DATA RETENTION POLICY

National Development Programme (NDP)

December 2023

NDP BHABAN

BAGBARI, SHAHID NAGARKAMARKHANDA, SIRAJGANJ-6703, CELL PHONE: +8809639100600; WEBSITE: WWW.NDPBD.ORG

Aleya Akhtar Banu
Chairperson
National Development Programme (NDP)

Md. Alauddin Khan
Executive Director
National Development Programme (NDP)

Contents

Introduction

The National Development Programme (NDP), founded in 1992, is a prominent non-governmental organization (NGO) in Bangladesh, dedicated to promoting sustainable development in rural and marginalized communities. With its mission to improve the livelihoods of disadvantaged groups, NDP engages in various projects related to poverty alleviation, women's empowerment, education, health, and environmental conservation. The organization works closely with both national and international partners to implement impactful projects that foster social and economic development. As part of its operations, NDP collects, processes, and stores a substantial amount of data related to its project and programme participants, financial records, employee information, and various other operational details. To ensure that this data is managed responsibly and complies with local and international regulations, NDP has implemented this Data Retention Policy.

This policy outlines the procedures for retaining, archiving, and securely disposing of data across all departments, including Management Information Systems (MIS), Human Resources (HR), Finance, Information Technology (IT). It applies to all forms of data, both physical and digital, and to all employees, contractors, and third-party partners handling NDP's sensitive information. By establishing a clear data retention policy, NDP aims to ensure data security, optimize resource usage, and comply with legal requirements, all while continuing to advance its development objectives. The policy categorizes data into critical, confidential, operational, and non-critical categories, with specific retention periods assigned to each type to maintain the integrity and availability of essential information. Additionally, it addresses data security through encryption and controlled access, archiving procedures, and the roles and responsibilities of staff to enforce the policy.

Purpose

The primary purpose of this Data Retention Policy is to establish a comprehensive framework for managing, retaining, and securely disposing of data within the National Development Programme (NDP). Given the nature of NDP's operations, which involve collecting vast amounts of sensitive data—such as participant information, financial records, and employee details—it is critical to ensure that this data is handled in a manner that meets both legal obligations and internal organizational needs. This policy serves multiple purposes, including but not limited to:

Legal and Regulatory Compliance: One of the foremost purposes of this policy is to ensure that NDP complies with all applicable data protection laws and regulations in Bangladesh, including the Information and Communication Technology Act, 2006, and other relevant industry-specific regulations. These laws mandate that certain types of data, such as financial records or personal identifiable information (PII), must be retained for specific periods and safeguarded against unauthorized access. Failure to adhere to these regulations could result in severe legal penalties, reputational damage, and loss of trust among stakeholders. This policy ensures NDP's full compliance, reducing the risk of regulatory breaches.

Data Security and Privacy Protection: The protection of sensitive data is vital to safeguarding the privacy and security of NDP's stakeholders, including programme participants, employees, and partners. This policy outlines stringent access control measures, encryption protocols, and backup strategies to ensure that sensitive data is stored securely and can only be accessed by authorized personnel. Additionally, it ensures that when data is no longer required, it is disposed of securely, preventing unauthorized recovery and use.

Efficient Data Management: A structured approach to data retention helps NDP optimize the management of its data resources. By defining specific retention periods for different categories of data—such as critical, confidential, operational, and non-critical—NDP can avoid storing unnecessary or outdated information, thereby reducing storage costs and improving data management efficiency. This policy establishes clear guidelines for when data should be archived or deleted, ensuring that only relevant data is retained, and clutter is minimized.

Business Continuity and Risk Mitigation: Data is a critical asset for NDP, supporting its decision-making, reporting, and operational functions. Retaining essential records for appropriate periods allows NDP to ensure business continuity, particularly in the case of audits, project evaluations, or legal disputes. This policy helps mitigate risks related to the loss of crucial data by ensuring regular backups, secure archiving, and the availability of critical information when needed. It also ensures that NDP can efficiently respond to requests for information, whether from internal stakeholders, regulatory bodies, or external partners.

Clarity on Roles and Responsibilities: A critical purpose of this policy is to define the roles and responsibilities of different departments and individuals within NDP in relation to data retention and security. Clear guidelines ensure that each department—whether MIS, HR, Finance, IT, or R&D—understands its obligations when it comes to managing the data under its purview. By establishing accountability, this policy minimizes the risk of mishandling or unauthorized access to sensitive data.

Supporting Organizational Growth and Strategic Planning: NDP's long-term sustainability and growth are dependent on informed decision-making based on accurate and reliable data. By ensuring that necessary data is retained for the correct duration and accessible when required, this policy supports effective project planning, evaluation, and reporting. It enables the organization to track its progress, measure outcomes, and make informed decisions for future programme development and resource allocation.

Environmental and Sustainability Goals: In alignment with NDP's commitment to sustainability, this policy also aims to reduce the environmental impact associated with excessive data storage, particularly in terms of physical records. By specifying clear timelines for the disposal of non-essential physical documents and encouraging the use of digital archiving, NDP can contribute to more eco-friendly practices.

