DATA PROTECTION & CONFIDENTIALITY POLICY

Shatabdi NetBiz (SNBiz)

Policy Reference: SNBiz-POL-DPC-001
Version: 1.0
Effective Date: Upon Management Approval
Policy Owner: Chief Executive Officer
Review Frequency: Annually
Applicability: Management, Employees, Trainers, Assessors, Consultants, Contractors, Service Providers, and Authorized System Users

1. Policy Statement

Shatabdi NetBiz (SNBiz) is committed to protecting personal information, confidential business records, intellectual property, and other sensitive information entrusted to the organization.
We recognize that information security, privacy, confidentiality, and responsible data management are essential to maintaining stakeholder trust, professional integrity, operational reliability, and sustainable business relationships.
As a professional training, competency assessment, certification, and business support organization, SNBiz collects and processes information relating to clients, employees, trainees, suppliers, and other stakeholders.
We are committed to ensuring that information is collected lawfully, used for legitimate purposes, protected against unauthorized access, and retained only for appropriate periods.
Our Data Protection Commitment:
Protecting Information. Respecting Privacy. Maintaining Trust.

2. Policy Objectives

SNBiz is committed to:

1. Protecting personal, confidential, and sensitive information from unauthorized access, disclosure, alteration, loss, or misuse.
2. Collecting and processing information only for legitimate, specified, and lawful purposes.
3. Maintaining the confidentiality, integrity, and availability of organizational information.
4. Limiting access to information according to authorized responsibilities.
5. Implementing appropriate technical, administrative, and physical security measures.
6. Maintaining accurate training, assessment, certification, and business records.
7. Protecting client information, commercial agreements, and proprietary materials.
8. Establishing appropriate procedures for data sharing, retention, disposal, and incident reporting.
9. Respecting applicable individual data protection rights.
10. Continually improving information security and confidentiality practices.

3. Scope & Applicability

This policy applies to information collected, stored, processed, transmitted, or maintained by SNBiz, whether in electronic, printed, verbal, or other forms.
It covers:

- Corporate and client information.
- Training registration and participant records.
- Competency assessment results.

- Certificate issuance and verification records.
- Employee and trainer information.
- Supplier and contractor information.
- Financial, quotation, and invoicing records.
- Website inquiries and online registration forms.
- Digital learning platforms and administrative systems.
- Internal communications and business documentation.
- Confidential information received from clients and business partners.

The policy applies to all personnel and third parties authorized to access SNBiz information.

4. Information Classification

SNBiz shall classify information according to its sensitivity, business importance, and potential impact if disclosed or misused.

Public Information

Information approved for public disclosure, including published company profiles, approved promotional materials, course descriptions, and publicly accessible notices.

Internal Information

Operational information intended for authorized organizational use, including internal communications, schedules, administrative procedures, and routine business records.

Confidential Information

Information requiring restricted access, including client contracts, quotations, financial records, employee information, participant records, assessment results, and unpublished business documents.

Restricted or Sensitive Information

Information requiring enhanced protection, including passwords, system credentials, national identification information, financial account details, sensitive personal data, and confidential client information subject to contractual restrictions.

Information shall be handled according to its classification and applicable legal requirements.

5. Personal Data Collection & Processing

SNBiz shall collect personal information only where necessary for legitimate business, contractual, training, assessment, administrative, or legal purposes.

Personal information may include:

- Names and contact details.
- Organization and professional designation.
- Training registration information.
- Participant photographs, where necessary.
- Attendance and training completion records.
- Competency assessment results.
- Certificate identification and verification information.
- Employment and professional qualification records.
- Payment and transaction information.

SNBiz shall seek to ensure that:

- Individuals receive appropriate information about relevant data collection and use.
- Required consent or another applicable lawful basis is established.
- Data collection is limited to information reasonably necessary for the intended purpose.

- Information is not used for incompatible or unauthorized purposes.
- Personal data is maintained accurately and updated when necessary.
- Sensitive information receives additional protection.

6. Confidentiality & Non-Disclosure

Employees, trainers, assessors, consultants, and other authorized personnel must maintain the confidentiality of information obtained through their professional responsibilities.

Confidential information shall not be disclosed to unauthorized persons or organizations without an appropriate legal, contractual, or organizational basis.

Personnel shall not:

- Share confidential client documents without authorization.
- Disclose participant assessment results to unauthorized parties.
- Use business information for personal financial gain.
- Share system passwords or access credentials.
- Copy confidential records for unauthorized personal use.
- Publish client names, photographs, or project details without appropriate authorization.
- Discuss sensitive organizational information in public or unsecured environments.

Confidentiality obligations shall continue after employment, contractual engagement, or business relationships end, subject to applicable law.

7. Training, Assessment & Certification Data

SNBiz recognizes that training and competency assessment records require accuracy, confidentiality, and controlled access.

