Data Privacy and Protection Policy: V.1

Table of Contents

Objective

In course of its activities for the society, Tech Mahindra Foundation (TMF) handles and processes various types of data. To govern such activities, this Data Privacy and Protection Policy (DP3/Policy) has been framed. The purpose of this Policy is to establish internal guidelines for lawful, fair, and transparent collection, usage, storage, sharing, and protection of personal data handled by Tech Mahindra Foundation. TMF is committed to protecting the privacy of it's beneficiaries, employees, donors, volunteers, partners, vendors, and implementing agencies in line *with the Digital Personal Data Protection Act, 2023 (DPDP Act)*, the Information Technology Act, 2000, and related rules. This Policy serves as TMF's internal governance framework to ensure responsible data handling, privacy risk mitigation, and accountability across all operations.

Scope

This policy applies to all data which consists of personal information and sensitive personal information collected, processed or stored by TMF, including:

- Data collected from beneficiaries during enrolment, participation, monitoring, and reporting.
- Data collected from employees, interns, contractual staff and volunteers for HR administration, payroll, attendance, and compliance.
- Data collected from donors for donation records, engagement, and compliance.
- Data collected and processed by vendors, implementing agencies (IAs), and partners related to contractual or statutory obligations.
- Data stored in TMF's MIS, HR, payroll, attendance systems as well as in physical records.

Applicability

This Policy applies to all persons and entities involved in handling personal data under TMF operations, including:

- All TMF offices, programs, projects, and digital platforms operating within India.
- All TMF employees, contractual staff, interns and volunteers who access or handle Personal Data or Sensitive Personal Data.
- All vendors, consultants, implementing agencies (NGOs), and third-party service providers engaged by TMF who collect, process, or store personal data on its behalf.
- All digital and physical records maintained, processed, or managed by TMF, including those held in its MIS, HR, payroll, attendance, donor management, or partner systems.

This Policy shall be interpreted and enforced in accordance with the Digital Personal Data Protection Act, 2023, and, until fully superseded, the relevant provisions of the Information Technology Act, 2000 and any associated rules or notifications issued by the Government of India. For additional secure measures, extra steps have been built in by TMF.

Definitions (as per DPDP Act, 2023 and adapted for TMF)

4.1 Associate: An Associate includes all TMF employees, interns, volunteers, or contractual workers. Their personal data—such as contact details, attendance, salary, and performance records—is collected and processed for HR, payroll, and statutory compliance purposes.

4.2 Beneficiary: A Beneficiary is any individual who takes part in or receives support through TMF programs, projects, or initiatives. This includes students, Teachers, trainees, persons with disabilities (PwDs), or any person whose information is collected for enrolment, participation, assessment, placement, or support activities.

4.3 Board: The Data Protection Board of India established by the Central Government.

4.4 Certain Legitimate Uses: The specified purpose for which the Data Principal voluntarily provide their personal data to the Data Fiduciary, and in respect of which they have not indicated to the Data Fiduciary that they do not consent to the use of their personal data.

4.5 Consent: A clear, informed, voluntary agreement by the Data Principal to process their data for specific purposes.

4.6 Consent Manager: A person registered with the Board, who acts as a single point of contract to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform; for the purposes of this policy, Consent Manager shall additionally be working as Data Protection Officer (DPO) also.

4.7 Data Breach: A Data Breach is any unauthorized or accidental access, disclosure, alteration, destruction, or loss of personal data that compromises its confidentiality, integrity, or availability.

4.8 Data Fiduciary: The entity that decides why and how personal data is processed. In TMF's case, TMF acts as the Data Fiduciary responsible for determining the purpose and means of processing the data.

4.9 Data Principal: The individual whose personal data is processed, including beneficiaries, employees, donors, and, in case of minors or persons with disabilities (PwD), such minors/PwD along with their lawful guardians.

4.10 Data Processor: A person or organization (e.g., vendor, IA) that processes personal data on behalf of the Data Fiduciary, following their instructions and complying with data protection laws.

4.11 Data Protection Officer (DPO): The designated TMF official responsible for overseeing data protection compliance and being the point of contract for grievance redressal mechanism as per the law. Till Data Fiduciary is not notified by as Significant Data Fiduciary by the Government, the Consent Manager shall also hold DPO's responsibilities for internal compliance purposes.

4.12 Deemed Consent: Consent that is assumed or not explicitly obtained due to legal provisions, such as emergencies, legal obligations, or public interest activities.

4.13 Digital Personal Data: Digital Personal Data refers to any data about an individual who is identifiable by or in relation to such data; processed, stored, or transmitted electronically. This includes data collected via web forms, databases, email systems, servers, and other digital platforms.

4.14 Donor: A Donor is any individual, organization, or institution providing funds or resources to TMF programs. TMF may collect basic details of donors for communication, reporting, and compliance. Donors

who access or verify beneficiary data for monitoring purposes must follow TMF's privacy and data protection requirements.

4.15 Implementing Agency (IA): An Implementing Agency is an external Non-Profit organization working with TMF to run projects or programs. These agencies may collect and enter beneficiary data into TMF's Management Information System (MIS) and must keep all such data secure and confidential. They must also safely dispose of records as instructed by TMF and confirm data destruction in writing.

4.16 Partner: A partner is an individual, organization, or institution providing technical knowledge, resources or any other support to TMF programs, directly or indirectly, in a *non-financial* manner. TMF may collect basic details of partner/s for communication, reporting, and compliance. Partners who access or verify beneficiary data for monitoring purposes must follow TMF's privacy and data protection requirements. A partner, when transacting with TMF, when pays to TMF, immediately shall be treated as a Donor. Similarly, if the partner is paid by TMF, for it's support, it shall become a Vendor and the rules shall accordingly apply.

4.17 Personal Data (PI): Data about an identifiable individual, typically includes but is not limited to Full name, Date of birth, Gender, contact details (address, phone number, email), Educational qualifications, Employment information, Caste category, Marital status, Photographs, any other information that can directly or indirectly identify a person

4.18 Processing: In relation to personal data means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organization, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;

4.19 Sensitive Personal Data (SPI): Categories of Personal Data for which enhanced safeguards shall be applied, such data being more sensitive and harmful and discriminatory (to Data Principal) if misused. It includes, but is not limited to information related to Aadhaar, PAN, financial, health, biometric, caste, gender and/or disability. [DPDP Act, 2023 does not define Sensitive Personal Data, however, TMF has voluntarily created this special category for more security]

4.20 Vendor: A Vendor is any external company/firm/organization/individual, (a consultant or a service provider) engaged by TMF to deliver goods or services such as payroll, attendance, IT maintenance, website management, or data storage. Vendors who may access or process personal data on TMF's behalf are bound to follow TMF's data protection and confidentiality rules, as per this policy and otherwise.

Core Principles of Data Privacy

Tech Mahindra Foundation (TMF) follows eight core principles of data privacy, consistent with the Digital Personal Data Protection Act 2023 and internal governance standards.

All Associates, Implementing Agencies, vendors, and partners must apply these principles while processing personal data.