Scope

This Data Retention Policy applies to all data collected, processed, stored, and disposed of by the National Development Programme (NDP) in the course of its operations. It covers both physical and digital data generated or received by NDP across various departments, including Management Information Systems (MIS), Human Resources (HR), Finance, Information Technology (IT), and Research and Development (R&D). The scope of this policy encompasses data related to project participants, employees, financial transactions, and other essential records, ensuring their secure retention and timely disposal in compliance with regulatory requirements and organizational needs. The scope of this policy includes the following key areas:

Project/Programme Participants' Data

NDP handles large amounts of data related to participants of its various development programmes and projects, including but not limited to demographic information, progress reports, and outcome evaluations. This data is crucial for tracking the impact of NDP's work and for reporting to donors and partners. The policy applies to:

Personal Data: Information that identifies individuals such as names, contact details, age, and other personal details of programme participants.

Project Performance Data: Reports, progress evaluations, and feedback forms that assess project outcomes.

Sensitive Data: Any health-related, financial, or personal data that requires additional safeguards.

This policy ensures that such data is retained for the required period based on project timelines, donor expectations, and legal mandates, while also providing clear procedures for securely archiving or deleting the data when it is no longer needed.

Financial Records

Financial data is one of the most critical areas covered by this policy. NDP manages various financial records related to operational budgets, payroll, donor funding, and procurement processes. These records are essential not only for day-to-day financial management but also for audits, donor reporting, and regulatory compliance. The scope includes:

Aleya Akhtar Banu
Chairperson
National Development Programme (NDP)

Md. Alauddin Khan
Executive Director
National Development Programme (NDP)

Transaction Records: Receipts, invoices, bank statements, and other financial transaction details.

Budget Reports: Annual, quarterly, and project-specific financial plans and expenditures.

Payroll Information: Employee salary records, tax documentation, and benefits information.

Audit and Tax Documents: Records required for external audits and compliance with Bangladesh's tax regulations.

This policy ensures the secure retention of financial records for specified durations (e.g., seven years) in compliance with accounting and regulatory requirements. It also outlines the procedures for archiving or disposing of these records securely once they are no longer required.

Employee Information

The HR department manages sensitive personal data related to NDP's employees, such as employment contracts, performance evaluations, disciplinary records, and payroll information. The policy applies to:

Personal Identifiable Information (PII): Employee names, addresses, national ID numbers, and other personal data.

Employment Contracts and Records: Documentation of employment terms, job descriptions, and performance appraisals.

Health and Benefits Information: Health insurance, retirement benefits, and leave records.

This policy ensures that employee data is retained throughout the employment period and for a set time afterward (e.g., five years after employment ends) in compliance with labor laws, and that it is securely archived or deleted as required.

Operational Data

NDP generates operational data as part of its everyday activities, such as meeting minutes, internal reports, communications, and administrative records. This data supports the functioning of NDP and its various departments. The policy applies to:

Meeting Minutes and Reports: Internal discussions, decisions, and progress reports.

Internal Communications: Emails, memos, and other forms of internal communication that document organizational operations.

This policy provides guidelines for how long operational data should be retained (typically two to three years), based on its relevance to ongoing organizational functions.

Digital and Physical Formats

The scope of this policy extends to data in both digital and physical formats. Digital data includes electronic files stored on servers, cloud platforms, or backup drives, while physical data includes paper documents such as signed contracts, printed reports, and handwritten records. This policy outlines distinct procedures for handling the retention and disposal of both formats to ensure consistency and security across all storage media.

Third-Party Data

NDP may engage third-party service providers to manage or process certain types of data, such as external payroll processors, financial auditors, or research collaborators. This policy applies to all data that third parties handle on behalf of NDP and establishes clear expectations regarding the secure storage, retention, and disposal of this data. Contracts with third parties must include provisions that ensure their compliance with NDP's data retention policy.

1. Data Across Departments

The policy is applicable to data managed by the following departments:

Management Information Systems (MIS): Ensuring data systems are secure and that project-related data is backed up and archived properly.

Human Resources (HR): Responsible for the retention and management of employee records, contracts, and performance-related data.

Finance: Responsible for ensuring financial records are securely stored and retained for the legally required period.

Information Technology (IT): Oversees digital security, access controls, and the technical aspects of data storage, encryption, and backups.

Exclusions

This policy does not apply to personal data or information that employees manage for personal use and not for organizational purposes. It also excludes any non-business-related communications or documents created outside of official NDP activities.

2. Legal and Regulatory Compliance

The National Development Programme (NDP) operates within a framework of legal obligations and regulatory requirements that govern how data is collected, stored, managed, and disposed of. As a Bangladeshi organization, NDP is bound by several local laws, including the Information and Communication Technology (ICT) Act, 2006, which provides clear directives on the management of electronic data, and various other regulations that pertain to data privacy and security. These legal frameworks aim to protect the privacy of individuals and organizations while ensuring that sensitive information is handled responsibly and securely.

NDP's commitment to legal and regulatory compliance is paramount to maintaining the trust of its beneficiaries, partners, employees, and stakeholders. The organization must ensure that its data management practices align with national laws concerning data protection and privacy. For example, certain categories of data, such as personally identifiable information (PII) or financial records, are subject to stringent legal requirements that dictate how long they must be retained and under what conditions they can be accessed, transferred, or disposed of. Failure to comply with these regulations can lead to severe consequences, including financial penalties, legal action, and reputational damage.

