DATA PROTECTION POLICY

I. PURPOSE

M. S. Swaminathan Research Foundation ("MSSRF", the "Foundation") is committed to respect your privacy and to legally comply with all applicable data protection and privacy laws.

a. This Data Protection Policy ("**Policy**") shall apply to personal data collected, processed, transferred, and stored by the Foundation, either in digital format or in non-digital format where such data is subsequently digitised.
b. This Policy aims to safeguard all the Personal Data that is collected by the Foundation.
c. This Policy provides for certain principles to protect the collection, processing, transfer, and storage of data in accordance with the applicable laws and read with the **Standard Operating Procedure (SOP)**.

II. POLICY STRUCTURE

This Policy is divided into two parts:

a. **Part I** pertains to the programmes of the Foundation and the management of data related to programmes.

b. **Part II** applies to employees and associated persons, outlining their responsibilities and compliance requirements.

III. DEFINITIONS:

In this Policy, unless the context otherwise requires:

a. "**Applicable Law"** means all applicable data protection and privacy laws as amended from time to time, including:
    - The Digital Personal Data Protection Act, 2023
    - The Information Technology Act, 2000
    - Any other relevant Acts, or Rules or Directions promulgated by appropriate authorities
b. "**CERT-In**" means the Indian Computer Emergency Response Team as set up under the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013. CERT-In functions under the Ministry of Electronics and Information Technology and is the nodal agency for responding to computer security incidents as and when they occur. Any individual or entity affected by a Cyber Security Incident may report the same to CERT-In, and certain Cyber Security Incidents must mandatorily be reported.

CERT-In then addresses these incidents and provides support depending on the type and severity of incident, affected entity, available resources, etc.

c. "**Cyber Security Incident**" means any real or suspected adverse event in relation to cyber security that breaches anything contained in this Policy, and causes unauthorised access to the Foundation's resources, disruption of activities, misuse of computer resources resulting in data leak or unauthorised data access breaching confidentiality norms or unauthorised changes to data or information.

d. "**Data Principal**" means the individual whose Personal Data is collected or processed. If the individual is:
    - A person below the age of 18 years, verifiable consent to process, collect data and exercise all connected rights has to be obtained from the parents or court-appointed guardian of such persons;
    - A person with disability, consent to process, collect data and exercise all connected rights has to be obtained from lawful guardian;

e. "**Data Protection Officer"** refers to an employee of the Foundation who is given responsibility under Clause VIII (*Appointment of Data Protection Officer*) of this Policy.

f. **"Data Protection Board (DPB)"** is an independent body established to oversee and enforce data protection regulations, investigate breaches, adjudicate disputes, and impose penalties for violations of data protection laws, ensuring compliance and promoting accountability

g. "**Personal Data**" shall mean any data about an individual who is identifiable by or in relation to such data. Such Personal Data can be collected by the Foundation from the employees, consultants, contractual staff, job applicants, program participants, and other individuals during the operations of the Foundation. The following data, including but not limited to, will be considered as Personal Data of an individual:

- Name including Parents/Spouse names
- Gender/sexual orientation
- Photographs
- Home Address
- Phone numbers including emergency contact numbers
- Email IDs
- Employment and Academic details
- Identity Documents Details (Adhaar card number; PAN card number; Driving license number etc.)
- Resumes of prospective candidates
- Passwords
- Financial information such as bank account, credit card, debit card or other payment instrument details
- Physical, physiological, and mental health conditions
- Sexual orientation
- Medical records and history
- Biometric information.

Personal Data also includes information about funders, beneficiaries, and donors, including but not limited to:

- Name and contact details
- Financial contributions and transaction details
- Banking details
- Organizational affiliation (if applicable)
- Communication records and consent preferences
- Any other relevant personal information collected as part of MSSRF's engagement with these stakeholders

PART 1 – PROGRAMMES

IV. APPLICABILITY

This Data Protection Policy applies to all research, development, and programmatic activities undertaken by MSSRF across its core thematic areas and special projects. It governs the collection, processing, storage, and sharing of data within the following domains but not limited to :

A. Coastal and Marine System
B. Biodiversity Management
C. Nutrition and Health
D. Agri Food System
E. Climate Resilience
F. Gender and Institutions Building
G. Technology
    a. Biotechnology
    b. Ecotechnology
    c. Geographic Information System
    d. Artificial Intelligence

V. PERSONAL DATA PROTECTION PRINCIPLES

The collection and processing of Personal Data shall be done in accordance with the following principles:

a. **Anonymity**: Personal data collected for research, development, and programmatic activities shall be anonymized before processing whenever feasible. Any identifiers that could link the data to specific individuals shall be removed unless necessary for the purpose of the program.
b. **Purpose Limitation**: Personal data shall only be used for the specific objectives of Foundation's thematic programs and research activities or for audit purposes. It shall

not be processed for any other purpose without explicit consent or legal authorization of the Data Principal.

