POLICY DOCUMENTS FOR EMPLOYEE ENGAGEMENT

1. **CHILD PROTECTION POLICY**
2. **CONFLICT OF INTEREST POLICY**
3. **DATA SECURITY POLOICY**
4. **WHISTLEBLOWER POLICY**

CHILD PROTECTION POLICY

By Change Initiatives
Date: 15/09/2017

Change Initiatives (CI) is committed to ensuring all children are safe and protected. The safety, rights and wellbeing of children participating in CI's programmes are a priority in its daily operations. This Child Protection Policy intends to guide CI's employees, volunteers and associates, in developing appropriate relationship with the children involved in the activities or programmes performed by CI and thereby strives to create a safe environment for the children.

An employee/ volunteer or any associate must not:

1. Physically assault/ abuse children;
2. Embarrass any child;
3. Initiate any sort of physical contact with a child which may make the child or any observer feel uncomfortable;
4. Take children to a private place, which is away from the vicinity of other staff or children;
5. Give gifts or take photographs in a personal capacity;
6. Show materials or share jokes or stories that are sexual in nature or discuss such issues with a fellow staff in the vicinity of children

If any incidence occurs, employees/volunteers/ associates must:

1. Listen to the child
2. Note exactly whatever is said to CI employees/volunteers/ associates seriously (avoiding any assumption) and help the child to trust her/ his own feelings
3. Not to allow investigation of any allegation by the staff involved in it. Any disclosure by a child must be reported to the CI management or any organizational committee appointed for this purpose.
4. Speak immediately to the higher management for further advice and guidance
5. Treat all children with kindness
6. Never disclose any information about the children/ children's home, where CI operates, to any third party without consent of the family or organization management, as the case may be

If anyone comes across any violation of the above, that may immediately report to CI management or its authorized committee

This policy document is subject to five years review by CI management.

Name of the Employee: _____

Signature: _____

Date: _____

CONFLICT OF INTEREST POLICY
By Change Initiatives
Date: 15/09/2017

Conflicts of interest are potential problem areas that may affect the integrity of the organisation and the financial and value for money aspects of its activities. The most obvious areas are procurement, recruitment, disbursement and community works- where benefits are delivered to most vulnerable persons.

This conflict-of-interest policy of Change Initiatives (CI) is directed to its directors, officers, members of the management and all employees who can influence the operations of CI. This will include, for example, person(s) involved in the process and decisions in procurement, recruitment, grants making, disbursement and all those working directly with the communities where their positions can be used to their personal gains, which are detrimental to the beneficiaries.

Conflicts of interest may arise in the following areas:

1. Persons involved in initiating, processing and approving procurement transactions
2. Persons involved in initiating, processing including interviewing, selecting, hiring and assigning salary and benefits
3. Persons involved in initiating, processing including interviewing, selecting, approving awarding and following up grants or sub-grants
4. Persons involved in initiating, reviewing, approving and authorising payments
5. Persons working directly with communities, in the delivery of benefits accruing from CI programmes/ projects.

All conflicts of interest must be declared well in advance of any engagement where a potential conflict of interest may arise.

CI will not allow any form of deliberate, undeclared conflict of Interest. Any violation of this policy will be considered as an act of misconduct and anyone subject to this policy who is found in violation will be held accountable to the extent of the effect of his or her actions.

The policy is subject to 5 years review by the management.

If anyone comes across any violation of the above, that may immediately report to CI management or its authorized committee

This policy document is subject to five years review by CI management.

Name of the Employee: _____

Signature: _____ Date: _____

Policy Statement

All identified business data at Change Initiatives (CI) shall be controlled and protected in all phases of its life cycle including collection, processing, transmission, storage, exchange and retirement.

Roles and Responsibilities

Information Owner

Chief Functionary shall be the Information Owner and shall be overall responsible for all business information assets. Responsibilities would include, but not be limited to:

i. Nominate Information Sub-owners for each Program under CI.
ii. Assigning business information classification and periodically reviewing the classification to ensure it still meets business needs

Information Sub-owner

Program/ Project Directors shall act as Information Sub-Owners and shall be responsible for following:

i. Ensuring security controls are in place commensurate with the classification
ii. Reviewing and ensuring currency of the access rights associated with information assets they own
iii. Determining security requirements, access criteria and backup requirements for the information assets they own

Data Protection Officer

Program Managers will primarily be the Data Protection Officer (DPO) for protection of information managed at the head office and the branch managers for respective branches or field offices

i. As DPO, s/he shall be responsible for implementation of this policy for Data Identification and Data Inventory Management.
ii. DPO should maintain a Data Distribution list, of all identified data, having details of users who have been approved for access of these data. Details should include User, Data and Access Time Period.

Data Consumer (End User)

The end users shall be any employee including program/ project officers and staff, contractors or vendors of CI who use information systems resources as part of their job. Responsibilities include:

i. Maintaining confidentiality of log-in password(s)
ii. Ensuring security of information entrusted to them as a part of job responsibility
iii. Using information assets and resources for management approved purposes only
iv. Adhering to all information security policies, procedures, standards and guidelines
v. Promptly reporting security incidents to management

IT System Administrators

IT System administrators shall be responsible for day-to-day operational management of information systems including performing backups, restoration, administration of user IDs and access rights, reporting and following up on security violation reports etc.