5.1 Fair and Lawful Processing:

Personal data shall be collected and used fairly, lawfully, and only for defined and authorized purposes.

5.2 Purpose Limitation:

Data must be processed solely for the program, project, HR, donor, or compliance purpose for which it was collected. Any new use requires DPO approval.

5.3 Data Minimization:

Only data strictly necessary for the intended purpose shall be collected and retained.

5.4 Accuracy:

Data must be kept accurate and updated. Individuals shall have the means to request correction through the DPO.

5.5 Storage Limitation:

Data shall be retained only for as long as necessary to fulfil the lawful purpose for which it was collected, including the duration of TMF's programs, projects, or related statutory obligations

Where continued retention is required for program analysis, reporting, or to prevent duplicate enrolments, data may be preserved in anonymized or aggregated form.

TMF will periodically review stored data to ensure its ongoing necessity and will securely delete, archive, or anonymize records that are no longer required.

5.6 Respect for Data Subject Rights:

TMF shall uphold Data Principal's rights to access, correction, erasure, and withdrawal of consent within prescribed timelines.

5.7 Transparency:

Individuals must be informed of how their data is collected, used, shared, and protected through TMF's privacy notices and communications.

5.8 Security:

Appropriate technical and organizational safeguards—such as encryption, access control, and audits—shall be applied to prevent unauthorized access or misuse.

Salient Features

6.1 Beneficiaries' Data

- Collected during enrolment and delivery of program.
- Used for program delivery, data analysis, forecasting, impact assessment (anonymized where feasible) and or for internship/training/placement purposes.
- Stored securely in MIS servers with role-based access.
- Shared with regulators/donors only as required or with consent.
- Beneficiaries have the right to access, correct, delete, withdraw consent, and request/raise grievances with the DPO.
- Beneficiaries shall execute a Beneficiary Data Privacy Declaration prior to collection of data, in the format as provided under Annexure 3 herewith.

6.2 Associate's Data

- Collected for HR, payroll, and compliance.
- Stored in HR/payroll/attendance systems with access controls.
- Shared with vendors only for payroll/statutory purposes.
- Retained during employment and statutory retention periods.

6.3 Donors' Data

- Collected for receipts, engagement, and compliance.
- Stored securely in donor management systems.
- Shared only with regulators/auditors where required by law.
- Donors shall execute the Non-Disclosure and Data Processing Agreement (NDPA) as per the template annexed as Annexure – 4.

6.4 Vendors' Data

- Collected for onboarding, payments, and compliance.
- Stored securely in vendor/finance systems.
- Vendors must sign Non-Disclosure and Data Processing Agreements (NDPAs) and comply with privacy requirements. The Vendors who both store and process data on their servers are required to execute the NDPAs as per the format provided under Annexure -1. The Vendors who only process data without storing it, will sign the NDPA as per the format under Annexure -2.

6.5 Implementing Agencies' Data Handling

- Implementing agencies engaged by TMF collect beneficiary data and directly enter it into TMF's MIS.
- Implementing agencies shall sign NDPAs as provided under Annexure- 6 and must ensure all their staff handling data, sign NDPAs on confidentiality and data protection as per the format provided under Annexure - 7.
- Implementing agencies must store data securely and prohibit unauthorized sharing.
- At program end or annually, implementing agencies must shred physical data and delete digital copies, unless otherwise approved by TMF.
- Implementing agencies must provide TMF with a written certification on official letterhead confirming data destruction or retention status (in case requested by TMF or in compliance of any applicable law).
- Implementing agencies not to share beneficiary data externally without TMF's prior written approval.

6.6 Data Security

TMF enforces encryption, restricted access, and periodic audits for all systems.

6.7 Data Retention and Disposal

- Data retained for legal, donor, or project requirements.
- Secure destruction of physical and digital records upon expiry.
- IAs required to certify compliance in writing.

6.8 Data Breach Management

- All breaches reported promptly to the DPO.
- Notifications made to regulators and affected individuals where legally required.

Associate Roles and Responsibilities

All associates of TMF (employees, volunteers, interns, and contractual staff) who handle Personal Data or Sensitive Personal Data are individually accountable for safeguarding such data. They must comply with this policy, the DPDP Act, 2023, and related guidelines issued by TMF, time to time.

The following responsibilities apply:

7.1 Adherence to Policies

- Associates must fully comply with all TMF data protection policies, standards, and procedures.
- Associates must understand and apply the Eight Core Principles of Data Privacy in their day-to-day work (as provided under Section 5 above).

7.2 Use of Authorized Devices and Credentials

- Only TMF-issued devices (desktops, laptops, MIS, HR systems) and login credentials may be used for accessing data.
- Use of personal devices or unauthorized applications for storing or processing Personal Data is strictly prohibited, unless explicitly approved by TMF IT/DPO.

7.3 Consent and Approval for Data Access

- Associates may only access Personal Data where proper consent has been obtained from the Data Principal.
- Additional approval from the relevant DPO is mandatory before processing sensitive data.

7.4 Consultation with DPO

- Before accessing or processing Sensitive Personal Data (SPI) such as Aadhaar, PAN, health data, caste, or biometric details, associates must consult TMF DPO.
- This ensures that data classification, risk mitigation, and necessary safeguards are in place.

7.5 Prohibition on Personal Use of Assets

- TMF's systems, devices, and data are strictly for business purposes.
- Associates are strictly prohibited from using data for personal gain, external communication, marketing, or unauthorized work.

7.6 Data Storage Restrictions

- Associates must not copy, download, or store Personal Data outside of TMF's authorized systems (e.g., MIS, HR, donor platforms).
- Data should never be stored on local hard drives, USB drives, or cloud accounts, which are personal.

7.7 Cloud Service Usage

- Any Cloud-based services may only be used if they are pre-approved by TMF DPO.
- Use of unapproved cloud apps (e.g., Google Drive, Dropbox, WhatsApp backups) for storing PI/SPI is forbidden.

7.8 Compliance with Donor and Partner Privacy Policies

- Associates working on donor-funded projects must comply with both TMF's policies and donor/partner data protection requirements, including contractual obligations.
- Any conflict of requirements must be escalated to the DPO for resolution.

7.9 Awareness and Reporting

- Completion of annual privacy and security training is mandatory.
- Associates must promptly report any suspected or actual incident related to privacy violation, data breach, or unauthorized access, to the DPO, using TMF's incident reporting mechanism.

7.10 Handling Hard Copy Data

- Associates must never leave printed personal data unattended.
- Physical data must be locked securely when not in use.
- Disposal must be done only using shredders or secure disposal bins.

7.11 Disciplinary Compliance

- Failure to comply with this policy may result in disciplinary actions under HR policies, up to and including termination.
- Severe breaches (such as intentional misuse, negligence, or unauthorized disclosure) may result in regulatory reporting to the Data Protection Board of India and legal consequences.

Detailed Policy and Roles & Responsibilities

8.1 TMF as Data Fiduciary

TMF acts as the Data Fiduciary, responsible for lawful collection, processing, and protection of all Personal and Sensitive Personal Data. Data shall be processed only with consent or under lawful basis, for defined purposes, ensuring accuracy, minimization, and appropriate safeguards. TMF upholds individuals' rights and reports any breach to regulators and affected persons as required by the DPDP Act 2023.