The policy also acknowledges the importance of compliance with sector-specific regulations, particularly those governing the non-profit and development sectors. NDP works closely with international partners, donors, and government agencies, many of whom may have additional data protection requirements. This means that the organization must be mindful of both local and international standards when handling sensitive information, especially data pertaining to project beneficiaries, financial transactions, and contractual agreements. Data retention periods must comply with the statutory requirements outlined in relevant regulations. For instance, financial records are often required to be maintained for several years to comply with auditing and taxation laws. Similarly, employee data must be retained for a specified period to comply with labor laws, and certain types of project data must be preserved for accountability and reporting purposes to donors. By adhering to these retention periods, NDP ensures that it remains compliant with the law while also preserving necessary records for audits, legal reviews, and future reference.

Moreover, NDP recognizes the need for data security and privacy, as stipulated by national legislation. The organization is responsible for safeguarding sensitive information against unauthorized access, breaches, or loss. This includes implementing robust security measures, such as encryption and access controls, to ensure that confidential and sensitive data is protected. Legal compliance also extends to the way data is transferred or shared with third parties. Contracts with external vendors or partners must clearly define the responsibilities of each party regarding data protection, ensuring that third-party data processors are fully compliant with NDP's standards and legal obligations.

In addition to ensuring compliance with existing regulations, NDP must remain adaptable to changes in the legal landscape. Laws and regulations surrounding data protection and privacy are evolving, particularly with the increasing digitization of data and the rise in cybersecurity threats. As such, the organization is committed to regularly reviewing and updating its data retention policies to ensure ongoing compliance. This includes keeping abreast of any new legislation, legal interpretations, or regulatory changes that may impact the way data is managed.

3. Data Classification and Categorization

To manage the various types of data handled by the National Development Programme (NDP), a structured classification system is essential. This system ensures that data is managed appropriately based on its sensitivity, importance to the organization, and applicable legal and regulatory requirements. The classification of data also helps determine the levels of access, retention periods, and security protocols needed for each type of information. NDP classifies its data into four main categories: Critical, Confidential, Operational, and Non-critical. These categories help define the level of protection and handling that each type of data requires, ensuring compliance with regulations while optimizing data management processes.

3.1. Critical Data

Critical data includes information that is essential to NDP's operational continuity, compliance with legal obligations, and overall functioning. Any compromise to the security, availability, or integrity of this data could result in significant harm to the organization, its beneficiaries, or partners. This data often has strict legal retention requirements, as well as a high level of security and controlled access.

Financial Records: This includes all transactional data, tax records, audit reports, budget documents, and payroll information. These records are essential for legal compliance, internal audits, and financial reporting. Financial records must be securely stored and retained for a minimum of 7 years, or longer, depending on specific regulatory requirements.

Contracts and Legal Agreements: Contracts with partners, donors, employees, and other stakeholders fall under this category. The retention of these documents is critical for legal and compliance purposes, ensuring NDP can meet its contractual obligations and respond to any disputes that arise.

Grant and Donor Information: Detailed data on grants, including donor agreements, project proposals, and financial disbursement records, are classified as critical, as they form the backbone of NDP's project funding.

Retention and Handling of Critical Data:

- Retention periods are typically 7 to 10 years, depending on legal mandates.
- High-level access controls and encryption must be applied.
- Regular audits are required to ensure compliance with both internal and external legal frameworks.

3.2. Confidential Data

Confidential data involves sensitive information that, if compromised, could harm NDP's beneficiaries, employees, or its reputation. This category of data is not necessarily subject to the same strict legal retention requirements as critical data, but it still requires a high level of protection to maintain privacy and confidentiality.

Employee Information: This includes personal identifiable information (PII), such as names, addresses, contact details, national identification numbers, employment contracts, and performance reviews. Employee data is critical for HR operations but also contains highly sensitive information that must be protected under privacy laws.

Participant and Beneficiary Data: Data related to individuals or communities who participate in NDP’s programmes or projects. This data often includes sensitive personal information, such as demographics, health information, socio-economic status, and progress tracking. Protecting this information is essential to uphold the trust between NDP and the communities it serves.

Retention and Handling of Confidential Data:

- Employee information must be retained for the duration of employment and an additional 5 years after termination.
- Participant data will typically be retained for 5 years after project completion, unless otherwise specified by regulatory or funding requirements.
- Strict access controls should be in place, with only authorized personnel granted access to confidential data.
- Data encryption both at rest and in transit is mandatory.
- Regular reviews and purging of outdated or irrelevant data must be conducted.

3.3. Operational Data

Operational data includes records and information that are necessary for the day-to-day functioning of NDP but do not have the same legal, financial, or privacy implications as critical or confidential data. While this data is essential for running operations smoothly, it generally has shorter retention periods and less stringent security requirements.

Meeting Minutes and Internal Reports: Documents related to internal meetings, project progress reports, and other administrative records fall under operational data. This information helps ensure NDP's projects and initiatives are on track but is not considered sensitive.

Project Documents: This includes internal project documentation, drafts, proposals, and communications related to the execution of projects.