Data Classification

Based on its sensitivity to business operations, all identified data should be classified under one of the following categories:

Classification	Description	Examples
Public	Information that is available to the general public and intended for distribution outside the organization. This information may be freely disseminated without potential harm.	- Information available on the organization's website - Information in program brochures, reports
Internal	Information that is deemed sensitive due to financial or legal ramifications and which is for use only by authorized CI employees and auditors, consultants, vendor personnel, legal and regulatory authorities.	- Organizations policy documents - Standard operating procedure documents - Minutes of the meetings
Confidential	Information that is proprietary to CI and its unauthorized disclosure could adversely impact the organization, its employees and other stakeholders.	- Beneficiaries' and employees' personal identification information - Beneficiaries' account information
Top Secret	Information that is so confidential that leak of such information can severely impact the organization, its employees and all the relevant stakeholders	- Organization's financial information - Information related to key IT Infrastructure

Data Protection and Sharing

Following controls should be implemented for the protection of data:

1. Access to data should be controlled based on classification of data and need to know basis.
2. Access to electronic data, stored on system, should be provided after user authentication at least with unique user ID and Password based on a clearly defined password policy.
3. Access to electronic data, stored on system, should be limited to appropriate privilege level according to job responsibilities as per business requirement.
4. Access to data for consultants/third party users should be provided on need-to-know basis

Data Storage

1. Data Storage and Retention should be done with measures adequate to its classification.
2. Confidential data should only be stored in locations which are approved by DPO.
3. Password protection should be used for files/folders and email accounts on users

4. Confidential papers/printed documents should be kept in cabinets with lock and key mechanism in fire proof safe. Only authorized persons should have access to such documents. Key allocation should be recorded in a key maintenance register and key access should be reviewed by data protection owners.

Data Retention and Retirement

1. Information owner/sub-owners should define the data retention period based on operational need.
2. After expiry of defined retention period, data should be disposed or discarded with appropriate methods based on data classification.

Data Exchange and Disclosure

1. A Non-disclosure agreement should be signed prior to exchanging data with third parties, applicability of which will be decided by CI management.
2. All information security requirements must be defined clearly in the service agreement with third-party for data protection.
3. Only the relevant and minimum amount of data necessary should be shared with third parties.
4. Such agreement should also cover the acceptance of third-party for full co-operation and assistance in case of any incident or fraud detection

Monitoring and Review

1. All access to, modification or deletion of data by users should be logged. Logging methods and levels should be decided based on data classification.
2. All privileged access to data stores should be logged and monitored. These should be reviewed by overseeing authority on regular basis.
3. CI should conduct annual compliance audit to verify compliance to this policy and applicable legal, regulatory and industry requirements for data protection.

The policy is subject to 3 years review by management.

If anyone comes across any violation of the above, that may immediately report to CI management or its authorized committee

This policy document is subject to three years review by CI management.

Name of the Employee: _____

Signature: _____ Date: _____

Change Initiatives (CI) is committed to adhere to the standards of ethical, moral and legal conduct of its operations. To maintain these standards, the organisation encourages its employees and associates who have concerns about any suspected misconduct to come forward and express these concerns without fear of punishment or unfair treatment. This policy aims to provide an avenue for the employees to raise concerns on any violations of legal or regulatory requirements, incorrect or misrepresentation of any financial statements and reports, taking bribes, form parties etc.

Raising a concern

Every person, to whom this policy applies to, is encouraged to raise their concerns about any bribery issue or suspicion of malpractice at the earliest possible stage and these should be raised with the anti corruption committee or any such committee appointed for this purpose in writing.

The contents of such complaint should not be like normal grievance redressal matters or be a route to raising malicious or unfounded allegations against colleagues. The act of making allegations made recklessly, maliciously or with foreknowldege that the allegations are false, will be viewed as a serious disciplinary offense.

Protection

A whistleblower has the right to protection from retaliation. Retaliation includes discrimination, reprisal, harassment or vengeance in any manner. The employee will not be at the risk of losing her/his job or suffer loss in any other manner like transfer, demotion, refusal of promotion as a result of reporting under this policy.

If the whistleblower faces any retaliatory action or threats as a result of making a disclosure, the same should be infomrmed to the empowered committee in writing immediately. The committee will take cognizance of each and every such complaint/ feedback and investigate the same and may also recommend appropriate steps to protect the whistleblower and ensure implementaion of such steps of protection.

Confidentiality

Reports of concerns, and investigations pertaining thereto, shall be kept confidential to the extent possible. Disclosure of reports of concerns to individuals not part of the investigation team will be viewed as serious offence and may result in disciplinary action, upto and including termination of employment.

Accountability of whistleblower

- Bring to early attention ofthe management or committee any improper practice s/he/they become aware of
- Avoid anonymity when raising a concern
- Follow the procedure prescribed in this policy for making a disclosure
- Co-operate with investigating authorities, maintaining full confidentiality
- In exceptional cases, where the whistleblower is not satisfied with the outcome ofthe investigation carried out by the Whistle officer orthe committee, s/he can make a dierct appeal to the board/ executive committe of the organisation.

Accountability of concerned official(s) and anti-corruption committee/ empowered committee

- Conduct the enquiry in a fair, unbiased manner
- Ensure complete fact finding
- Maintain strict confidentiality
- Decide on the outcome of the investigation, whether an improper practice has been committed and if so by whom
- Recommend an appropriate course of action- suggest disciplinary actions including dismissal and preventive measures
- Record committee deliberations and document the final report

The policy document is subject to five years review ny the management.

If anyone comes across any violation of the above, that may immediately report to CI management or its authorized committee

This policy document is subject to three years review by CI management.

Name of the Employee: _____

Signature: _____ Date: _____

The original signed statement should be placed in the employee's personnel file and a copy should be provided to the employee.