8.2 TMF as Data Processor

When TMF processes data on behalf of donors, partners, or government agencies, it shall follow their documented instructions, apply confidentiality and security controls, and restrict processing strictly to the agreed purpose. TMF shall not use or disclose such data for any unrelated purpose and it will promptly report incidents or breaches to the concerned fiduciary.

8.3 Vendors and IA's as Data Processors

All vendors and implementing agencies handling TMF data act as Data Processors and must sign valid NDPAs. They shall process data only as instructed, maintain adequate safeguards, restrict access to authorized staff, and provide compliance confirmations or audit reports when requested. Breach or misuse may result in contract termination and legal action.

8.4 Business Units and Program Heads

Program Heads and Functional Leads are accountable for ensuring lawful data handling within their operations. They must conduct Privacy Impact Assessments (PIAs), maintain Records of Processing Activities (ROPA), implement required safeguards, and ensure that vendors and NGOs comply with TMF privacy requirements and approved data-processing agreements.

8.5 Collection and Use of Data

Personal data shall be collected only for lawful, communicated and necessary purposes related to TMF programs, HR, donor engagement, or statutory requirements. Any new or secondary use must have explicit consent and prior DPO approval. Sensitive data shall be collected only when essential and approved and shall be handled with appropriate protection measures, as defined under this policy.

8.6 Data Security

TMF applies technical and organizational safeguards—encryption, access control, audit logging, and restricted storage—to prevent unauthorized access, loss, or misuse. Portable storage use is not allowed and shall be permitted in exceptional cases, only when the data is encrypted and approved by DPO. Physical data shall be stored securely and accessed only by authorized personnel.

8.7 Sharing and Transfers

TMF may share Personal or Sensitive Personal Data only for lawful and approved purposes related to its programs or statutory obligations. Data may be shared with authorized vendors, NGOs, donors, or authorities under signed NDPAs. Only the minimum data required shall be shared. Cross-border transfers shall be avoided as far as possible

and, if unavoidable, may occur only with CEO's prior approval under the guidance of the DPO. All sharing is documented and reviewed for compliance.

8.8 Retention and Disposal

Data shall be retained only for as long as required to serve its lawful or operational purpose, including program continuity, audit, reporting, or prevention of duplicate enrolments. Once no longer needed, records shall be securely deleted, anonymized, or archived per TMF's data-retention procedures. Program Heads and the DPO shall ensure periodic review and certified disposal by vendors or NGOs.

8.9 Incidents and Breaches

All suspected or actual data-privacy incidents or breaches must be reported immediately to the Data Protection Officer (DPO). The DPO shall record the incident, coordinate with the IT and relevant Program Heads to contain the breach, assess its impact, and implement corrective measures.

Where a breach risks exposure of Personal or Sensitive Personal Data, the DPO—under direction of the CEO—shall notify the Data Protection Board of India and affected individuals as required under the DPDP Act 2023.

Data Protection Officer (DPO) – Roles and Responsibilities

TMF shall designate a Data Protection Officer (DPO) who will:

- Act as the primary contact for data principals, regulators, and external stakeholders.
- Monitor compliance with this policy and the DPDP Act, 2023.
- Provide guidance on Privacy Impact Assessments (PIAs) and Records of Processing Activities (ROPA).
- Conduct regular training, awareness sessions, and audits.
- Oversee incident reporting, investigation, and breach notifications.
- Handle grievance redressal from beneficiaries, employees, and donors.
- Advise management on privacy risks and mitigation strategies.

Retention and Disposal

TMF retains Personal and Sensitive Personal Data only for the period necessary to achieve the purpose for which it was collected, including operational continuity, audit, donor, and statutory requirements.

Upon completion of the retention period or cessation of lawful purpose:

- Digital records shall be permanently deleted or anonymized using secure wiping tools.
- Physical records shall be shredded or incinerated under supervision.
- IAs and vendors shall confirm in writing the secure destruction or retention status of any TMF data held by them.

Aggregated and anonymized data may continue to be used for impact assessment, research, and statistical analysis in alignment with TMF's mission.

Monitoring and Compliance

- TMF conducts audits, risk assessments, and compliance checks.
- Non-compliance may lead to corrective action or escalation.

Children's Privacy

- Data of children under 18 years collected only with parental/guardian consent.
- Only minimal necessary data collected.
- Shared only with explicit guardian consent.
- Unlawfully collected children's data deleted promptly.

Data Handling Guidelines

A. Beneficiaries' Data

Category	Examples	Handling Guidelines	Retention Approach	Disposal / Anonymization
Personal Data (PI)	Name, Date of Birth, Gender, Contact Details, Education, Program ID	Stored in MIS with access restricted to authorized personnel.	Retained while the beneficiary participates in the program and for as long as records are needed for reporting, audit, or regulatory compliance.	Deleted or anonymized from MIS after DPO review confirming the purpose has ended.
Sensitive Personal Data (SPI)	Aadhaar, PAN, Bank Details, Caste, Health, Biometric	Encrypted; access restricted to authorized staff only.	Retained only until program and funding reconciliations are complete or longer if legally required.	Securely erased from digital systems; hard copies shredded or incinerated under DPO supervision.
Anonymized Data	Statistical or impact summaries	De-identified and used for analysis or forecasting.	May be retained indefinitely in aggregated, non-identifiable form.	—
Beneficiary Data handled by IA's	Data entered into TMF MIS (no local storage)	Access limited to unique logins; hard copies secured.	Retained only for current and immediately preceding program cycles.	Physical copies shredded annually or upon project end; confirmation provided to TMF.

B. Associates' Data

Category	Examples	Handling Guidelines	Retention Approach	Disposal / Anonymization

Personal Data (PI)	Name, Address, Employee ID, Contact Details	Stored in HR systems with controlled access.	Retained through employment and as long as required for statutory, tax, or audit obligations.	Securely deleted or archived after compliance confirmation.
Sensitive Personal Data (SPI)	Aadhaar, PAN, Bank, Salary, Biometric	Encrypted; processed by approved vendors only.	Retained for lawful HR and statutory purposes.	Secure erasure certified by vendor and HR Head.

C. Donors' Data

Category	Examples	Handling Guidelines	Retention Approach	Disposal / Anonymization
Personal Data (PI)	Name, Email, Address, Phone	Stored in donor databases with access control.	Retained while donor relationship or statutory record-keeping requirement continues.	Erased or anonymized after financial audits are complete.
Sensitive Personal Data (SPI)	PAN, Bank Details	Encrypted; used only for tax and compliance purposes.	Retained until completion of required filings and audits.	Deleted after statutory closure.

D. Vendors / IAs Data

Category	Examples	Handling Guidelines	Retention Approach	Disposal / Anonymization
Contract and Identity Data	Contact Names, Emails, Bank Details, PAN, Agreements	Stored in Project Management system / Drive with restricted access.	Retained while the contract is active and as required for audit or legal reference.	Secure deletion upon contract closure; vendor/NGO to certify destruction in writing.

