DATA SECURITY AND GOVERNANCE POLICY

Effective from: _____

1. INTRODUCTION:

1.1. This Data Security and Governance Policy ("**Policy**") sets out the framework and practices adopted by Myna Mahila Foundation, including its subsidiaries, affiliates, successors, assigns and representatives worldwide (in connection with any activity pertaining to Data Principals within the territory of India) ("**MMF**") to ensure secure, lawful, and transparent handling of Data (as defined below) in accordance with applicable laws.

1.2. MMF agrees and acknowledges that, as the entity determining the purposes and means of processing Data, including Personal Data (as defined herein), it shall be responsible for ensuring compliance with all requirements under applicable laws. MMF further agrees and acknowledges that it shall ensure that any Data Processor engaged by it to Process such Data on its behalf complies with all such applicable requirements.

1.3. MMF is committed to the principles of data minimisation, purpose limitation, storage limitation, and accountability in handling Data of, *inter alia*, its employees, customers, vendors, service providers, and partners.

1.4. The Policy covers:

1.4.1. Physical Access

1.4.2. Digital Access

Unit No. 10/11, Building No. 34/A,
GM Link Road, Natwar Parekh
Compound, Govandi (W), Mumbai,
Maharashtra, India – 400 043

+91 720 888 0031
+91 932 612 7527

contact@mynafoundation.com

1.4.3. Access Monitoring

1.4.4. Data Security Audit

1.4.5. Loss, destruction or damage by accident or incident

1.4.6. Third party service providers

1.4.7. Data Security Breach

The Policy includes in its scope all Data which MMF collects either in hardcopy or digital copy.

1.5. The Policy applies to all employees, interns, volunteers, consultants, contractors, vendors, partners, third-party service providers, casual workers, agency workers, apprentices, whether temporary or permanent, and to all programs, projects, research, donor activities, community outreach, and advocacy efforts undertaken by MMF.

2. DEFINITIONS:

In the Policy, the following words and phrases have the following meanings:

3.1. "**Aggregated Data**" means Data that has been combined from several measurements and presented in summary form without identifying individuals.

3.2. "**Anonymisation**" means the irreversible process of transforming Personal Data to a form in which the Data Principal cannot be identified, directly or indirectly.

3.3. "**Automated**" means any digital process capable of operating automatically in response to instructions given or otherwise for the purpose of Processing Data.

3.4. "**Biometric**" means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', 'facial patterns', 'hand measurements' and 'DNA' for authentication purposes.

3.5. "**Child**" means an individual who has not completed the age of 18 (eighteen) years.

3.6. "**Consent**" means any freely given, specific, informed, and unambiguous indication of the wishes of the Data Principal, by which the Data Principal, through a statement or a clear affirmative action, signifies agreement to the Processing of Personal Data relating to them.

3.7. "**Data**" means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or Processing by human beings or by Automated means and includes Personal Data.

3.8. "**Data Fiduciary**" means any person who alone or in conjunction with other persons determines the purpose and means of processing of Personal Data.

3.9. "**Data Principal**" means the individual to whom the Personal Data relates and where such individual is a Child, includes the parents or lawful guardian of such a Child, and where such individual is a person with disability, includes her lawful guardian, acting on her behalf.

3.10. "**Data Processor**" means any person who Processes Personal Data on behalf of MMF;

3.11. "**Grievance Officer**" is an officer at the level of _____ posted at the office of the MMF, having its registered address at 310, B Wing, Bldg No. 6, Aaraju CHS Ltd, G M Link Road, Natwar Parekh Compound, Govandi (West), Mumbai, Maharashtra, India, 400043, who would redress grievances of the people/entities relating

to Data protection/sharing and carry out periodic assessments of the Data governance, privacy, and security.

3.12. "**Password**" means a secret word or phrase or code or passphrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information.

3.13. "**Personal Data**" means any information relating to a Data Principal who can be identified, directly or indirectly, by reference to such data alone or in combination with other identifiers such as name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that Data Principal.

3.14. "**Pseudonymisation**" means the process by which identifying fields within a data record are replaced by artificial identifiers, but re-identification is possible with additional information held separately.