c. **Data Minimization**: Only the necessary data relevant to Foundation's research, interventions, and programmatic goals shall be collected and processed. The collection of irrelevant or excessive data shall be avoided. Any data not relevant to the Foundation's research, financial statements, interventions and programmatic goals, if inadvertently collected, shall be deleted.
d. **Data Security**: Adequate technical and organizational measures shall be implemented to ensure the security and confidentiality of all Personal Data collected under Foundation's programs.
e. "**Implementation Partner**" refers to any entity, organization, or service provider engaged by the Foundation to execute specific projects, initiatives, or activities in alignment with the Foundation's objectives.
f. **Notice and Transparency**: Individuals, including legal guardians of minors, shall be provided with clear and concise notices regarding the collection, processing, and use of Personal Data across Foundation's programs. Notices shall be easily accessible and comprehensible, outlining the scope, purpose, and handling of data.
g. **Consent**: Where applicable, explicit and informed consent shall be obtained before collecting and processing Personal Data, particularly for minors and vulnerable communities. Consent shall be voluntary, specific, and unambiguous, with individuals having the right to withdraw consent at any time.
h. **Data Retention**: The Foundation shall retain collected data only for as long as it serves the intended research or programmatic purpose or for audit purposes. Once the purpose is fulfilled, data shall be securely deleted unless retention is required for legal, ethical, or research integrity reasons.
i. **Erasure and Modification**: Data Principals or their representatives may request MSSRF to review, correct or delete their personal information. The Foundation shall comply with such requests within a reasonable timeframe unless specific data must be retained for legal or research purposes.

This policy ensures that all data collected across MSSRF's thematic programs is handled responsibly, ethically, and in compliance with applicable data protection standards.

VI. PROCESS FOR DATA COLLECTION

Personal Data will only be collected and processed by the Foundation as per the process outlined here, which strives to ensure that the informed consent of the Data Principal is obtained after providing them with all the requisite information. The process for obtaining consent and the detailed requirements for the notice have been outlined in the **SOP**.

a. **Notice to Data Principals**: The notice shall be presented in a manner that is clear, understandable, and independent of any other information that MSSRF has provided, or may provide. The notice shall use plain and unambiguous language to enable the Data Principal to give specific and informed consent. It shall, at a minimum, include:

i. Clear list of the types of Personal Data being collected and used.
ii. The reason for collecting the data, along with a simple breakdown of the goods, services, or features that will be provided using this data.

b. **Exemptions:** Under certain limited or exceptional circumstances, the Foundation may, as permitted or required by Applicable Laws, process Personal Data without providing notice or seeking consent. These circumstances may include:
   i. Investigation of specific allegations of criminal activity.
   ii. To comply with any valid judgement or decree or order issued by a competent court.
   iii. To take measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health.
   iv. To take measures to ensure safety of, or provide assistance or services to, any individual during any disaster, or any breakdown of public order.
   v. To safeguard the Foundation from loss or liability, such as maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee.
   vi. Anonymized data may be shared with external partners, researchers, or stakeholders for the purpose of collaboration and evaluation. Such sharing shall be carried out in accordance with data protection regulations and contractual agreements. Data sharing shall be restricted to aggregated and anonymized formats to prevent re-identification.

VII. TRANSFER OF DATA

a. If Personal Data needs to be shared with a third party for program-related activities—such as research collaborations, training programs, field interventions, community outreach, impact assessments, healthcare initiatives, or financial assistance—only the minimum necessary information required to provide the service shall be shared.

b. The Foundation shall ensure that any third party receiving data has implemented adequate safeguards to protect the shared information. Before engaging in data sharing, a Data Sharing Agreement (DSA) shall be established to define the obligations, responsibilities, and security measures required as outlined in the **SOP** to ensure transparency, accountability, and adherence to data protection principles..

c. Cross-border transfers of Personal Data shall be conducted only in compliance with relevant national and international data protection regulations. MSSRF shall obtain the necessary approvals and implement appropriate legal, technical, and contractual safeguards before such transfers.