Administrative Correspondence: Emails, memos, and other non-sensitive communication related to daily operations also fall under this category.

Retention and Handling of Operational Data:

- Typically retained for 3 years, after which it may be archived or deleted if no longer needed.
- Access to operational data should be role-based but does not require the same level of protection as critical or confidential data.
- Regular backups should be conducted to avoid accidental loss.

3.4. Non-Critical Data

Non-critical data comprises information that is of limited use or relevance to the organization's ongoing operations. This data often includes outdated records, drafts, and marketing materials that are no longer needed for business activities. While non-critical data can usually be discarded sooner than other types of data, it must still be handled securely to prevent unauthorized access during its storage and disposal phases.

Marketing Materials: Old versions of brochures, leaflets, or any other promotional content that is no longer in use.

Outdated Records: Historical documents or data that are no longer relevant to ongoing operations, such as old project plans, outdated contacts, or past event records.

Drafts and Temporary Files: Unused drafts of reports, documents, or files that have served their purpose but are no longer needed.

Retention and Handling of Non-Critical Data:

- Typically retained for a maximum of 1 year.
- After this period, data is either securely deleted or archived, depending on the potential future need.
- Access controls are minimal but must still prevent unauthorized access.
- Data Sensitivity and Access Controls

4. Data Retention Periods

The data retention periods outlined in this policy ensure that NDP complies with legal and regulatory requirements, operational needs, and best practices for data management. Each type of data has a designated retention period based on its importance, sensitivity, and legal obligations. These retention periods are intended to balance the need to retain critical data for operational and audit purposes while ensuring that unnecessary or outdated data is not stored longer than required, thus minimizing storage costs and reducing the risk of data breaches.

4.1. Critical Data

Critical data encompasses essential information that is fundamental to NDP's operations, legal compliance, and long-term strategic goals. This data must be retained for extended periods to meet legal, regulatory, and audit requirements.

Financial Records: NDP's financial records, including transaction reports, invoices, contracts, tax documents, and audit reports, are crucial for ensuring accountability and transparency. These records are subject to both national regulations and internal audit requirements. As such, NDP will retain financial records for a minimum of 7 years, in compliance with the taxation laws of Bangladesh. This period ensures that the organization can provide financial documentation if requested by auditors, donors, or legal entities.

Contracts and Agreements: Contracts signed with vendors, partners, donors, and government bodies form the backbone of legal agreements. NDP will retain these documents for a period of 10 years after their termination or expiry to protect the organization from potential legal disputes or claims.

Donor Agreements and Project Records: Agreements with donors and project reports are considered critical, especially when they involve financial or operational commitments. These documents must be retained for a minimum of 10 years after the completion of the project to meet donor reporting obligations and provide transparency.

4.2. Confidential Data

Confidential data includes sensitive information related to employees, beneficiaries, and proprietary organizational knowledge. Strict retention periods are applied to ensure data is not retained longer than necessary to reduce the risk of unauthorized access or data breaches.

Employee Records: This category includes personal identifiable information (PII), employment contracts, performance reviews, disciplinary actions, and payroll data. Employee records will be retained for the duration of their employment at NDP. Upon the employee's departure, either due to termination or resignation, their records will be retained for an additional 5 years. This ensures compliance with employment law and provides sufficient documentation should any post-employment disputes or inquiries arise.

Participant/Beneficiary Data: Data collected from project or programme participants, including personal information, progress reports, and assessments, is considered confidential. NDP will retain participant data for 5 years after the completion of the respective project. This retention period aligns with donor requirements and allows for reporting or evaluation purposes, while ensuring that data is not stored indefinitely.

Internal Communications: Sensitive communications involving management decisions, HR matters, or legal discussions are retained for 3 years after the discussion or decision has been concluded. These communications will be securely archived to ensure confidentiality and future reference.

4.3. Operational Data

Operational data includes the information necessary for NDP's day-to-day activities and business processes. This data may not be subject to strict legal retention requirements but is essential for organizational efficiency.

Meeting Minutes and Internal Reports: NDP regularly generates internal reports, meeting minutes, and operational documents that facilitate decision-making and strategy development. These documents will be retained for a period of 3 years to allow for operational continuity and institutional knowledge retention. After 3 years, they will either be archived for reference or securely disposed of if no longer relevant.

Project Implementation Data: Documentation created during the planning and implementation of projects, such as work plans, progress reports, and evaluations, will be retained for 5 years after the project's conclusion. This ensures that NDP has access to project history for future planning, assessments, and compliance with donor requirements.

4.4. Non-Critical Data

Non-critical data refers to information that, while useful in the short term, does not have long-term value to NDP. It is often generated during temporary or routine activities and can be safely deleted once its purpose has been served.

Marketing Materials: Drafts of promotional materials, event invitations, and campaign communications are categorized as non-critical data. These documents will be retained for a period of 1 year after their initial use, after which they will be securely deleted unless needed for historical reference or ongoing campaigns.

General Correspondence: Routine email communications or memos that do not contain critical or sensitive information are also classified as non-critical. These will be retained for 1 year before they are securely deleted.