3.15. "**Personal Data Breach**" means any unauthorized Processing of Personal Data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to Personal Data, that compromises the confidentiality, integrity or availability of Personal Data.

3.16. "**Process**" in relation to Personal Data, means any operation or set of operations performed on Personal Data, whether or not by Automated means, including but not limited to the collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

4. COLLECTION OF DATA:

4.1. The Personal Data that MMF may collect, store, and use includes but is not limited to:

4.1.1. Name;

4.1.2. Bank account details;

4.1.3. Contact information (including residential address, residential number, mobile phone number, and email address);

4.1.4. Citizenship and country of residence;

4.1.5. CVs, qualifications and areas of subject matter expertise;

4.1.6. Date of birth (age);

4.1.7. Dietary requirements;

4.1.8. Driver's licence, driving record, vehicle licence plate, parking tickets, traffic fines, GPS location, and route(s) travelled;

4.1.9. Gender;

4.1.10. Government-issued identification numbers;

4.1.11. Hobbies and interests;

4.1.12. Immigration status and information, such as passport and other identity documentation, citizenship, residency and other visas, details regarding family composition (names, genders, ages, including re spouse, dependents, and parents) and criminal convictions;

4.1.13. Languages spoken;

4.1.14. Localisation data;

4.1.15. Marital status;

4.1.16. Medical history;

4.1.17. Moving image and voice from video (both CCTV and creative videos);

4.1.18. Payment details;

4.1.19. Photographs;

4.1.20. Signatures;

4.1.21. Sexual orientation;

4.1.22. Personal Data contained or revealed through the use or maintenance of communications methods (for example, through voicemails, conference calls, telephone, video or telepresence, e-mails, correspondence, documents, and other work product and communications);

4.1.23. Next of kin.

4.2. Personal Data may be collected in various ways including the following:

4.2.1. From the employees;

4.2.2. From the public domain;

4.2.3. From other parties, such as:

4.2.3.1. Data providers;

4.2.3.2. Former employees; and

4.2.3.3. Miscellaneous third parties such as background checking agencies, due diligence service providers, police departments, MMF-approved and third party travel management systems.

4.3. MMF shall collect only such Personal Data as is necessary for clear, specific, and lawful purpose(s) that is / are legitimately connected to MMF's business operations.

4.4. A pre-collection checklist shall be maintained to assess the necessity and proportionality of each data element under Clause 3.1. The checklist may include, inter alia:

4.4.1. What is the purpose of collecting this Data?

4.4.2. Is this Data essential to achieve the stated purpose? If not, it shall not be collected (e.g., if age is sufficient, avoid collecting date of birth).

4.4.3. Is there a lawful basis for collecting this Data?

4.4.4. Can the purpose be achieved using anonymized or pseudonymized Data instead?

4.4.5. Is the extent of Data collection proportionate to the intended purpose?

Where anonymized or pseudonymized Data can achieve the same objective, preference shall be given to those alternatives.

4.5. MMF shall not collect Personal Data that is not essential or directly related to the declared purposes of Processing.

4.6. Justifications for collection of Personal Data shall be carefully documented and reviewed every 3 (three) months by designated compliance officers within MMF.

4.7. Every request made to a Data Principal for consent shall be accompanied or preceded by a notice given by MMF to the Data Principal. This notice shall include:

4.7.1. A simple, itemised explanation of the Data being collected;

4.7.2. The specific purpose for which the Data is being collected and is proposed to be Processed;

4.7.3. Information on how the Data Principal can exercise their rights, including withdrawing their consent;

4.7.4. The grievance redressal mechanism in case of a data leakage.

The notice shall be made available in English or in any other language specified in the Eighth Schedule to the Constitution of India, based on the preference of the Data Principal.

4.8. MMF shall obtain valid consent from the Data Principal prior to the collection and Processing of Personal Data. The consent should be traceable at all stages including collection, validation, updating, renewal and withdrawal.

4.9. The consent given by the Data Principal shall be free, specific, informed, unconditional, and unambiguous with a clear affirmative action, and shall signify an agreement to the Processing of her Personal Data for the specified purpose and be limited to such Personal Data as is necessary for such specified purpose.