E. General Provisions

1. Periodic Review: Program Heads and the DPO review stored data annually to verify necessity and initiate secure disposal where no lawful purpose remains.
2. Suspension of Deletion: If data is required for legal, audit, or investigation purposes, deletion may be deferred with DPO approval.
3. Documentation: All disposal actions must be recorded in the Data Disposal Register maintained by the DPO.
4. IA Certification: Each IA must annually confirm compliance with TMF's retention and destruction requirements on official letterhead.

Compliance and Disciplinary Actions

- All Associates must comply with this policy.
- Violations may result in disciplinary action under HR policies, including termination.
- Vendors/IAs/partners violating this policy may face contract termination, penalties, or legal action.
- Severe breaches may be reported to the Data Protection Board of India.

Acronyms & Abbreviations

The following acronyms and abbreviations are used in this Policy and shall have the meanings set forth below:

- TMF — Tech Mahindra Foundation. The Data Fiduciary responsible for determining the purpose and means of processing personal data under this Policy.
- DPDP Act — Digital Personal Data Protection Act, 2023. The Indian legislation governing processing of digital personal data.
- DPO — Data Protection Officer. TMF's designated officer responsible for data protection compliance, grievance redressal and acting as a point of contact for Data Principals and regulators.
- PI — Personal Information (Personal Data). Data relating to an identifiable individual (as defined in Section 4.16).
- SPI — Sensitive Personal Information (Sensitive Personal Data). Categories of personal data that require enhanced protection (as defined in Section 4.18).
- MIS — Management Information System. TMF's central digital system for storing and processing beneficiary and program data.
- ROPA — Records of Processing Activities. Documentation maintained by TMF or its Business Units that records the processing activities carried out (purpose, categories of data, recipients, retention, safeguards).
- PIA — Privacy Impact Assessment (also called Data Protection Impact Assessment). A risk assessment performed for new projects, systems, or processes that involve processing of PI/SPI.
- DPA — Data Processing Agreement. A contract between TMF (Data Fiduciary) and a Data Processor (vendor/IA) setting out data processing terms and obligations.
- NDPA — Non-Disclosure and Data Processing Agreement. TMF's template agreement combining confidentiality and data processing obligations for vendors/IAs that process TMF data.
- NDA — Non-Disclosure Agreement. A confidentiality undertaking (individual or corporate) to protect TMF Confidential Information.
- PII — Personally Identifiable Information. Alternative term sometimes used interchangeably with PI/Personal Data. (Used only where present in external documents.)
- SPI/PI — (When used together) denotes both Sensitive Personal Information and Personal Information categories.
- DPB — Data Protection Board of India. The regulatory body constituted under the DPDP Act for enforcement, adjudication, and guidance. (Referred to in the Policy as "Board".)

- NDPA (Vendor/IA) — Where referenced, indicates the applicable variant of the NDPA depending on vendor role (e.g., storage & processing, access-only, IA MIS-entry).
- PF / ESIC — Provident Fund / Employees' State Insurance Corporation. Statutory payroll-related schemes referenced when discussing payroll/vendor processing (used where applicable).
- IT Act — Information Technology Act, 2000. Indian law relevant to IT and cybersecurity obligations.
- TMF IT — TMF's Information Technology function/team responsible for systems, access, and technical security controls.
- HR — Human Resources (TMF HR function).
- GDPR — General Data Protection Regulation (EU). Mentioned only where comparative or international references occur in documents or vendor materials.
- SLA — Service Level Agreement. Contractual document describing service performance and availability standards for vendors.

List of Annexures:

- Annexure -1: sample NDPA format for vendors (Data storage in their server & Data processors)
- Annexure -2: sample NDPA format for vendors (Data processors)
- Annexure 3: Beneficiary Data Privacy Declaration format
- Annexure 4: Sample NDPA format for Doners (with whom we are sharing beneficiary data)
- Annexure 5: Generic Data Privacy policy for public use
- Annexure -6: NDPA with Implementing Agencies
- Annexure 7: NDPA Format for all Implementing Agency staff having access to MIS and beneficiary data

Annexure -1:

Non-Disclosure and Data Processing Agreement (NDPA)

(For Vendors Storing and Processing Data)

This Agreement ("Agreement") is entered into on this ___ day of _____, 20,

By and Between:

Tech Mahindra Foundation (TMF), a company registered under Section 25 of the Companies Act, 1956 (now Section 8 of the Companies Act, 2013), having its registered office at [Insert Address], hereinafter referred to as "TMF";

AND

[Insert Vendor/Service Provider Name], a company/firm having its registered office at [Insert Address], hereinafter referred to as the "Vendor."

TMF and the Vendor are collectively referred to as the "Parties" and individually as a "Party."

1. Purpose

TMF engages the Vendor to provide [Insert Services: e.g., payroll processing, attendance system, performance management, website hosting, data analytics, cloud infrastructure, etc.].

As part of these services, the Vendor will store and process personal and sensitive personal data ("Data") belonging to TMF's beneficiaries, employees, donors, volunteers, and partners on its own servers or hosted systems.

This Agreement defines the Vendor's obligations to maintain confidentiality and protect such Data in strict compliance with the Digital Personal Data Protection Act, 2023 (DPDP Act) and all other applicable Indian laws and regulations.

2. Definitions

- Personal Data (PI): Any data that relates to an identifiable individual, such as name, contact details, address, employee ID, enrollment ID, attendance, or performance records.
- Sensitive Personal Data (SPI): Includes Aadhaar, PAN, bank details, salary, caste, biometric, health/disability information, or any other category defined as sensitive by applicable law.
- Confidential Information: All TMF-related data, reports, credentials, and documents shared or generated under this Agreement, including PI/SPI, MIS records, HR/payroll data, attendance logs, donor records, and program information.
- Processing: Any operation performed on data, including collection, storage, access, transmission, analysis, disclosure, or deletion.
- Data Breach: Unauthorized access, use, disclosure, alteration, loss, or destruction of TMF data.
- Data Fiduciary: TMF, which determines the purpose and means of data processing.
- Data Processor: The Vendor, which processes TMF data on behalf of TMF.

3. Vendor Obligations

The Vendor agrees and undertakes to:

3.1 Lawful and Limited Processing

- Process TMF Data strictly for the purposes specified in this Agreement and only under TMF's documented instructions.
- Not collect or process any additional data not authorized by TMF.

3.2 Confidentiality

- Maintain strict confidentiality of all TMF Data and prevent unauthorized access, use, or disclosure.
- Ensure all Vendor staff, agents, or subcontractors who access TMF Data sign individual NDAs and complete privacy and data protection training.

3.3 Data Security and Storage

- Host TMF Data only on secure servers/data centres owned, leased, or managed by the Vendor within India.
- Implement industry-standard security controls (e.g., encryption, firewalls, access control, intrusion detection, regular vulnerability assessments).
- Maintain logical segregation of TMF Data from other clients' data.
- Retain access and activity logs for audit and investigation purposes.