5. Archival and Deletion Timelines

After the designated retention periods, data that is no longer needed for active use will be archived or securely deleted based on its classification:

Archiving: Data that still holds long-term value, such as project documentation or donor agreements, will be transferred to secure archival storage after its active retention period ends. This data will be retained in the archive for an additional 3-5 years before being re-evaluated for deletion.

Secure Deletion: Data that has reached the end of its retention period and no longer holds any operational, legal, or historical value will be securely deleted. For digital data, secure deletion methods such as data wiping will be employed to ensure that it cannot be recovered. Physical documents will be shredded or incinerated in compliance with national data protection regulations.

6. Secure Storage and Access Controls

The National Development Programme (NDP) recognizes the critical importance of ensuring that all data, especially sensitive and confidential information, is securely stored and accessible only to authorized personnel. This section outlines the protocols for securely storing both physical and digital data, defining access levels, and implementing robust security measures to protect data throughout its lifecycle.

6.1. Physical Storage Security

NDP stores various physical documents and records that require protection from unauthorized access, damage, or loss. The following measures are implemented to safeguard physical records:

Restricted Access: All physical records are stored in secure, access-controlled locations such as locked filing cabinets or designated storage rooms. Access to these areas is limited to authorized personnel, determined by the department heads (e.g., Finance, HR).

Security Protocols: Sensitive documents such as financial records, employee files, and project participant information are kept in designated secure areas with restricted access. The MIS, Finance, and HR departments have clear guidelines on who can access these documents, which are strictly monitored to prevent unauthorized access.

Aleya Akhtar Banu
Chairperson
National Development Programme (NDP)

Md. Alauddin Khan
Executive Director
National Development Programme (NDP)

Environmental Protection: Physical storage areas are equipped with fire alarms, surveillance cameras, and climate control systems to protect against environmental risks such as fire, humidity, or water damage. Regular inspections are carried out to ensure optimal storage conditions.

6.2. Digital Data Security

Given the increasing reliance on digital systems, NDP places significant emphasis on the secure storage of digital data. The following guidelines are established to ensure the protection of electronic records:

Role-Based Access Control (RBAC): NDP employs a role-based access control system to ensure that only authorized individuals can access certain types of data. Access rights are assigned based on job responsibilities and organizational roles, ensuring that employees can only view or modify the data necessary for their work.

Critical Data: Restricted to high-level management and authorized personnel from relevant departments (e.g., Finance, HR).

Confidential Data: Accessible only to employees directly involved in specific projects or tasks.

Operational and Non-Critical Data: Accessible to general staff as needed for daily operations.

Password Protection and Authentication: All digital data stored within NDP's systems, including servers, cloud platforms, and local databases, are protected by strong password policies. Passwords are regularly updated, and multi-factor authentication (MFA) is used for accessing sensitive systems to reduce the risk of unauthorized access.

Encryption: Sensitive data, such as participant information, financial records, and personal employee information, is encrypted both in transit and at rest. NDP uses industry-standard encryption methods (e.g., AES-256) to ensure that data remains secure, whether stored on internal servers, cloud platforms, or during transmission across networks.

Data Backup: Regular backups of all critical and confidential digital data are performed to ensure data recovery in case of accidental deletion, data corruption, or system failures. NDP maintains both on-site and off-site backups, with secure cloud backups being part of the overall data recovery strategy. Backup systems are tested periodically to verify their integrity.

Firewalls and Security Protocols: All systems used for storing digital data are protected by firewalls, intrusion detection systems (IDS), and other cybersecurity measures. Regular security audits are conducted to identify potential vulnerabilities and ensure compliance with security protocols.

6.3. Access Control Measures

To prevent unauthorized access and ensure data integrity, NDP enforces strict access control policies for both physical and digital data.

Authorization Protocols: Each department head is responsible for assigning access levels to their team members based on their roles. These access permissions are regularly reviewed to ensure that individuals only have access to the data necessary for their duties.

Audit Trails: For all sensitive or confidential digital data, audit trails are maintained to monitor who accesses or modifies the data. Any suspicious or unauthorized access attempts are flagged for immediate investigation by the IT department. These records are reviewed periodically to ensure compliance with the data retention policy.

6.4. Data Segmentation

To improve security, NDP segments its data based on sensitivity and usage requirements. This segmentation helps to apply appropriate access controls and storage measures for each type of data.

Critical and Confidential Data: Stored in separate, highly secure servers or databases with stringent access restrictions.

Operational and Non-Critical Data: Stored in general databases or servers with moderate security, as they do not contain sensitive information.

By segmenting data, NDP ensures that even if one system is compromised, the exposure of sensitive information is minimized.

6.5. Data Security Training

NDP ensures that all employees are adequately trained in data security protocols, including the proper handling, storage, and disposal of both physical and digital records. Regular training sessions are conducted to ensure staff members are aware of the latest data protection methods, security threats, and the importance of compliance with access control policies.

6.6. Data Breach Response Plan

In the event of a data breach, NDP has a comprehensive data breach response plan in place. This plan includes:

- Immediate containment of the breach.
- Notification of relevant authorities and stakeholders, including affected parties.
- A thorough investigation to determine the cause of the breach.
- Remediation steps to prevent future breaches, including system upgrades, employee retraining, and policy adjustments.