4.10. All consent forms must include a clear age declaration, such as: "*I confirm that I am 18 years of age or older and hereby consent to the collection and use of my data in accordance with MMF's Data Security and Governance Policy, solely for the purposes of [research/program delivery/monitoring and evaluation] as explained to me.*" Digital forms may use checkboxes with a similar declaration that must be ticked before the form can be submitted.

4.11. Every request for consent shall be presented to the Data Principal in clear and plain language, giving her the option to access such request in English or any language specified in the Eighth Schedule to the Constitution and providing the contact details of a Data Protection Officer, if applicable, or the Grievance Officer, or of any other person

Unit No. 10/11, Building No. 34/A,
GM Link Road, Natwar Parekh
Compound, Govandi (W), Mumbai,
Maharashtra, India – 400 043

+91 720 888 0031
+91 932 612 7527

contact@mynafoundation.com

authorised by MMF to respond to any communication from the Data Principal for the purpose of exercise of her rights under applicable laws. The contact details are as follows:

_____

_____

4.12. All consent obtained shall be recorded with date and timestamp.

4.13. Where consent given by the Data Principal is the basis of Processing of Personal Data, such Data Principal shall have the right to withdraw her consent at any time, with the ease of doing so being comparable to the ease with which such consent was given. The consequences of the withdrawal shall be borne by the Data Principal, and such withdrawal shall not affect the legality of Processing of the Personal Data based on consent before its withdrawal.

4.14. If a Data Principal withdraws her consent to the Processing of Personal Data, MMF shall, within a reasonable time, cease and cause its Data Processors to cease Processing the Personal Data of such Data Principal unless such Processing without her consent is required or authorised under applicable laws.

5. CHILDREN'S DATA:

MMF does not knowingly collect or Process Data relating to children. To ensure compliance, the following mechanisms are in place:

5.1. All digital and physical data collection formats (including but not limited to mobile applications, registration portals, paper forms, surveys, and chatbots) must include a compulsory age or date-of-birth field.

5.2. Offline data collection (e.g., community outreach, mobile clinics) must begin with an age confirmation step. Digital platforms will implement automated age verification mechanisms to restrict submission by individuals below the age of 18.

5.3. Field personnel will request proof of age such as Aadhaar, school ID, or verbal confirmation from a parent/guardian, and will not proceed if the individual is underage.

5.4. All individuals involved in data collection and processing – including field officers, community mobilizers, researchers, interns, and data entry staff – must be trained on:

5.4.1. How to verify age reliably in both in-person and remote settings.

5.4.2. The importance of excluding minors from data pipelines.

5.4.3. What to do if they accidentally collect a minor's data.

5.5. If a minor's Personal Data is inadvertently collected:

5.5.1. It must be permanently and securely deleted from all storage systems (servers, physical files, backups) within 15 days of discovery.

5.5.2. A record of the deletion must be maintained (without retaining the Data itself) stating:

5.5.2.1. the nature of the Data deleted.

5.5.2.2. date of detection and deletion.

5.5.2.3. how the Data was received.

5.5.2.4. actions taken to prevent recurrence.

This protocol should be built into MMF's incident response workflow, and all staff should be aware of the reporting channel (Grievance Officer's email).

5.5.3. All internal systems must automatically restrict access to such Personal Data by:

5.5.3.1. implementing role-based access control so only designated compliance officers within MMF can view flagged entries.

5.5.3.2. isolating Personal Data flagged as potentially underage from programmatic, research, or analytical use until verified and deleted.

5.6. The Grievance Officer / Data Protection Officer (as applicable) of MMF shall ensure that audits are conducted every 3 (three) months to review:

5.6.1. a random sample of collected Personal Data for age-related red flags;

5.6.2. whether all tools in use have functioning age-gating mechanisms;

5.6.3. staff adherence to SOPs during data collection;

5.6.4. any past incidents of underage Personal Data collection and how they were resolved.

Audit reports must include action items and timelines for remediation where lapses are found.

5.7. MMF is committed to safeguarding the privacy of children. These mechanisms will be reviewed every 6 (six) months and updated to align with evolving laws, technological standards, and sectoral best practices.

6. PURPOSE LIMITATION:

6.1. The use of Personal Data shall be strictly limited to the specific purposes for which it was originally collected. Any new or repurposed use of Personal Data shall be preceded by a legitimate interest assessment and documented justification.