VIII. APPOINTMENT AND DUTIES OF DATA PROTECTION OFFICER

a. The Foundation shall appoint a Data Protection Officer, whose official contact information shall be published on the Foundation's website.
b. Data Principals, whose data has been collected by the Foundation, can approach the Data Protection Officer with regard to any complaints, queries, or concerns they may have with regard to their data.
c. The Data Protection Officer shall receive and respond to any complaints,queries or grievances of Data Principals, and facilitate the exercise of Data Principals' rights in relation to their Personal Data and how it is processed after confirming their identity.
d. In case the Data Protection Officer cannot fulfil a request of any Data Principal, a reasonable justification shall be provided for the same.
e. The Data Protection Officer shall take appropriate measures to process requests from Data Principals within a reasonable time and provide them with information in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

IX. REASONABLE SAFEGUARDS TAKEN BY THE FOUNDATION

The Foundation is committed to protecting Personal Data in its possession or under its control, including data handled by any third party on its behalf. To prevent data breaches, the Foundation ensures the following security measures:

a. **Securing Personal Data:** Personal Data is protected through encryption, obfuscation, masking, or the use of virtual tokens.

b. **Access Control:** Measures are in place to regulate access to computer systems handling Personal Data, ensuring only authorized personnel can access it.

c. **Monitoring and Detection:** Logs and monitoring systems track data access to detect, investigate, and prevent unauthorized access.

d. **Backup and Recovery:** In case of data loss, the Foundation ensures continued data processing through backups and recovery mechanisms.

e. **Retention for Security Purposes:** To aid in detecting and investigating security incidents, logs and relevant data are retained for at least one year unless the law requires a different retention period.

f. **Security in Third-Party Agreements:** Any external party handling the Foundation's data is contractually required to follow strict security safeguards.

g. **Technical and Organizational Measures:** The Foundation implements necessary security protocols and best practices to maintain the confidentiality, integrity, and availability of Personal Data.

h. **Notification of Data Breaches:** If a Personal Data breach occurs, the Foundation will promptly inform the Data Protection Board affected individuals in a clear and timely manner through their registered communication channels. The process for breach notification, response, and mitigation is outlined in the **SOP** to ensure a structured and effective approach to handling such incidents. The notification will include:

i. Details of the breach, including its nature, extent, timing, and location.
ii. Possible consequences for the affected individual.
iii. Measures taken by the Foundation to reduce risks.
iv. Recommended steps the individual can take to protect themselves.
v. Contact information of a representative available to address any concerns

i. **Procedure for Cybersecurity Incidents** In the event of a Cybersecurity Incident**,** the DPO shall promptly notify all Data Principals whose Personal Data has been compromised. The process, including the **timeline, method** of communication, and remedial measures, shall be carried out in accordance with the **SOP** to mitigate risks and safeguard affected individuals.

j. **Consent for Processing of Personal data of Children and individuals with disabilities :** Before processing the Personal Data of a child or a person with a disability, the Foundation ensures that verifiable consent is obtained from their parent or lawful guardian. The Foundation also verifies that the consenting individual is an adult using reliable identity and age details or authorized verification methods, such as Digital Locker services. The **SOP** shall set out the **step-by-step process** for the following:

i. Obtaining and verifying parental/guardian consent before data processing.

ii. Documenting and storing consent records securely.

iii. Validating identity and age details using government-approved verification methods.

iv. Handling consent withdrawal requests from parents or guardians.

k. **Annual Data Protection Assessment and Audit**: The Foundation shall conduct a Data Protection Impact Assessment and an audit every twelve months to ensure compliance with applicable data protection laws and regulations. This process is detailed in a separate process document which will help evaluate risks, assess data security measures, and confirm adherence to the provisions of this policy.

l. **Reporting and Compliance Oversight**: The Foundation shall ensure that an independent assessment team prepares a comprehensive report highlighting significant findings from the Data Protection Impact Assessment and audit. This

report shall be submitted to the relevant oversight body for review and necessary action

m. **Algorithmic and Data Processing Due Diligence**:
The Foundation shall implement strict due diligence measures to ensure that any algorithmic software used for storing, processing, sharing, or managing Personal Data does not pose a risk to individuals' rights. This includes ensuring transparency, fairness, and accountability in data processing practices.

n. **Data Localization and Transfer Restrictions**: The Foundation shall comply with data localization requirements as per government regulations.

X. RIGHTS OF DATA PRINCIPAL

The Data Principal shall continue to have the following rights with respect to the data they have provided:

a. **Right to withdraw consent***:* The Data Principal has the right to withdraw the consent she had given earlier for the collection and processing of her Personal Data. The withdrawal of consent, however, would not affect the legality of the processing of Personal Data before the withdrawal.

b. **Right to access information about Personal Data**: The Data Principal has the right to request and obtain from the Foundation:
   i. a summary of Personal Data being processed and the processing activities involved.
   ii. the identities of any third parties with whom the Personal Data has been shared, and a description of the shared data; and
   iii. any other information about the Personal Data and its processing, as prescribed under any Applicable Law.