6.7. Periodic Security Audits

NDP conducts regular security audits and risk assessments to ensure that all physical and digital storage systems meet the required security standards. These audits are critical in identifying potential vulnerabilities and ensuring that access controls and encryption methods are up to date.

7. Archiving and Deletion Procedures

Managing data throughout its lifecycle is a critical component of NDP's commitment to data security and regulatory compliance. Data archiving and deletion are key processes that ensure information is preserved when necessary and securely disposed of when no longer required. These procedures are designed to safeguard sensitive information, optimize storage resources, and minimize the risk of data breaches or unauthorized access.

7.1. Archiving Procedures

Data archiving is the process of moving inactive or less frequently accessed data from primary storage systems to long-term storage solutions. The purpose of archiving is to retain data that is not actively in use but still required for compliance, auditing, or historical purposes.

7.1.1 Criteria for Archiving

Data will be archived when it is no longer required for day-to-day operations but still has value for legal, regulatory, or historical reasons. Archiving typically occurs after the following criteria have been met:

Completion of Projects: Data related to projects, such as participant information, reports, and financial transactions, will be archived upon the project's completion and when it is no longer actively used by NDP staff.

End of Financial Cycles: Financial records, such as budget documents, transaction logs, and audit reports, will be archived once a fiscal year is completed and reviewed.

Employee Data: For employees who have left the organization, personal and professional records will be archived after their employment has ended and the necessary review or audit has been completed.

7.1.2 Archival Methods

The archived data will be stored using secure methods that ensure both accessibility for legal or auditing purposes and the protection of sensitive information. The following archiving methods will be applied:

Digital Data: All digital data, including project files, financial records, and HR data, will be transferred to a dedicated archival server. This server will be separate from the main operational systems to ensure data is not accidentally modified or deleted.

Encryption: Archived data will be encrypted to protect sensitive information.

Access Control: Only authorized personnel, such as department heads or legal representatives, will have access to archived data.

Backup Systems: Archived data will be backed up on secure storage devices to prevent any loss in the event of a system failure.

Physical Data: Physical documents such as contracts, signed agreements, and financial statements will be moved to secure off-site storage facilities or designated archive rooms within NDP’s premises.

Environmental Controls: These storage areas will have environmental controls (e.g., temperature and humidity regulation) to ensure the long-term preservation of physical records.

Access Logs: Access to physical archives will be monitored and logged to maintain accountability.

7.1.3 Retention Periods for Archived Data

The retention periods for archived data vary depending on the type of data and applicable legal or regulatory requirements:

Project Data: Archived for a period of 5 years after the completion of the project or as required by donors and partners.

Financial Data: Retained for 7 years to meet local regulatory requirements.

Employee Data: Retained for 5 years after the end of employment.

7.2. Deletion Procedures

Once data reaches the end of its defined retention period, NDP will implement a secure and irreversible deletion process. Data that is no longer needed must be removed to mitigate risks related to unauthorized access, reduce storage costs, and ensure compliance with data protection regulations.

7.2.1 Criteria for Data Deletion

Data will be deleted when:

- It has fulfilled its purpose and is no longer required for NDP’s operations.
- The legally mandated retention period has expired.

- It is no longer needed for future references, audits, or compliance purposes.

7.2.2 Secure Data Deletion Methods

To ensure the complete and irreversible destruction of data, NDP follows the following secure deletion protocols based on the nature of the data:

7.3 Digital Data

Permanent Deletion: All digital data stored on NDP's servers or cloud platforms will be permanently erased using data wiping tools that ensure data cannot be recovered. This includes removing data from primary servers, archival servers, and backup systems.

Overwriting: For particularly sensitive data, NDP will use software tools that overwrite the data multiple times to prevent recovery through advanced techniques.

Decommissioning Storage Devices: Before any storage devices, such as hard drives or backup tapes, are decommissioned, they will be physically destroyed or securely wiped to ensure no data remains accessible.

7.4 Physical Data

Shredding: Paper records and physical media (e.g., CDs, DVDs) containing sensitive data will be shredded using cross-cut shredders. This process ensures that documents cannot be reconstructed or read.

Incineration: For particularly sensitive information or materials requiring higher security, incineration will be used as a destruction method, particularly for items like expired security badges, confidential legal documents, or obsolete identification materials.

7.4.1 Deletion Documentation

NDP will maintain a Deletion Log to track all data deletion activities for accountability purposes. This log will include:

- A description of the data that was deleted.
- The date the deletion took place.
- The method used for deletion.
- The department responsible for overseeing the deletion.
- Authorization from relevant managers or department heads to confirm the deletion.
- This log will be reviewed during regular audits to ensure compliance with the Data Retention Policy.

7.5. Data Disposal Compliance

NDP's data deletion processes comply with national regulations, as well as any specific guidelines provided by donors or international partners. To avoid regulatory non-compliance, data deletion is carried out with extreme care, ensuring that sensitive information, especially related to financials or personal identifiable information (PII), is securely destroyed.

7.6. Exception Handling

In specific circumstances, NDP may retain data beyond its regular retention period. Such exceptions include:

Ongoing Legal Actions: Data related to active legal cases or investigations will be preserved until the resolution of the case.