6.2. MMF shall not collect Personal Data for secondary purposes, unless fresh, free, informed, specific, and unambiguous consent is re-obtained from the Data Principal. This consent request shall clearly state the new purpose of Processing, identify any new entities or Data Processors with whom the Personal Data will be shared (if applicable), and provide a clear and accessible method for the Data Principal to grant or refuse consent, as well as to withdraw consent at any time. All such consents shall be logged with a timestamp and maintained as part of the Data Processing record.

6.3. In cases where Personal Data is collected on a continuous or daily basis – such as biometric and location data via the human resource management system – appropriate consent mechanisms and privacy notices shall be provided to individuals at the time of collection.

7. TRANSPARENCY:

7.1. MMF, or any person acting on its behalf who collects, receives, possesses, stores, deals with, or handles Personal Data, shall provide a privacy policy for the handling of such Data, ensure that it is made available to the Data Principals concerned, and publish it on MMF's website, applications, and at all physical data collection points, where applicable. Such policy shall provide for:

7.1.1. Clear and easily accessible statements of its practices and policies;

7.1.2. Type of Personal Data collected;

7.1.3. Purpose of collection and usage of such Personal Data;

7.1.4. Disclosure of Personal Data as provided under applicable laws;

7.1.5. Reasonable security practices and procedures as provided under applicable laws.

7.2. The privacy policy shall be available in English and in at least one of the languages listed in the Eighth Schedule of the Constitution of India, based on the primary region of operation or collection.

8. RIGHTS OF DATA PRINCIPALS:

8.1. Data Principals shall have the right to obtain from MMF, where they have given consent for the Processing of Personal Data, or for certain specified purposes for which the Data Principal has voluntarily provided such Personal Data, upon making a request in the manner prescribed:

8.1.1. a summary of Personal Data which is being Processed and the Processing activities undertaken by MMF with respect to such Personal Data;

8.1.2. the identities of all other Data Fiduciaries and Data Processors with whom the Personal Data has been shared, along with a description of the Personal Data so shared; and

8.1.3. any other information related to the Personal Data of such Data Principal and its Processing, as may be prescribed.

The requirements (7.1.2) and (7.1.3) do not apply to any sharing of Personal Data by MMF with another Data Fiduciary who is authorized by law to obtain such Personal Data where such sharing is pursuant to a request made in writing for the purpose of prevention or detection or investigation of offences or cyber incidents, or for prosecution or punishment of offences.

8.2. Data Principals shall have the right to correction, completion, updating and erasure of their Personal Data for the Processing of which they have given consent, or for certain specified purposes for which the Data Principals have voluntarily provided such Personal Data, in accordance with any requirement or procedure under any law for the time being in force.

8.2.1. Upon receiving a request for correction, completion or updating from a Data Principal, MMF shall:

8.2.1.1. correct the inaccurate or misleading Personal Data;

8.2.1.2. complete the incomplete Personal Data; and/or

8.2.1.3. update the Personal Data.

8.2.2. Upon receipt of a request for erasure of Personal Data, MMF shall erase the Data Principal's Personal Data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.

7.4. Where applicable, Data Principals shall have the right to request de-identification, anonymisation, or erasure of Data used for research purposes after such purpose has been fulfilled.

7.5. Data Principals shall have the right to have readily available means of grievance redressal provided by MMF. MMF shall respond to any grievances referred within 24 (twenty-four) hours from the date of its receipt.

7.6. Data Principals shall have the right to nominate, in such manner as may be prescribed, any other individual, who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data Principal, in accordance with applicable laws.

8. ACCESS CONTROLS:

8.4. Access to Personal Data shall be granted strictly on a "need to know" basis. MMF shall define user roles and assign access permissions based on job responsibilities.

8.5. MMF shall review all access rights on a regular basis, but in any event at least once a year, and positively confirm all system users. Any lapsed or unwanted logons which are identified shall be disabled immediately and deleted unless positively reconfirmed.