3.4 Access Control and Authorization

- Restrict data access to authorized personnel with a legitimate need.
- Review and update access privileges quarterly.
- Immediately revoke access when an employee leaves or changes role.

3.5 Sub-Processor Management

- Not engage any subcontractor or third party for data handling without TMF's prior written approval.
- Ensure approved sub-processors follow equivalent data protection and confidentiality standards.

3.6 Data Retention and Disposal

- Retain TMF Data only for the duration of the Agreement or as required by law.
- Upon completion, termination, or TMF's written instruction:
    - Return all TMF Data in an agreed format;
    - Permanently delete or destroy all digital and physical copies; and
    - Provide written certification of destruction signed by an authorized representative.

3.7 Breach Notification and Incident Management

- Notify TMF within 24 hours of discovering any Data Breach or system compromise.
- Provide a written report detailing the nature of the breach, affected data, and mitigation measures.
- Cooperate fully with TMF in containment, investigation, and remediation.

3.8 Cross-Border Data Transfer

- Not transfer or host TMF Data outside India unless specifically permitted under the DPDP Act and with TMF's prior written consent.

3.9 Audit and Inspection Rights

- Permit TMF or its authorized auditors to inspect Vendor systems, policies, and procedures related to TMF Data upon reasonable notice.
- Promptly implement any corrective actions directed by TMF following such audits.

3.10 Compliance and Indemnity

- Comply with the DPDP Act, IT Act 2000, and all related data privacy and cybersecurity regulations.
- Indemnify and hold TMF harmless from any loss, penalty, or liability resulting from the Vendor's non-compliance, negligence, or breach of this Agreement.

4. Data Ownership

All Personal and Sensitive Personal Data processed under this Agreement remains the exclusive property of TMF.

The Vendor acts solely as a Data Processor and shall not claim ownership, rights, or independent use of such Data.

5. Duration of Confidentiality

These obligations remain enforceable:

- Throughout the term of engagement; and
- For five (5) years after termination or longer if required by law.

6. Remedies and Enforcement

TMF reserves the right to:

- Suspend or terminate Vendor access for any non-compliance;
- Seek injunctive relief, financial damages, and other legal remedies;
- Report the breach to the Data Protection Board of India or other authorities as per the DPDP Act.

7. Governing Law and Jurisdiction

This Agreement shall be governed by and construed in accordance with the laws of India. Disputes shall fall under the exclusive jurisdiction of the courts at Pune

8. Entire Agreement

This Agreement constitutes the entire understanding between the Parties regarding confidentiality and data processing. It supersedes all prior communications, agreements, or arrangements.

9. Signatures

For Tech Mahindra Foundation (TMF)	For Vendor
Name: _____	Name: _____
Designation: _____	Designation: _____
Signature: _____	Signature: _____
Date: _____	Date: _____

Schedule A – Minimum Data Security Requirements

1. Servers must be protected by up-to-date antivirus and firewalls.
2. Data encryption (AES 256-bit or equivalent) both at rest and in transit.
3. Regular data backups, securely stored and encrypted.
4. Multi-factor authentication for administrative access.
5. Annual independent security audit or penetration testing.

Schedule B – Categories of Data Processed *(to be defined from vendor to vendor)*

The Vendor may process the following data categories:

- Employees: Name, ID, contact details, attendance, payroll, bank, and compliance data.
- Beneficiaries: Name, gender, contact, Aadhaar, caste, education, health, and program details.
- Donors: Name, address, email, PAN, bank, and contribution details.

Annexure -2

Non-Disclosure and Data Processing Agreement (NDPA)

(For Vendors with Access & Processing Only – No Storage)

This Agreement ("Agreement") is entered into on this ___ day of _____ 20__,

By and Between:

Tech Mahindra Foundation (TMF), a company registered under Section 25 of the Companies Act 1956 (now Section 8 of the Companies Act 2013), having its registered office at [Insert Address], hereinafter referred to as "TMF";

AND

[Insert Vendor/Service Provider Name], a company/firm having its registered office at [Insert Address], hereinafter referred to as the "Vendor."

TMF and the Vendor are collectively referred to as the "Parties" and individually as a "Party."

1. Purpose

TMF engages the Vendor to provide [Insert Services: e.g., MIS maintenance / IT support / system testing / audit services / data analytics support].

The Vendor will access and process personal and sensitive personal data ("Data") belonging to TMF's beneficiaries, employees, donors, volunteers, and partners within TMF's authorized systems only. The Vendor is not permitted to store, copy, or host TMF Data on its own servers or devices.

This Agreement defines the Vendor's obligations to maintain confidentiality and ensure data protection in compliance with the Digital Personal Data Protection Act 2023 (DPDP Act) and other applicable Indian laws.

2. Definitions

- Personal Data (PI): Information relating to an identifiable individual (name, contact details, address, employee ID, beneficiary enrolment ID etc.).
- Sensitive Personal Data (SPI): Aadhaar, PAN, bank details, salary, caste, biometric, health/disability information or any other data defined as sensitive by law.
- Confidential Information: All data, records, credentials, and reports shared or generated under this Agreement including PI/SPI, MIS data, attendance or payroll information, program reports, and system documentation.
- Processing: Any operation performed on data such as access, review, analysis, verification, reporting, or deletion.
- Data Fiduciary: TMF, which determines the purpose and means of processing.
- Data Processor: The Vendor, when accessing and processing TMF Data on its behalf.
- Data Breach: Any unauthorized access, disclosure, alteration, or loss of TMF Data.

3. Obligations of the Vendor

The Vendor shall strictly comply with the following obligations:

3.1 Authorized Access Only

- Access TMF Data solely through TMF-approved systems, networks, and credentials.
- Use only devices authorized by TMF; personal devices or unsecured networks are prohibited.

3.2 No Storage or Copying

- Shall not download, copy, print, screenshot, or otherwise store any TMF Data locally on servers, laptops, drives, or cloud accounts.
- Temporary technical copies (e.g., browser cache or log files) must be deleted immediately after use.

3.3 Confidentiality and Staff Accountability

- Ensure that only authorized, trained employees handle TMF Data.
- Require each authorized employee to sign an individual confidentiality undertaking.
- Maintain a current list of authorized users and share it with TMF quarterly.

3.4 No Secondary Use

- Use TMF Data solely for the contracted service purpose and not for any personal, commercial, or analytical use unrelated to TMF's instructions.

3.5 Access Revocation

- Immediately disable system access for any employee who leaves the Vendor's organization or project.
- Inform TMF within 24 hours of such changes.

3.6 Data Breach Notification

- Notify TMF within 24 hours of any actual or suspected Data Breach or unauthorized access.
- Provide full incident details and cooperate in investigation and remediation.

3.7 Security Controls

- Implement strong authentication (MFA), session timeouts, and encrypted connections for all access.
- Keep antivirus and system patches up to date.
- Segregate TMF Data from other client data in any shared infrastructure.

3.8 Audit and Inspection

- Allow TMF or its authorized representative to audit processes and controls related to TMF Data upon reasonable notice.
- Implement corrective actions as advised by TMF post-audit.