Accordingly:

- Participant registration information shall be used for authorized training and administrative purposes.
- Assessment results shall be accessible only to authorized personnel and appropriate recipients.
- Certificates shall be issued based on verified training or assessment records.
- Certificate records shall be protected against unauthorized modification or deletion.
- Assessment documents and performance observations shall not be disclosed without an appropriate basis.
- Participant photographs and identification information shall be processed only where necessary and lawful.
- Certificate verification systems shall disclose only information appropriate for legitimate verification.

Public certificate verification shall be designed to confirm certificate authenticity without unnecessarily exposing personal information.

8. Website, Online Forms & Digital Systems

SNBiz shall seek to maintain appropriate security controls for its corporate website, online training platform, registration forms, certificate verification system, and administrative applications.

Relevant controls shall include:

- Secure website connections using HTTPS.
- Appropriate administrator authentication.

- Role-based access restrictions.
- Strong password requirements.
- Regular software and security updates.
- Protection against unauthorized access and malicious activity.
- Secure handling of uploaded documents and participant information.
- Appropriate backup and recovery arrangements.
- Monitoring and correction of identified security vulnerabilities.

Website forms shall collect only information necessary for their stated purposes.
Personal information submitted through online forms shall not be publicly displayed or shared for unrelated purposes without an appropriate lawful basis.

9. Access Control & User Responsibilities

Access to organizational information shall be granted according to legitimate job responsibilities and operational requirements.
SNBiz shall seek to implement the principle of least privilege, ensuring that users receive only the access necessary to perform their assigned duties.
Authorized users shall:

- Protect their login credentials.
- Avoid sharing accounts or passwords.
- Use organizational information only for authorized purposes.
- Report suspected unauthorized access.
- Secure devices and documents containing confidential information.
- Avoid transferring sensitive records through unapproved communication channels.
- Notify management when access rights require modification or removal.

Access permissions shall be reviewed periodically and updated when responsibilities change or engagements end.

10. Information Security & Cybersecurity

SNBiz shall adopt proportionate technical and organizational measures to protect information systems and business records.
Measures may include:

- Firewalls and appropriate website security controls.
- Malware protection.
- Secure authentication and multi-factor authentication where available.
- Software updates and vulnerability management.
- Encrypted communication and storage where appropriate.
- Secure backup procedures.
- Device access controls.
- Restricted administrative privileges.
- Security awareness and user guidance.

Security measures shall be selected according to the sensitivity of the information, operational risks, and available resources.

11. Data Sharing & Third-Party Processing

SNBiz may share relevant information with clients, trainers, assessors, service providers, regulatory authorities, or other authorized parties where necessary and lawful.

Before sharing confidential or personal information, SNBiz shall consider:

- The legitimacy and necessity of the disclosure.
- The recipient's authority to receive the information.
- Applicable consent and other legal requirements.
- Contractual confidentiality obligations.
- Appropriate security arrangements.
- The minimum information necessary for the intended purpose.

Third-party service providers processing information on behalf of SNBiz shall be expected to maintain appropriate confidentiality and security protections.

International data transfers, where applicable, shall be assessed against relevant legal and contractual requirements.

12. Client Confidentiality & Intellectual Property

SNBiz respects the confidentiality of information received from clients and business partners.

Client-specific operational procedures, internal reports, training requirements, assessment findings, and commercial information shall not be disclosed or reused outside authorized purposes.

Training materials, manuals, presentations, assessment tools, software, and other intellectual property shall be used in accordance with applicable ownership, licensing, and contractual arrangements.

Employees and representatives shall not reproduce, distribute, or commercially exploit protected materials without appropriate authorization.

13. Data Accuracy & Integrity

SNBiz shall seek to maintain reliable and accurate organizational records.

Relevant personnel shall ensure that:

- Information is recorded accurately.
- Training attendance and assessment results reflect actual activities.
- Certificate details correspond with approved records.
- Financial and administrative records are not deliberately falsified.
- Errors are reported and corrected through appropriate procedures.
- Unauthorized modifications are prevented or detected where reasonably practicable.

Changes to critical records should be traceable through appropriate system controls or administrative documentation.

14. Data Retention & Secure Disposal

SNBiz shall retain information only for as long as necessary to fulfill legitimate business purposes, contractual obligations, applicable legal requirements, or justified recordkeeping needs.

Retention periods shall be established according to the nature and sensitivity of the information.

When information is no longer required, it shall be securely deleted, destroyed, or anonymized, as appropriate.

Disposal arrangements may include:

- Secure deletion of electronic files.
- Controlled removal of obsolete system records.
- Shredding of confidential printed documents.
- Secure disposal or sanitization of storage devices.
- Removal of unnecessary access permissions.

Data subject to legal preservation requirements, disputes, or investigations shall not be destroyed until the relevant obligation has ended.