9. DATA PROCESSORS AND THIRD PARTIES:

9.4. MMF shall share Personal Data with third parties only where a written contract is in place between MMF and the third party, and subject to the following conditions:

9.4.1. The third party has a need to know the Personal Data.

9.4.2. Sharing the Personal Data complies with the notice that has been provided to the Data Principal (and, where applicable, the Data Principal's consent has been obtained).

9.4.3. The third party has agreed to comply with the Policy and has put adequate measures in place in ensure the security of the Personal Data.

9.4.4. The third party only acts on MMF's documented written instructions.

9.4.5. The third party will assist MMF in allowing Data Principals to exercise their rights in relation to data protection and in meeting MMF's obligations in relation to the security of Processing, the notification of Personal Data Breach and audits, as required under applicable laws.

9.4.6. The third party will delete or return all Personal Data to MMF upon request or upon termination of the engagement, whichever is earlier.

9.4.7. The third party will submit to audits.

9.4.8. The third party shall comply with applicable laws.

9.4.9. The third party receiving the Personal Data from MMF or any person on its behalf shall not disclose it further.

9.5. MMF shall maintain a live register of all third parties acting on its behalf.

9.6. A record of Data Processing activities, including purpose, categories of Personal Data collected, and third-party disclosures, shall be maintained and reviewed by MMF once in every 3 (three) months.

9.7. Disclosure of Personal Data by MMF to any third party shall require prior permission from the Data Principal, unless such disclosure is necessary for compliance of a legal obligation, provided that the Personal Data shall be shared, without obtaining prior consent from the Data Principal, with Government agencies mandated under the law to obtain the Personal Data for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency shall send a request in writing to MMF possessing the Personal Data stating clearly the purpose of seeking such Data, and also state that the Data so obtained shall not be published or shared with any other person.

9.8. MMF or any person on its behalf shall not publish the Personal Data.

9.9. MMF, or any person acting on its behalf, may transfer Personal Data to any body corporate or a person in India, or outside India (that ensures the same level of data protection that is adhered to by MMF),

provided that such transfer is not restricted by the Government of India, either by (i) notification of the recipient country as a restricted jurisdiction, or (ii) prohibition or restriction on the transfer of specific categories of Personal Data. All such transfers shall be subject to applicable laws, including any additional compliances prescribed by the Government of India.

10. REASONABLE SECURITY SAFEGUARDS:

10.4. MMF has implemented such security practices and standards that include managerial, technical, operational and physical security control measures that are commensurate with the Data being protected with the nature of business.

10.5. All Data shall be encrypted both when stored (at rest) and when being transmitted (in transit). Encryption methods must conform to recognized security standards and be appropriate to the level of risk associated with the Data.

10.6. All business agreements entered into by MMF, including but not limited to Non-Disclosure Agreements, Memoranda of Understanding, and service agreements, shall, at a minimum, incorporate the following:

10.6.1. Clearly define the categories of Personal Data being shared, the duration for which such Personal Data will be processed, the extent of Processing permitted, the basis of consent, and the rights of the Data Principal.

10.6.2. Identify which party determines the purposes and means of Processing and which party Processes Data on behalf of MMF.

10.6.3. Include express provisions regarding the engagement of sub-processors, ensuring they are contractually bound to the same Data protection obligations as the primary Data Processor.

10.6.4. Outline technical and organizational security measures to protect Personal Data.

10.6.5. Specify protocols for identifying, managing, and responding to Personal Data Breach.

10.6.6. Affirm that rights of the Data Principal are upheld.

10.6.7. Grant MMF the right to audit and inspect the Data Processor or Service Provider's facilities, policies, and procedures.

10.6.8. Require the Data Processor or Service Provider to maintain detailed records of all Personal Data Processing activities and make them available to MMF or competent authorities upon request.

10.6.9. Include indemnification clauses to compensate for any damages or losses arising from such breach or non-compliance.

10.7. MMF shall deploy and maintain intrusion detection and/or prevention systems to monitor for unauthorized access attempts and unusual network activity.

10.8. MMF shall maintain a documented security incident response plan that sets out procedures to detect, report, investigate, and

Unit No. 10/11, Building No. 34/A,
GM Link Road, Natwar Parekh
Compound, Govandi (W), Mumbai,
Maharashtra, India – 400 043

+91 932 612 7527

contact@mynafoundation.com

resolve actual or suspected security incidents and includes defined roles, escalation steps, timelines, and mechanisms for internal and external reporting.