3.9 Compliance and Indemnity

- Comply with the DPDP Act 2023, the Information Technology Act 2000, and related rules.
- Indemnify and hold TMF harmless from any loss, claim, penalty, or damage arising from breach, negligence, or non-compliance by the Vendor or its employees.

4. Data Ownership

All Personal and Sensitive Personal Data accessed under this Agreement shall remain the exclusive property of TMF.

The Vendor acknowledges that it acts only as a Data Processor and has no ownership or retention rights over the Data.

5. Duration of Confidentiality

Vendor obligations shall remain in force:

- During the term of engagement; and
- For five (5) years after termination of this Agreement or longer if required by law.

6. Remedies and Enforcement

In the event of breach or unauthorized use of TMF Data, TMF may:

- Suspend or terminate Vendor access immediately;
- Seek injunctive relief and claim financial damages;
- Report the incident to the Data Protection Board of India as mandated under the DPDP Act.

7. Governing Law and Jurisdiction

This Agreement shall be governed by and construed in accordance with the laws of India. Any dispute shall be subject to the exclusive jurisdiction of the courts at Pune.

8. Entire Agreement

This document represents the entire understanding between the Parties with respect to confidentiality and data processing and supersedes all prior arrangements or communications.

9. Signatures

For Tech Mahindra Foundation (TMF)	For Vendor
Name: _____	Name: _____
Designation: _____	Designation: _____
Signature: _____	Signature: _____
Date: _____	Date: _____

Schedule A – Minimum Security and Access Requirements

1. All user accounts must use strong passwords and multi-factor authentication.
2. System access limited to approved IP ranges or VPNs.
3. No data export or file transfer from TMF systems without written approval.
4. Automatic logout after period of inactivity.
5. Audit trails retained for a minimum of 90 days for forensic review.

Schedule B – sample Categories of Data Accessed

Depending on the scope of services, the Vendor may access the following data categories within TMF systems:

- Employee Data: Name, ID, attendance, role, performance, payroll records.
- Beneficiary Data: Name, gender, contact details, education, program participation.
- Donor Data: Name, email, contact details, donation records.

Annexure 3

Tech Mahindra Foundation

Beneficiary Data Privacy Declaration

Program Name: _____
Location/Center: _____
Date: _____

Declaration

I, _____, accept, agree and declare as follows:

1. Privacy Notice: The *Privacy Notice* of Tech Mahindra Foundation (TMF), available at www.techmahindrafoundation.org/data-privacy-policy, has been read by me / explained to me. I have understood its contents and agree with them.
2. Information Collected: I understand that TMF will collect and record details necessary for program participation and reporting, which may include My:
    - Name, contact details, address, age, and gender.
    - Educational and employment background.
    - Family and income details.
    - Aadhaar number or other identification information.
    - Health or disability details (where relevant).
    - Program-related data such as enrolment, attendance, assessments, placements, and photographs/videos.

3. Consent for Use and Retention:

I grant my consent to TMF for:

- Collecting, storing, and processing my personal and sensitive personal data securely in TMF's MIS and related systems.
- Retaining my data for the duration of the program and as long as required for lawful, reporting, or audit purposes; after which it may be anonymized or securely deleted.
- Using my data for program delivery, training, placement, support, and communication.
- Using my data in anonymized form for analysis, forecasting, and donor or government reporting.
- Sharing my data only with authorized partners, donors, or statutory authorities where required by law and in line with TMF's Data Privacy and Protection Policy.

4. Data Protection:

I understand that TMF will maintain appropriate security controls to protect my data and will never sell or misuse it.

5. **My Rights:**

   I understand that under the Digital Personal Data Protection Act 2023, I have the right to:

   - Request access to or correction of my data.
   - Request deletion of my data when no longer legally required.
   - Withdraw my consent at any time by contacting the Data Protection Officer (DPO) of TMF.

6. **Consent by Guardian (if under 18 years):**

   If I am below 18 years of age, my parent or guardian will review and sign this declaration to provide consent on my behalf.

Beneficiary Details

Full Name: _____
Age: _____
Gender: _____
Signature / Thumb Impression: _____
Date: _____

Parent / Guardian Declaration

(To be completed if beneficiary is below 18 years of age)

I, _____, confirm that I am the _____ of the above beneficiary.

I consent to the collection, storage, processing, and lawful retention of the beneficiary's personal and sensitive data by TMF for the stated program [insert program name], in accordance with TMF's Data Privacy and Protection Policy and the Digital Personal Data Protection Act 2023.

Parent / Guardian Details

- Name: _____
- Relation to Beneficiary: _____
- Aadhaar Number: _____
- Signature: _____
- Date: _____

For Office Use Only

TMF Representative Name: _____

Signature: _____

Date: _____

Annexure 4:

Non-Disclosure and Data Processing Agreement (NDPA)

(Between Tech Mahindra Foundation and Donor)

This Agreement ("Agreement") is entered into on this ___ day of _____, 20,

By and Between:

Tech Mahindra Foundation (TMF), a company registered under Section 25 of the Companies Act, 1956 (now Section 8 of the Companies Act, 2013), having its registered office at [Insert Address], hereinafter referred to as "TMF";

AND

[Name of Donor / Donor Organization], having its principal place of business at [Insert Address], hereinafter referred to as the "Donor."

TMF and Donor are collectively referred to as the "Parties" and individually as a "Party."

1. Purpose

TMF may share or provide access to beneficiary data and related program information with the Donor for the purpose of program monitoring, reporting, verification of data accuracy, compliance, and evaluation. This Agreement sets out the Donor's obligations to maintain confidentiality and process such data in accordance with applicable laws, including the Digital Personal Data Protection Act, 2023 (DPDP Act).

2. Definitions

- Confidential Information: Includes all personal data and sensitive personal data of beneficiaries, employees, volunteers, or donors, such as name, contact details, Aadhaar, PAN, caste, health/disability information, education, employment, photographs, program-related records, MIS data, and any related reports or analysis.
- Processing: Any operation performed on beneficiary data, including collection, recording, verification, storage, use, disclosure, analysis, or deletion.
- Sensitive Personal Data (SPI): Includes Aadhaar, PAN, caste, bank details, health/disability status, or biometric data, which requires higher safeguards.

3. Obligations of the Donor

The Donor agrees to:

1. Use Limitation – Process beneficiary data only for the purposes defined in Section 1 and not for personal, commercial, or unauthorized use.
2. Lawful Processing – Ensure all processing complies with the DPDP Act, 2023 and related regulations.
3. Confidentiality – Keep all beneficiary data strictly confidential and prevent unauthorized disclosure.
4. Data Security – Implement appropriate technical and organizational safeguards (encryption, access controls, restricted access) to protect beneficiary data.