   However, points (ii) and (iii) above shall not apply when the Foundation shares Personal Data with third parties authorized by law to obtain such data, for purposes such as for crime prevention, investigation, or prosecution of offences or cyber incidents, based on a written request in accordance with law.

c. **Right to correction and erasure of Personal Data**:
   i. The Data Principal has the right to correct, complete, update or erase her Personal Data, which she had previously consensually given, in line with Applicable Laws.
   ii. The Foundation shall, upon receiving a request for correction, completion or updating from a Data Principal, —
      1. correct the inaccurate or misleading Personal Data;
      2. complete the incomplete Personal Data; and
      3. update the Personal Data.

iii. If a Data Principal requests the erasure of her Personal Data, the Foundation shall comply unless the retention of that data is necessary for a specified purpose or to comply with any Applicable Law.

d. **Right to Nominate***:* A Data Principal shall have the right to nominate another person who, in the event of the Data Principal's death or incapacity, can exercise the Data Principal's rights under Applicable Laws.

XI. DATA PROTECTION CHANGES IN POLICY

The Foundation will conduct periodic reviews of this Policy and may change, modify, add, or remove portions of this Policy.

PART II – EMPLOYEES

I. APPLICABILITY

This Policy shall apply to all:

a. Full-time and part-time employees of the Foundation; and
b. Persons associated with the Foundation but not directly employed by the Foundation, including consultants (full-time and part-time), contractual staff (whether on the payroll of the Foundation or a third-party agency), interns/apprentices (with or without stipend or remuneration), trainees, and persons on probation.

All individuals covered under this Policy must understand and adhere to its provisions. Any contravention of this Policy will result in formal disciplinary action, which may include termination of employment or association with the Foundation

II. PRINCIPLES

a. **Purpose Limitation:** Data collected from employees shall only be used for employment-related purposes and shall not be processed for any other purpose without further consent.

b. **Interventions:** Only necessary data relevant to employment shall be collected and processed, avoiding irrelevant or extraneous data.

c. **Data Security:** Adequate technical and organizational measures shall be implement

d. ed to ensure data security and confidentiality.

e. **Consent:** Written consent shall be obtained from employees for the collection and processing of sensitive data such as financial information, wherever applicable.

f. **Data Retention:** The Foundation shall cease to retain collected data once the purpose for retention no longer applies.

Type of Data	Retention Period
Financial Data	6 years
Employee Data	3 years

g. **Erasure and Modification:** Employees may request MSSRF to edit or delete their personal information, and such requests shall be processed within a reasonable time unless legal obligations require retention.

III. DATA PROCESSING

MSSRF shall ensure that all collected data is processed exclusively by authorized personnel for legitimate operational, administrative, and legal purposes. This includes but is not limited to:

a. Employee management and administration, including recruitment, performance evaluation, and contract management.
b. Payroll and reimbursement processing, ensuring accurate compensation and financial management.
c. Regulatory compliance and reporting, fulfilling obligations under labour laws, taxation, and other applicable regulations.
d. Security and access management, ensuring workplace safety, IT system integrity, and controlled access to sensitive data.
e. Training and professional development, using data for workforce skill enhancement and capacity-building programs

IV. DATA STORAGE

Personal data shall be stored securely with restricted access to authorized personnel only. Measures shall include:

a. Access strictly on a need-to-know basis

b. Storage in password-protected systems

c. Periodic cyber audits to ensure network security

d. Any individualized data shall be deleted once retention is no longer necessary for its outlined purpose.

V. TRANSFER OF DATA

a. If the data is going to be transferred to a third party for any purpose like employee pick up/drop facilities, background verification, medical/health checks, insurance

providers, training programs, etc., only as much information as is absolutely necessary to render the services should be shared.

b. MSSRF will ensure that when data is shared with any third party, such party has adequate safeguards to protect the shared data.

Cross-border transmission of Personal Data shall be carried out only after complying with the relevant national requirements for the transfer in each state.

VI. MONITORING AND COMPLIANCE

The DPO appointed in accordance with Clause VIII of Part 1 of this policy, shall be responsible for overseeing data protection measures and ensuring compliance with this policy and relevant data protection laws. Contractors must provide proof of data protection policies before engaging in projects. Regular assessments and audits shall be conducted to ensure compliance with this policy and relevant data protection laws.

VII. REPORTING AND INCIDENT RESPONSE

Any data security breaches or incidents shall be promptly reported to relevant authorities, with corrective measures taken. MSSRF shall also notify affected partner organizations of potential security risks.

VIII. GRIEVANCES AND CONTACT

The DPO serves as the main point of contact for employees and authorities regarding data privacy concerns, inquiries, grievances and requests. For submission of any grievances, questions, queries, or concerns, please contact the DPO at [contact@mssrf.res.in].