10.9. MMF shall conduct periodic vulnerability assessments of all systems used to store or Process Personal Data or Sensitive Personal Data, including mobile applications, the human resource management system, and platforms used for research and chatbot development to identify and address vulnerabilities, including at third-party-operated systems where applicable, to identify and remediate security flaws.

10.10. All systems used by MMF or its third-party service providers shall follow structured procedures for applying software updates and security patches, particularly where vulnerabilities are identified that may affect confidentiality, integrity, or availability of Data.

10.11. MMF shall implement authentication mechanisms commensurate with the sensitivity of Data accessed, including but not limited to the use of multi-factor authentication, strong password policies, and session timeouts.

10.12. Access to Personal Data shall be restricted through Role-Based Access Control to ensure that only authorized personnel with a legitimate business need can access such information.

10.13. Upon the exit of an employee, MMF shall promptly revoke all access privileges, including email, computer systems, remote access, and any other internal platforms. Appropriate internal protocols shall be followed to determine who, if anyone, may access the former employee's files. MMF shall also ensure that

any equipment issued to the employee, such as laptops, USB drives, or other devices, is returned before their final departure from the premises.

11. DATA RETENTION AND DELETION:

11.4. MMF shall retain Data only for as long as necessary to fulfil the purpose of collection or as required under applicable laws. A Data Retention Schedule, mapping each Data category to its legal or operational retention period, shall be maintained and published internally.

11.5. MMF shall, unless retention is necessary for compliance with any law for the time being in force, erase Personal Data, upon the Data Principal withdrawing her consent or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier; and cause its Data Processor to erase any Personal Data that was made available by MMF for processing to such Data Processor. MMF shall obtain written confirmation from the said Data Processor that all Data has been securely and permanently deleted from the Data Processor's systems.

11.6. MMF shall notify Data Principals at least 48 (forty-eight) hours prior to erasure that their Personal Data will be erased.

11.7. Upon the Data Principal withdrawing consent, or the fulfilment of the purpose, or expiration of the retention period, whichever is earlier, Personal Data shall be securely deleted or anonymized in a timely manner.

12. PERSONAL DATA BREACHES:

12.4. Upon becoming aware of a Personal Data Breach, MMF shall within 72 hours notify the affected Data Principals using any registered mode of communication with MMF, including a description of the Personal

Data Breach, potential consequences for the Data Principal, and safety measures that the Data Principal shall adopt.

12.5. MMF shall designate a Point of Contact to liaise with CERT-In on all matters relating to cyber incident reporting and response, and shall ensure that system logs are securely stored on an ongoing basis for a minimum period of 180 (one-eighty) days.

12.6. MMF shall mandatorily report the following cyber security incidents to CERT-In within 6 (six) hours of becoming aware of such incidents:

12.6.1. Compromise of critical systems or information;

12.6.2. Targeted scanning or probing of critical networks or systems;

12.6.3. Identity thefts, spoofing or phishing attacks;

12.6.4. Unauthorised access of IT systems or data;

12.6.5. Defacement of a website or intrusion into a website;

12.6.6. Malicious code attacks, including ransomware;

12.6.7. Denial of Service or Distributed Denial of Service attacks;

12.6.8. Data breach or Data leak;

12.6.9. Attacks through malicious mobile applications;

12.6.10. Attacks on servers, databases, or APIs;

12.6.11. Unauthorised access to social media accounts.

12.7. Mandatory 6-hour reporting shall apply if incidents fall into any of the following categories:

12.7.1. Cyber incidents of severe nature such as DoS, DDoS, intrusion, ransomware;

12.7.2. Data breaches or data leaks, including of Personal or Sensitive Data;

12.7.3. Large-scale or frequent incidents impacting IT resources or websites;

12.7.4. Cyber incidents impacting the safety or security of human beings.

12.8. MMF, when dealing with electronic records, shall ensure the security of such records by implementing appropriate safeguards, including but not limited to, (i) protection against unauthorized access; (ii)

Unit No. 10/11, Building No. 34/A, GM Link Road, Natwar Parekh Compound, Govandi (W), Mumbai, Maharashtra, India – 400 043
+91 720 888 0031
+91 932 612 7527
contact@mynafoundation.com

protection against alteration or tampering; (iii) maintaining the security of computer systems, software, and hardware; (iv) protecting electronic signatures; and (v) taking periodic backups.