Audit Requirements: If a regulatory audit is underway or anticipated, relevant data will be retained until the audit is completed.

Special Requests from Donors: Data related to donor-funded projects may be retained longer if requested by the funding agency.

8. Auditing and Monitoring

Auditing and monitoring are critical components of the data retention policy at National Development Programme (NDP). These processes ensure that the organization remains compliant with internal guidelines, regulatory requirements, and industry standards regarding the management, storage, and disposal of data. A well-structured auditing and monitoring framework not only helps in identifying areas of non-compliance but also serves to continuously improve the overall data management practices of the organization.

8.1. Purpose of Auditing and Monitoring

The primary purpose of auditing and monitoring is to verify that the data retention practices across all departments—MIS, HR, Finance, IT, and R&D—are in strict alignment with the policy. Audits ensure that:

- Data is being retained for the appropriate amount of time according to its classification (critical, confidential, operational, or non-critical).
- The secure storage and deletion protocols are followed to protect sensitive data from unauthorized access or breaches.
- Retention schedules are adhered to, ensuring that outdated or unnecessary data is properly archived or securely deleted in a timely manner.
- All employees, contractors, and third-party partners are complying with the organization's data retention policies.

8.2. Audit Frequency

Audits are conducted annually by the Internal Audit Team to ensure that the data retention policy is being followed across all departments. However, additional audits may be conducted under the following circumstances:

Aleya Akhtar Banu
Chairperson
National Development Programme (NDP)

Md. Alauddin Khan
Executive Director
National Development Programme (NDP)

Regulatory Changes: If new laws or regulations related to data retention come into effect, immediate audits will be conducted to ensure compliance.

Internal Changes: If significant changes occur within NDP's operational processes, such as system upgrades or restructuring, an interim audit may be necessary.

Breach Investigations: In the event of a data breach or unauthorized access, a specialized audit will be conducted to assess the effectiveness of the policy and identify weaknesses.

8.3. Scope of Auditing

The scope of each audit includes, but is not limited to, the following:

Retention Schedules: Ensure that all types of data are retained for the specified durations as outlined in the policy.

Access Controls: Verify that access to sensitive data is restricted to authorized personnel only and that proper authentication measures are in place.

Archiving and Disposal Procedures: Confirm that data archiving is performed securely and that all data scheduled for deletion is permanently and securely erased.

Storage Security: Review the physical and digital storage methods to ensure they meet NDP's standards for data protection, including encryption, backups, and disaster recovery protocols.

Backup and Recovery: Assess the backup system to ensure that critical data can be recovered in case of data loss or system failure, while adhering to retention policies.

Policy Awareness: Assess whether all employees are adequately trained in the data retention policy and are following the correct procedures.

8.4. Audit Process

The auditing process at NDP follows a structured approach:

Pre-Audit Planning: Prior to conducting the audit, the audit team meets with department heads to define the audit objectives, scope, and areas to be examined. Departments will be informed of the audit schedule and any necessary data or documents that need to be prepared.

Data Collection: The audit team collects data from various departments, including system logs, access records, and retention schedules, to evaluate the organization's compliance with the data retention policy. They will also review physical storage locations and perform checks on archived and deleted data.

Data Review and Analysis: Collected data is analyzed to identify discrepancies, gaps, or breaches in the policy. This includes reviewing whether data is being retained longer than necessary or whether sensitive information is being improperly accessed or stored.

Audit Reporting: After completing the review, the audit team compiles a detailed report outlining the findings. The report will highlight:

- Areas of compliance
- Areas of non-compliance
- Risks identified, such as potential data security vulnerabilities or improper retention practices
- Recommendations for corrective actions and improvements.

Corrective Actions: Following the audit report, the relevant departments will be given a specific timeframe to address the identified issues. This may include implementing stricter access controls, improving data deletion protocols, or updating training programs.

Follow-Up Audits: In cases where significant non-compliance is identified, follow-up audits will be conducted within a set period (e.g., 3-6 months) to ensure that corrective actions have been successfully implemented.

8.5. Monitoring Mechanisms

In addition to formal audits, continuous monitoring mechanisms are in place to ensure real-time compliance with the data retention policy:

Automated Alerts: NDP's IT department uses software systems that automatically track data retention periods and send alerts when data is due for archiving or deletion.

Access Monitoring: Real-time monitoring of access logs is conducted to detect any unauthorized attempts to access sensitive or confidential data. Any anomalies are reported immediately to the Internal Audit Team and IT Security.

Backup Monitoring: Regular checks on backup systems ensure that backups are performed correctly and that data recovery processes are functioning as intended.

8.6. Reporting and Escalation

All findings from audits and monitoring activities are reported to NDP's Board of Directors and Executive Management Team. In the event of severe non-compliance or data breaches, immediate escalation procedures will be followed, including:

Notification to Regulatory Bodies: If data retention non-compliance results in legal breaches, relevant authorities will be informed in accordance with applicable laws.

Internal Investigation: The internal audit and IT security teams will conduct a thorough investigation to determine the cause of the breach and recommend remediation steps.

