitive data if collected for work or training needs
- **Non-Personal / Business Data**: Information related to NIST operations, such as:
  - Training content, reports, proposals
  - Audit records, internal communication
  - Financial, performance and commercial information

All data—whether personal or business—must be handled securely and responsibly, in line with the DPDP Act and GDPR.

Data Protection Principles

NIST Global follows these principles for all data:

- **Lawful and Fair Use:** Collected for clear, valid purposes
- **Minimal Collection:** Only what is necessary is gathered
- **Accuracy:** Kept correct and updated as required
- **Security:** Protected from unauthorized access, loss, alteration or misuse
- **Limited Retention:** Stored only as long as necessary
- **Transparency:** Individuals are informed about how their data is used.

Roles and Responsibilities

- **All Employees and Users**
  - Use data only for legitimate business purposes
  - Store data only on Zoho WorkDrive, Google Drive or official systems
  - Avoid saving or transferring data to personal devices or personal emails
  - Keep passwords secure and follow IT security guidelines
  - Report any suspected data breach immediately
- **Awarding/Regulatory Bodies and Learners**
  - Any suspected malpractice, misconduct or breach identified during training, assessment or certification activities is reported to the relevant awarding or regulatory body, as required. The awarding or regulatory body is expected to maintain confidentiality and ensure learner details are not disclosed to unauthorised persons.
  - Learners and participants must not share or exchange official training materials, assessment content, or any confidential client or organisational information with other participants or any unauthorised person.

Data Handling, Storage, Use, Retrieval and Retention

- Data is stored only on Zoho WorkDrive, Google Drive or other official systems, and not on personal devices unless formally approved.
- Important organisational records (such as accreditation certificates, approved training materials, course content, key email approvals, client authorisations and related reference documents) are archived in official systems for long-term reference, continuity, easy retrieval, and audit purposes.
- Data retrieval is permitted only through authorised official systems, ensuring that records can be accurately accessed, traced, and restored when required for operational, audit, regulatory, or client verification purposes.
- Access to retrieve data is role-based and limited to authorised personnel to maintain confidentiality, integrity, and data security
- Data is not shared through personal email or messaging apps; any external sharing has a clear purpose, approval and safeguards.
- Learner, client and employee data are used only for the services for which it was collected.
- Learner registration details, assessment records, results, certificates and attendance records for international training programmes are generally retained for 3–6 years for verification, audit, compliance and reference.

- For other business services, data is normally retained for up to 1-year after the service is completed; if a project lasts longer than 1-year, related records are retained for at least the project duration.
- After the retention period ends, all data (printed and electronic) is securely and permanently destroyed in line with legal, contractual and audit requirements.

Data Breach Reporting

- Any unauthorized access, loss, accidental sharing or suspected misuse must be reported immediately to the IT Department.
- Incident response steps are initiated promptly, documented and reviewed for improvement.

Policy Review

This policy will be reviewed annually or earlier if:

- Laws or regulations change, or
- NIST adopts new systems or expands data-related activities

Signed by **Chairman & MD** Effective Date: 26th Nov 2025

Mr Antony Selvaraj