5. Authorized Personnel Only – Limit access to only those donor representatives who require the data for authorized program purposes and ensure they are trained in confidentiality and data protection.
6. No Third-Party Sharing – Not transfer or disclose beneficiary data to any third party without prior written approval from TMF.
7. Accuracy and Verification – Process data for accuracy verification only to the extent necessary and report any discrepancies back to TMF.
8. Data Breach Notification – Immediately notify TMF of any breach, unauthorized access, or misuse of beneficiary data and cooperate in investigations and remedial actions.
9. Return/Destruction of Data – Upon program completion, termination of the relationship, or at TMF's request, return all beneficiary data or permanently delete/destroy it and provide written certification of destruction.

4. Data Ownership

All beneficiary data and Confidential Information remain the exclusive property of TMF. The Donor acknowledges that it acts as a Data Processor for such data and will not claim ownership or independent rights over it.

5. Duration of Confidentiality & Processing

The Donor's confidentiality and data protection obligations will remain:

- During the donor relationship with TMF; and
- For five (5) years after termination of the relationship, unless a longer duration is required under applicable laws.

6. Remedies

The Donor acknowledges that unauthorized use or disclosure of beneficiary data may cause irreparable harm to TMF and its beneficiaries. TMF is entitled to seek injunctive relief, damages, or other legal remedies for breach of this Agreement.

7. Governing Law and Jurisdiction

This Agreement shall be governed by and construed in accordance with the laws of India. Any disputes arising shall be subject to the exclusive jurisdiction of the courts at [Insert Location].

8. Entire Agreement

This Agreement constitutes the entire understanding between the Parties with respect to beneficiary data confidentiality and processing and supersedes all prior discussions or arrangements.

9. Signatures

For Tech Mahindra Foundation (TMF)

Name: _____

Designation: _____

Signature: _____

Date: _____

For Donor

Organization: _____

Authorized Representative: _____

Designation: _____

Signature: _____

Date: _____

Annexure 5:

Tech Mahindra Foundation

Privacy Notice for Beneficiaries and Donors

Effective Date: [Insert Date]

1. Who We Are

Tech Mahindra Foundation (TMF) is the Corporate Social Responsibility arm of Tech Mahindra Limited. We run education, employability, and inclusion programs across India.

We are committed to protecting your privacy and handling your personal information responsibly, in line with the Digital Personal Data Protection Act, 2023 (DPDP Act) and TMF's Data Privacy and Protection Policy.

2. What Data We Collect

For Beneficiaries (Students):

We may collect the following types of personal and sensitive personal data through admission, enrolment, and participation forms:

- Identity Details: Name, date of birth, gender, marital status, category (SC/ST/OBC/Minority/General), nationality.
- Contact Information: Address (permanent and correspondence), phone numbers (student, parent/guardian), email ID.
- Education & Employment: Highest qualification, stream/specialization, marksheets, certificates, employment details (employer, designation, salary, work experience).
- Government Identification: Aadhaar number, Aadhaar enrolment ID, PAN, voter ID, driving license, or passport (as applicable).
- Sensitive Personal Data (SPI): Aadhaar, PAN, caste certificate, health information (blood group, disability type, health status), biometric identifiers (if collected for attendance).
- Family & Income Details: Parent/guardian/spouse details, occupation, family income, number of family members.
- Other Details: Source of referral, photographs, videos, case studies, consent for social media/publicity use.
- Documents: Self-attested copies of educational certificates, Aadhaar, caste or disability certificates, photographs.

For Donors:

- Contact details: Name, phone, email, address.
- Donation details: Amount, date, purpose.
- PAN or bank details (when required for tax receipts and compliance).

3. How We Use Your Data

We use your data only for:

- Delivering, monitoring, and reporting on TMF's education and employability programs.
- Communicating with you regarding admission, training, placement, or program updates.
- Issuing donation receipts and complying with statutory requirements.
- Improving our services through data analysis and forecasting (with data anonymized where feasible).

We do not share your personal data outside TMF without your explicit consent, unless required by law or by authorized donors/regulators.

4. How We Store and Protect Your Data

- Beneficiaries' data is stored securely in TMF's MIS system with access restricted to authorized staff.
- Donors' data is stored securely in donor management systems.
- Sensitive data (such as Aadhaar, PAN, caste, bank, or health details) is encrypted and disclosed only where legally required or contractually permitted.
- IAs and vendors working with TMF must follow strict confidentiality, enter data directly into TMF's MIS, and certify secure destruction of physical/digital records when no longer required.

5. Your Rights

Under the DPDP Act, 2023, you have the right to:

- Access your personal data held by TMF.
- Request corrections to inaccurate or incomplete data.
- Ask for deletion of your data (unless retention is required by law).
- Withdraw consent for future processing of your data.
- Raise grievances with TMF's Data Protection Officer (DPO).

If you are not satisfied with TMF's response, you may escalate your complaint to the Data Protection Board of India.

6. Data Sharing

We may share your data with:

- Government authorities where legally required.
- Authorized vendors and IAs supporting TMF programs (bound by Data Processing Agreements and NDAs).
- Auditors, donors, and regulators for reporting and compliance.

All sharing is done securely, with safeguards, and only when necessary.

7. Contact Us

If you have any questions, concerns, or wish to exercise your rights, please contact:

Data Protection Officer (DPO): write to us Email: dpo@techmahindrafoundation.org

8. Consent Statement

By submitting your details through TMF's forms or website, you consent to TMF collecting, storing, and processing your data in accordance with this Privacy Notice and the DPDP Act 2023.

9. Policy Availability

Our full Data Privacy and Protection Policy is available at www.techmahindrafoundation.org/data-privacy-policy.

Annexure 6:

Non-Disclosure and Data Processing Agreement (NDPA)

(For Implementing agencies Entering Data Directly in MIS and Handling Hard Copies)

This Agreement ("Agreement") is entered into on this ___ day of _____, 20,

By and Between:

Tech Mahindra Foundation (TMF), a company registered under Section 25 of the Companies Act, 1956 (now Section 8 of the Companies Act, 2013), having its registered office at [Insert Address], hereinafter referred to as "TMF";

AND

[Insert Implementing agency Name], a registered organization having its office at [Insert Address], hereinafter referred to as the "IA."

TMF and the IA are collectively referred to as the "Parties" and individually as a "Party."

1. Purpose

The implementing agency is engaged by TMF to collect, verify, and directly enter beneficiary information into TMF's Management Information System (MIS) for implementation of TMF programs.

The IA may handle hard copies of beneficiary forms, ID proofs, and other supporting documents for verification and record-keeping.

This Agreement defines the IA's confidentiality and data protection obligations in accordance with the Digital Personal Data Protection Act, 2023 (DPDP Act) and other applicable Indian laws.

2. Definitions

- Personal Data (PI): Any information relating to an identifiable individual such as name, age, contact details, address, education, program enrollment ID, etc.
- Sensitive Personal Data (SPI): Aadhaar, PAN, bank details, caste, health/disability data, or any other category defined as sensitive under applicable law.
- Processing: Any operation performed on data such as collection, storage, access, transmission, analysis, or deletion.
- Confidential Information: All data, forms, reports, or information provided or collected under this Agreement, including PI/SPI, MIS data, physical records, and reports.
- Data Fiduciary: TMF, which determines the purpose and means of data processing.
- Data Processor: The IA, which processes TMF Data on TMF's behalf.
- Data Breach: Unauthorized access, loss, destruction, or disclosure of TMF data, whether physical or digital.