8.7. Policy Improvement

Audit and monitoring outcomes are used to continuously improve the data retention policy. Each audit cycle offers an opportunity to identify emerging risks, such as changes in technology or legal requirements, and adjust the policy accordingly. NDP is committed to evolving its data management practices to safeguard organizational data, ensure compliance, and optimize operational efficiency.

9. Communication and Training

Effective communication and training are critical components for ensuring the successful implementation and compliance of NDP's Data Retention Policy. All employees, contractors, and third-party partners who interact with or manage data must fully understand their roles and responsibilities in safeguarding sensitive information and adhering to data retention protocols.

9.1. Communication of the Policy

NDP is committed to making sure that the Data Retention Policy is well communicated across all levels of the organization. The following steps will be taken to ensure that the policy is accessible and understood by all relevant personnel:

Internal Communication Channels: The Data Retention Policy will be made available on NDP's internal platforms, such as the organization's intranet, email newsletters, or a designated policy portal. All employees will have access to the policy, and its importance will be highlighted during team meetings and internal communications.

Policy Awareness Campaigns: NDP will conduct awareness campaigns that include presentations, workshops, or seminars explaining the critical aspects of the policy, why it is necessary, and how it aligns with the organization's goals. Posters, infographics, and guides summarizing key points will be displayed in workspaces, ensuring the policy remains visible and understood.

Policy Updates: Whenever updates or changes are made to the Data Retention Policy, an official communication will be distributed to all departments. These updates will be accompanied by clear explanations of any changes and their implications. Employees will be required to acknowledge receipt of the updated policy and confirm their understanding through digital signatures or formal acknowledgments.

Communication to External Parties: Contractors, partners, and other third-party entities that work with NDP and have access to its data will also be informed about the Data Retention Policy. They will be required to adhere to the policy's standards and sign formal agreements that confirm their commitment to complying with NDP's data retention and protection guidelines.

9.2. Training Programs

To ensure full compliance and efficient implementation of the Data Retention Policy, NDP will conduct regular training sessions tailored to the needs of different departments. The objectives of these training sessions are to educate staff on best practices for data management, the importance of adhering to data retention schedules, and the security protocols required to protect sensitive data.

Onboarding Training: All new employees, upon joining NDP, will undergo onboarding training that includes a detailed session on the Data Retention Policy. During this training, new hires will be introduced to their data management responsibilities, the classification of data they will handle, and the specific retention and deletion protocols for their roles.

Department-Specific Training: Each department, such as HR, Finance, IT, and R&D, will have tailored training sessions relevant to the data they manage. For example, the Finance department will focus on retaining financial records, while the IT department will be trained on encryption, data security, and digital storage protocols.

Role-Based Access and Security Training: Employees will receive specific training on role-based access controls, emphasizing how they should handle sensitive data based on their access level. Staff will learn about encryption methods, password management, and secure handling of both physical and digital records.

Periodic Refresher Courses: To reinforce the importance of data retention and security, periodic refresher courses will be provided at least annually. These courses will revisit key concepts, address any updates to the policy, and introduce new practices or tools for improving data management.

Crisis Management and Data Breach Protocol Training: In case of data breaches, employees must know how to respond appropriately. Special training sessions will be conducted on how to report a breach, contain potential damage, and follow proper protocols to mitigate the risk. Employees will also be trained on how to safeguard data during emergencies or system failures.

9.3. Monitoring and Evaluation of Training Effectiveness

NDP will regularly assess the effectiveness of its training programs through various methods:

Feedback Surveys: After each training session, employees will be asked to provide feedback on the training content, clarity, and delivery. This feedback will be used to improve future training sessions.

Knowledge Assessments: Employees will undergo regular assessments, including quizzes or interactive exercises, to gauge their understanding of the Data Retention Policy. Employees who fail to demonstrate adequate knowledge will be required to attend additional training sessions.

Audit Reviews: During data retention audits, the audit team will evaluate how well employees are following the retention policies. Any gaps in understanding or compliance will be addressed with targeted training interventions.

9.4. Continuous Improvement in Communication and Training

As data management practices evolve and regulatory requirements change, NDP will continuously improve its communication and training efforts. The organization will stay updated on new technologies, data security trends, and changes in legislation to incorporate these into the policy and its training programs.

Conclusion

The National Development Programme (NDP) recognizes that efficient and responsible data management is crucial for both its operational success and its compliance with legal and regulatory obligations. By implementing this comprehensive Data Retention Policy, NDP aims to ensure that all data related to its project participants, employees, financial records, and operational activities are handled in a secure, transparent, and compliant manner. This policy not only safeguards sensitive information through secure storage, encryption, and access controls but also defines clear guidelines for the retention, archiving, and eventual secure deletion of data, minimizing risks associated with data breaches or non-compliance. The commitment to regular audits, reviews, and updates ensures that the policy remains relevant as NDP evolves, while tailored communication and training programs guarantee that all staff members and third-party partners are well-informed and actively participate in maintaining the integrity of data handling processes. By fostering a culture of accountability and awareness, NDP reinforces its dedication to upholding the highest standards of data protection, contributing to its overarching mission of sustainable development and community empowerment.

Aleya Akhtar Banu
Chairperson
National Development Programme (NDP)

Md. Alauddin Khan
Executive Director
National Development Programme (NDP)