12.9. MMF shall maintain a documented Security Incident Response Plan to promptly detect, assess, contain, and respond to security incidents, which shall include escalation protocols, defined roles and responsibilities, and timelines for mitigation.

12.10. In the event of a compromise involving Personal Data, MMF shall engage qualified cybersecurity professionals to assist with containment, forensic investigation, risk assessment, and implementation of remedial actions.

12.11. The Grievance Officer or the Data Protection Officer (if applicable) shall be responsible for complying with the obligations laid down in this Clause.

13. TRAINING AND AWARENESS:

13.4. All staff, including employees, volunteers, consultants, and community-based workers, shall undergo periodic training on, *inter alia*, secure handling of Personal Data, the identification of phishing and cyber threats, and MMF's internal procedures. All new staff must undergo Data security training within 15 days of joining.

13.5. All individuals volunteering or interning with MMF shall be provided with a mandatory orientation session before they commence any task that involves handling Personal Data. This orientation shall include an overview of MMF's approach to Data privacy and confidentiality, the ethical principles that apply to community- and research-related Data, and clear guidance on how Data may and may not be used or shared. The orientation shall also explain the importance of safeguarding photographs, videos, beneficiary data, and any other identifiable information they may encounter.

13.6. The training content shall be adapted to MMF's specific operational context, using practical examples drawn from its work in mobile clinics, research, digital tools, and community outreach.

13.7. Attendance and participation in such training sessions shall be documented, and assessments may be administered to ensure comprehension and retention of key information.

13.8. The Human Resources team, in consultation with the Grievance Officer, or any other person authorised by MMF in this behalf shall be responsible for developing, delivering, and tracking these training sessions.

13.9. Data access granted to individuals within MMF shall be limited strictly to what is necessary for their assigned roles.

13.10. Personnel involved in software development or system administration shall receive periodic training on secure coding practices, vulnerability mitigation, and secure system configuration.

14. AUDITS AND REVIEW

14.4. MMF shall undertake a periodic audit of its data protection practices, and such other measures, consistent with applicable laws.

14.5. The Policy shall be reviewed at least annually, or earlier if required due to changes in applicable law, technology, or business processes. All updates shall be communicated to relevant stakeholders and re-published wherever the Policy is made accessible.

15. GRIEVANCE REDRESSAL:

15.4. MMF shall establish an effective mechanism to redress the grievances of Data Principals.

15.5. MMF shall appoint a Data Protection Officer, if applicable, or a Grievance Officer, who shall:

15.5.1. represent MMF under applicable laws;

15.5.2. be based in India;

15.5.3. be responsible to MMF's Board of Directors; and

15.5.4. be the point of contact for the grievance redressal mechanism.

15.6. MMF shall include, in all its notices, consent forms, applications, chatbots, and websites, the business contact information of the Data Protection Officer, if applicable, or the Grievance Officer, who shall answer, on its behalf, questions, if any, raised by the Data Principals about the Processing of their Personal Data.

15.7. Data Principals may contact the Data Protection Officer / Grievance Officer at:
[Insert Name]
[Insert Email ID / Phone Number]
[Insert Office Address]

15.8. Complaints shall be acknowledged within 24 (twenty-four) hours and resolved within 7 (seven) days from the date of receipt of the complaint.

15.9. Any employee found to be non-compliant with the Policy may be subject to disciplinary actions, according to MMF's internal policies, including but not limited to warnings, access restrictions, termination, and legal action. MMF also acknowledges the penalties mandated under applicable laws in this respect.

16. ANNEXURES

16.1 KEY COMPLIANCE OBLIGATIONS

16.2 DRAFT MOU DATA PROTECTION

Approved by:

Unit No. 10/11, Building No. 34/A,
GM Link Road, Natwar Parekh
Compound, Govandi (W), Mumbai,
Maharashtra, India – 400 043

+91 720 888 0031
+91 932 612 7527

contact@mynafoundation.com