3. Obligations of the IA

The IA agrees to the following:

3.1 Data Collection and Entry

- Collect only the personal and sensitive personal data approved by TMF for program delivery.
- Enter all beneficiary data directly into TMF's MIS using official credentials.
- Ensure accuracy and completeness of data before submission.

3.2 Safe Custody of Hard Copies

- Store all physical beneficiary records (e.g., admission forms, ID proofs, attendance sheets) in locked cabinets or secure storage with controlled access.
- Limit access to authorized IA personnel who are trained and bound by confidentiality obligations.
- Maintain a register/log of who accessed the records and when.

3.3 Retention and Disposal of Hard Copies

- Retain physical documents for only the immediately preceding financial year.
- After the close of each financial year, the IA shall:
    - Shred all prior-year hard copies vertically (cross-cut preferred) to ensure non-retrievable destruction.
- In case of project completion, termination, or non-extension, the IA shall:
    - Immediately destroy all beneficiary-related physical and digital data (including PI and SPI).
    - Submit a data destruction certification on its official letterhead to TMF within 15 working days of termination.
    - Ensure no data copies remain in computers, mobile devices, or external drives.
    - Provide TMF with a written confirmation of shredding or safe disposal on the IA's official letterhead at the start of each new financial year.
    - Under no circumstances shall documents older than the last financial year be retained without TMF's written approval.

3.4 Termination or Non-Renewal of Project

- In case of project completion, termination, or non-extension, the IA shall:
- Immediately destroy all beneficiary-related physical and digital data (including PI and SPI).
- Submit a data destruction certification on its official letterhead to TMF within 15 working days of termination.
- Ensure no data copies remain in computers, mobile devices, or external drives.

3.5 Confidentiality and Staff Accountability

- All IA staff handling TMF data must:
    - Sign individual Non-Disclosure Agreements (NDAs) before gaining access.
    - Undergo TMF's privacy and data protection orientation.
    - Refrain from sharing, copying, or photographing beneficiary data.

3.6 Prohibited Activities

The IA shall not:

- Use TMF Data for any personal, promotional, or commercial purposes.
- Share or disclose data to third parties without TMF's written consent.
- Upload or store TMF data on any personal devices, cloud storage, or external systems.

3.7 Breach Notification

- Notify TMF within 24 hours of discovering any data breach, loss, or unauthorized access (digital or physical).
- Cooperate fully with TMF to investigate, contain, and mitigate any impact.

3.8 Compliance and Audit

- Comply with the DPDP Act 2023, IT Act 2000, and all applicable Indian data protection and cybersecurity regulations.
- Allow TMF or its authorized representatives to audit physical recordkeeping and MIS entry processes at reasonable notice.
- Implement corrective actions promptly as directed by TMF.

3.9 Indemnity

The IA shall indemnify and hold harmless TMF against any loss, claim, penalty, or liability arising from:

- Breach of this Agreement;
- Violation of confidentiality or data protection obligations;
- Failure to securely store or destroy data as per this Agreement.

4. Data Ownership

All beneficiary data—digital and physical—collected or processed under this Agreement is the exclusive property of TMF.

The IA acts only as a Data Processor and shall not claim ownership, rights, or control over such data.

5. Duration of Confidentiality

All obligations under this Agreement shall remain valid:

- During the tenure of the project; and
- For five (5) years after its termination or completion, unless a longer retention period is mandated by law.

6. Remedies and Enforcement

TMF reserves the right to:

- Suspend or terminate this Agreement in case of non-compliance;
- Seek injunctive relief and damages for breach;
- Report the incident to the Data Protection Board of India as required under the DPDP Act.

7. Governing Law and Jurisdiction

This Agreement shall be governed by and construed under the laws of India. Any disputes shall fall under the exclusive jurisdiction of the courts at [Insert Location].

8. Entire Agreement

This document constitutes the entire understanding between the Parties regarding confidentiality and data processing and supersedes all prior discussions, correspondence, or understandings.

9. Signatures

For Tech Mahindra Foundation (TMF)	For Implementing Agency
Name: _____	Name: _____
Designation: _____	Designation: _____
Signature: _____	Signature: _____
Date: _____	Date: _____

Schedule A – Minimum Physical and Digital Security Measures

1. Hard copies stored in locked cabinets within secure, access-controlled premises.
2. Access logs maintained for record retrieval and handling.
3. Shredding (vertical or cross-cut) performed using mechanical shredders.
4. No personal devices (e.g., mobile phones, USBs) permitted while handling forms.
5. TMF MIS access restricted to authorized users only, with unique credentials.
6. MIS passwords not to be shared or reused.
7. Annual written confirmation of safe disposal submitted on official letterhead.

Schedule B – Data Categories and Purpose

The IA may collect and process the following data strictly for TMF program purposes:

- Personal Data (PI): Name, gender, contact details, address, education, age, guardian name, and enrollment details.
- Sensitive Personal Data (SPI): Aadhaar, PAN, caste, bank details, health/disability data, and supporting identity documents.

Purpose: Beneficiary identification, enrollment, monitoring, reporting, and compliance.

Annexure 7:

NDA Format for all Implementing Agency (IA) staff having access to MIS and beneficiary data

Non-Disclosure Agreement (NDA) – Implementing agency Staff

I, _____[Full Name of Staff], working with _____[IA Name], in the role of _____ [Designation/Role], acknowledge that as part of my duties I will collect, enter, and/or access beneficiary data in the Tech Mahindra Foundation (TMF) Management Information System (MIS).

I understand and agree that:

1. **Confidentiality of Data**
    - I will treat all beneficiary data (personal and sensitive personal data) as confidential.
    - This includes names, contact details, Aadhaar, caste, education, attendance, and program participation records.
2. **Authorized Use Only**
    - I will use the MIS and the data only for program-related purposes as instructed by TMF and my organization
    - I will not share, copy, or use the data for any personal or unauthorized purpose.
3. **Data Security**
    - I will keep my login credentials safe and not share them with anyone.
    - I will access the MIS only through authorized devices/networks.
4. **No Unauthorized Disclosure**
    - I will not disclose any beneficiary data to anyone outside TMF or my organization without written approval.
5. **Return/Deletion**
    - On termination of my role, or when instructed, I will return or delete any beneficiary data in my possession.
6. **Consequences of Breach**
    - I understand that violation of this NDA may lead to disciplinary action by my organization, termination of my access to TMF MIS, and reporting to legal authorities under the Digital Personal Data Protection Act, 2023.

Staff Details

Full Name: _____

Designation/Role: _____

Implementing agency Name: _____

Signature: _____

Date: _____

Witness (Implementing Agency Supervisor/Manager)

Name: _____

Signature: _____

Date: _____

AMENDMENT HISTORY

Version	Date	Author	Reviewed by	Approved by	Nature of changes
1.0	22-10-2025	Chief Data Officer	Head HR	COO/CEO	First Integration Issue

Thank You

Visit us at techmahindrafoundation.org