15. Individual Privacy Rights

SNBiz shall respect applicable rights of individuals regarding their personal information.
Subject to legal requirements and relevant exceptions, individuals may be entitled to:

- Receive information about the collection and use of their personal data.
- Request access to personal information held about them.
- Request correction of inaccurate or incomplete information.
- Request deletion or restriction of processing where applicable.
- Withdraw consent where processing depends on consent.
- Raise concerns about inappropriate use or disclosure.
- Exercise other applicable statutory rights, including data portability where relevant.

Requests shall be reviewed and handled within applicable legal timeframes.
SNBiz shall take reasonable steps to verify the identity and authority of a requester before disclosing or modifying protected information.

16. Data Breach & Security Incident Management

A data security incident may involve unauthorized access, disclosure, alteration, destruction, loss, or compromise of information.
Employees and authorized personnel shall promptly report suspected incidents to the designated management or technical representative.
SNBiz shall seek to:

1. Identify and assess the incident.
2. Contain the immediate security threat.
3. Protect affected systems and information.
4. Determine the nature and extent of potential exposure.
5. Preserve relevant evidence.
6. Assess legal, contractual, and regulatory notification obligations.
7. Notify affected parties and authorities where required.
8. Implement corrective actions.
9. Review lessons learned to reduce the likelihood of recurrence.

Incidents shall be managed according to their severity, potential impact, and applicable requirements.

17. Business Continuity & Data Recovery

SNBiz recognizes that information availability is essential to uninterrupted training, assessment, certification, and administrative services.
We shall seek to maintain appropriate backup and recovery arrangements for critical business information.

These arrangements may include:

- Scheduled backups of important databases and records.
- Secure storage of backup information.
- Restricted access to backup systems.
- Periodic verification of backup integrity.
- Recovery procedures for essential applications.
- Contingency arrangements for website or system disruptions.

Business continuity measures shall be proportionate to organizational needs and operational risks.

18. Employee Awareness & Confidentiality Training

SNBiz shall promote awareness of information security and confidentiality responsibilities among employees and relevant service providers.

Awareness activities may address:

- Protection of personal information.
- Password and account security.
- Phishing and fraudulent communications.
- Safe handling of confidential documents.
- Secure use of email and digital platforms.
- Reporting of suspicious activity.
- Appropriate use of client and participant information.

Personnel with access to sensitive systems or information may receive additional role-specific guidance.

19. Legal & Regulatory Compliance

SNBiz is committed to fulfilling applicable data protection, cybersecurity, confidentiality, and contractual requirements.

These include relevant provisions of Bangladesh's Personal Data Protection Act, 2026, applicable cybersecurity legislation, and other legal requirements relevant to the organization's activities.

Where appropriate, SNBiz shall also consider internationally recognized information security and privacy management principles, including ISO/IEC 27001 and ISO/IEC 27701.

The organization shall review relevant legal developments and update its policies and procedures where necessary.

20. Responsibilities & Accountability

Chief Executive Officer / Management

Responsible for approving this policy, establishing accountability, allocating appropriate resources, and overseeing significant data protection and confidentiality matters.

Designated Data Protection or Information Security Responsible Person

Responsible for coordinating relevant privacy requests, security concerns, access reviews, incident management, and compliance activities within the authority assigned by management.

Employees, Trainers & Assessors

Responsible for protecting information accessed during their duties, following authorized procedures, and promptly reporting suspected breaches.

Website & System Administrators
Responsible for implementing and maintaining authorized technical controls, user permissions, system updates, backups, and relevant security measures.
Contractors & Third-Party Service Providers
Responsible for complying with applicable confidentiality, data protection, and contractual requirements when handling SNBiz information.

21. Monitoring, Review & Continual Improvement
SNBiz shall periodically review the effectiveness of its data protection and confidentiality arrangements.
Relevant monitoring activities may include:

- User access reviews.
- Security incident and breach records.
- Backup and recovery checks.
- Website and application security reviews.
- Privacy requests and complaints.
- Third-party security arrangements.
- Staff awareness activities.
- Corrective action implementation.

Identified weaknesses shall be evaluated and addressed according to their significance.
This policy shall be reviewed at least annually, or earlier following significant legal, technological, organizational, or operational changes.

22. Management Declaration
Shatabdi NetBiz recognizes that the protection of information is a fundamental obligation to its clients, participants, employees, business partners, and other stakeholders.
We are committed to maintaining trust through responsible data collection, secure information handling, confidentiality, professional accountability, and continuous improvement.
We believe that protecting information is not merely a technical requirement but an essential element of ethical and responsible business conduct.

Protecting Information. Respecting Privacy. Maintaining Trust.

For and on behalf of Shatabdi NetBiz (SNBiz)
Approved By: Chief Executive Officer

Signature: _____

Approval Date: _____

Next Review Date: _____
This policy becomes effective following formal management approval and communication to relevant personnel.