**Data Policy – Rights Based**

**Introduction**

As a rights-based organization, [organization’s name] is committed to using data responsibly in order to uphold the rights of the individuals, groups, and organizations with whom we work. Using data responsibly is not just an issue of technical security and encryption but also of safeguarding the rights of people to be counted and heard; ensure their dignity, respect and privacy; enable them to make informed decisions; and not be put at risk, when providing data.

[organization’s name] recognizes that people have rights with regards to the information related to them and that [organization’s name] has a responsibility to uphold those rights. The rights that form the backbone of this policy are:

A Right to be counted and heard

B Right to dignity and respect

C Right to make an informed decision

D Right to privacy

E Right to not be put at risk

This policy should not be seen as restricting or discouraging; rather, it sets out to facilitate the invaluable contribution that data makes to the quality of [organization’s name’s] work, upholding accountability and allowing [organization’s name] to raise the voices of those with whom we work.

For the purposes of this policy, “data” is considered to be the physical representation of information in a manner suitable for communication, interpretation, or processing by human beings or by automatic means. Data may be numerical, descriptive, audio, or visual1. The formal term for individuals from whom data is collected is “data subjects”. In this policy, however, we use the term “participants” and expand the definition to include any group, cooperative, or other entity with which [organization’s name’s] works that provide program data.

This document sets out the policy for the treatment of program data by [organization’s name] throughout the data lifecycle from planning to collection through to disposal. This data may pose varying degrees of risk to different stakeholders, including but not limited to the people who provide data, those that collect it, and [organization’s name]; therefore, this policy includes definitions and requirements for managing high-, medium-, and low-risk data.

This policy pertains to data from all of our programs (both project and program), funded by both restricted and unrestricted funds. It will apply to all aspects of the project and program cycle as well as research. [organization’s name] will uphold this policy for all projects where [organization’s name] is the data controller. [organization’s name] is responsible for ensuring that all external individuals or organizations it works with during the data lifecycle (partners, contractors, etc.) comply with the policy.

This policy is designed to be forward-looking and prepare [organization’s name] for the future, establishing systems to enable the organization to take full advantage of the current opportunities and future potential of the data revolution. Recognizing that the policy applies to a rapidly-changing technological context, [organization’s name] has a responsibility to stay abreast of the implications of these changes for its work. A set of minimum standards and guidelines accompanies this policy to provide details on how to operationalize the requirements and will be updated periodically.

**Policy Elements**

A. Right to be counted and heard

In order to ensure the rights of vulnerable and marginalized populations, including women, it is important that they are able to be counted and adequately represented as part of the information [organization’s name] collects and uses.

1. Where appropriate and possible, [organization’s name] will make every effort to ensure that vulnerable groups including women are fully represented in data collection, and that the resulting datasets can be disaggregated by gender and other relevant categories. [organization’s name] will make all reasonable effort to ensure the inclusion of participants from marginalized populations. [organization’s name] will ensure the accuracy of data collected, stored, and used, including making

efforts to keep information up-to-date and relevant. [organization’s name] will appropriately analyze, utilize, and disseminate the information it collects in

order to ensure participants’ right to be heard, especially within marginalized populations. This dissemination should include communicating findings to the surveyed population as part of [organization’s name]’s commitment to social accountability.

B. Right to dignity and respect

[organization’s name] will ensure that a participant’s personal dignity is maintained and respected in all phases of the data lifecycle.

Data will be collected in a manner that is culturally and contextually appropriate. It is necessary to be aware that there may be laws in addition to standards which

regulate how [organization’s name] works with participants. [organization’s name] will intentionally plan the data lifecycle in such a way as to not create an

excessive burden on participants, carefully considering what data are needed and why; how it will be used; and how to collect only the minimum data required to accomplish programmatic aims.

C. Right to make an informed decision

Participants have the right to be fully informed in order to make a decision about their participation in any data activity.

[organization’s name] and its agents will gain informed and voluntary consent4 before obtaining any information from participants. Data will only be used for the purpose it was collected for. All participants are free to choose whether or not to give their consent, without inducement or negative consequences should they choose not to participate. All participants and are free to withdraw their involvement in the data activity at any

stage without any negative consequences, including their participation in

[organization’s name] programs. If the data process involves minors, [ organization’s name] will get both their, and their parents’ or guardians’, consent, except in circumstances when it is inappropriate to do so. Consent will be based on a transparent and accurate assessment about the use of data and context. If the use or the context changes, [organization’s name] will re-evaluate whether re- consent is needed.

D. Right to privacy

[organization’s name] will ensure a participant’s right to privacy in the treatment of his/her data and has a responsibility to protect the identity of those providing data, unless otherwise outlined and agreed to in the informed consent.

[organization’s name] will ensure that, when appropriate, the process of data collection is conducted in an environment where the privacy of the participant (or group of participants in the case of focus group discussions) is upheld. [organization’s name] and its agents will not discuss or share in any form, information gathered from participants with any unauthorized (by [organization’s name]) persons.

[organization’s name] will minimize the collection of personal data, only collecting it when absolutely essential for the data activity. [ organization’s name] will ensure that where appropriate PII data is separated from other data collected and kept in a manner that allows the PII to be protected. [organization’s name] will ensure limited access to identified data records and store them securely. While [ organization’s name] encourages data sharing for transparency and accountability purposes, data which are shared openly must be anonymized, unless specific consent from the participant has been obtained, and it does not place participants at risk.

E. Right to not be put at risk

[organization’s name] will not put participants in any security risk as a result of its data activity. This principle is not pertinent when public officials or private sector actors who are acting in their official capacity. These individuals/ groups will be protected when acting as private citizens and not in their official capacity.

[organization’s name] and its agents will not collect non-essential data that could put participants at risk without justification and a clear process for managing and mitigating that risk. [ organization’s name] will take all reasonable measures to ensure that the process of data collection

and the totality of the data lifecycle have no negative physical, psychological, or political consequences for the participants. [ organization’s name] will store all high-risk data securely. [ organization’s name] will mitigate risk to all its participants, but especially participants from vulnerable

populations and groups or any participants engaged in sensitive topics/activities. Such topics must only be approached by personnel with the appropriate training and experience.

Additional Considerations

F. Gender

[organization’s name] will take particular care to use strategies that minimize or mitigate the impact of barriers to the participation of women, in order to ensure that their voices are heard and their opinions/experiences are accurately and fairly represented. Special attention must be paid to taking women’s particular needs into consideration during the entire data lifecycle.

G. Humanitarian Crises and Fragile States

Extra care will be taken with data collection in humanitarian conflict responses and fragile states. It is imperative that if data will compromise a person/s safety, those data should not be collected. In extreme cases where access is limited or denied, remote data collection may be considered. Measures must be taken to store data safely—see section D.

Enumerators or those conducting qualitative studies should likewise be protected. Enumerators must be trained on safety procedures and have access to support. Insurance policies should be in place to cover all eventualities. All conflict responses should be seen as high risk.

Governance and implementation of the Policy

The ultimate responsibility for this policy rests with the Board). Every 2 years, the Board shall commission a review of, and seek recommendations on, potential updates to the Responsible Program Data Policy. This effort ensures that the policy remains current and relevant, given the changing context in which [ organization’s name] operates. Following any updates to the policy, the set of minimum standards will also be reviewed and updated as required.

Policy implementation is the responsibility of [organization’s name] [appropriate staff] and their designates. Support for policy implementation will be provided by relevant personnel within each affiliate. Every two years, the Board shall commission a review of compliance with the policy, and seek recommendations on potential updates to the Responsible Program Data Policy.