Overview of NI-ABAE Anti-Bribery and Security Policies

Purpose of Document

This document provides an overview of key security policies, plans, and processes used to mitigate security issues. Also included is NI-ABAE's Anti-Bribery and Anti-Corruption Policy.

Anti-Bribery and Anti-Corruption Policy

Link to Policy: Anti-Bribery and Anti-Corruption Policy

Key Points:

- New Incentives - All Babies Are Equal Initiative (NI-ABAE) has zero tolerance for bribery and corruption.
- NI-ABAE has an Anti-Bribery and Anti-Corruption Policy which is part of the Employee Handbook. Senior managers are most likely to face situations where this policy is most relevant. In addition to this policy, as part of onboarding and terms of employment, all employees in Nigeria must sign various expense policies to reduce the chances of unethical engagements. Violation of these policies result in Disciplinary Actions.
- The organization takes a zero-tolerance approach to bribery and corruption and is committed to acting professionally, fairly, and with integrity in all dealings and relationships while implementing and enforcing effective systems to counter bribery and corruption. It is not acceptable for organization staff to give or accept facilitation payments and/or kickbacks of any kind.
- Staff is responsible for the prevention, detection, and reporting of any form of bribery and/or corruption. If a staff member is being extorted or coerced to pay facilitation payments and/or kickbacks when their safety, liberty, personal, and/or family well-being is under threat, the staff member is responsible to pay and immediately report the payment to the HR Manager (who has the responsibility to transmit the report immediately to the National Coordinator and Management) as soon as he/she is no longer under threat, within 24 hours.
- The policy is clearly communicated to ensure that all employees can understand concerning cases and raise them promptly with Human Resources.

NI-ABAE's Disciplinary Actions Policy is used to enforce policies -- policy and procedural breaches are tracked and escalated based on the severity of the breach and the number of times an employee has committed the breach.

Security Plan, Policies, and Related Processes

Link to Policies, Protocols, and Dashboards

- The Country Security Plan **(CSP)** is the key security document of the organization that speaks to the organizational policy, Standard Operating Procedures (SOPs), tools and management of the security of staff, the organization and our program in the North West.
- Security Dashboard: The incident reporting component is updated as the incidents occur (multiple times per week) while the other components are updated weekly with incidents for each clinic along with an assessment of incident severity. These reports are gathered from a variety of sources, including community stakeholders (such as community heads), local security enforcers, communities, networks, publicly circulated information, and membership access to information from local and international sources

- Weekly Security Assessment Reports: The security incidents are compiled into reports sent internally every week
- Clinic Schedule: Schedule for each staff for security confirmations and travel notifications
- Security Briefing Pack for Expatriates: Information on remaining safe while in Nigeria and/or in the field for non-Nigerian staff coming into Nigeria
- Clinic and Settlement Security Assessments: Risk-level, mitigation measures, and network coverage reports for all NI-ABAE clinics
- Summary Abduction Policy: This is a summary of the below comprehensive policy on abduction that is shared selectively; training is provided to all staff based on roles and responsibilities in case of an abduction
- New Incentives Abduction Policy and Procedures: The policy describes dealing with an abduction case in detail and is complemented with training for senior managers
- MOSS Audit: A tool updated monthly to assess how close the organization is to standard security policies and procedures of an NGO working in the Nigerian health sector
- Constant Companion Card: This tool is issued to all staff and it contains vital information for reference in case of an emergency by the staff or if a staff member is unconscious so that information is available to a nearby person. This will be carried by all staff so they know who to call in case of emergencies, along with their health and accident insurance information

Key Points:

- In line with the CSP, security tools and Standard Operating Procedures (SOPs) have been developed. The Security Unit issues security advisories to staff on a regular basis, as well as monthly internal reports to assess adherence to the CSP, identify critical gaps, and recommend improvements.
- The Security Unit is a separate Unit in the organization and manages the various security tools. These tools and processes are used to guide the day-to-day work of mitigating security threats in the organization. This is including but not limited to specific security questions that are programmed in daily data collection forms. The Security Unit is headed by a Security Manager and assisted by a Security Focal Person.
- In addition, Auditors (internal staff who are dedicated to program audits) conduct investigations to assess compliance to SOPs and report security incidents during routine program audits to identify information gaps and necessary reporting improvements.
- A contingency plan is currently being developed to address what is required when these SOPs fail while the Critical Incident Management Plan in the CSP is currently being expanded into a more detailed document with specific response to potential critical incidents. It is critical to understand that while the organization has not encountered a serious security incident to date, such security incidents can occur given the operating environment of the organization. The organization has witnessed the death of a staff member as a result of a car accident outside of work and the kidnapping of the relative of a staff member (unrelated to their employment).
- The management of SOPs include communication and training of staff after development, intermittent reminders to staff during supervision, review of data by the Console Unit, and spot checks by internal auditors to strengthen compliance.
- The Security Unit manages information sourcing, ensuring tools are up-to-date, and reviewing tools to make informed communications to staff to ensure staff safety and reporting recommendations to the National Coordinator and Management for decision-making. Managers have access to some of these tools for quick decision-making, operational planning, and implementation of program activities.
- Staff are trained on preventive action and responsive action through following SOPs (part of the Country Security Plan):
  - Road Safety
  - Cash Management
  - Abduction

    - Political
    - Ethnic and Religious Instability
    - Bad Governance
- Assessments of risks and threats are maintained at the level of the country (Nigeria), states, and clinic, along with details of incidents to inform staff activity and field travel.
- The Security Manager shares incidents with key team members if they are pertinent to NI clinics with significant action when needed. Information on incidents is disseminated to all managers in Nigeria on a weekly basis. In addition to this, the Security Unit shares monthly reports internally. Each monthly security report contains a MOSS Audit.
- Staff are instructed to wear seat belts during travel and vary their transportation routes when possible. Sensitization on the importance of following security procedures is done through in-person and virtual trainings on a monthly basis to constantly reiterate the importance of these policies. This is important because staff perceived level of risk is lower than what is required to take safety and security measures seriously since many staff are desensitized to security risks since they have grown up in this environment. Security is a part of staff job descriptions and responsibilities.
- A Crisis Management Team has been established with defined roles in Nigeria and at the HQ level to ensure the organization can take timely decisions and respond properly in case of serious issues affecting employee safety (e.g. abduction).
- The organization subscribes to a combination of insurance to mitigate security risks. Details of related insurance coverage and plans can be provided upon request.

Known Gaps and Actions Being Actively Addressed

- Ensuring that all field movements are conducted according to the Field Travel Standard Operating Procedures
- Lack of contingency plans for unanticipated events: development of plans and training for adverse situations not covered by SOPs is currently ongoing
- Lack of means of communication in remote locations where telecommunication service providers can be unavailable at times: ongoing assessment of need and review of the feasibility of a secondary/satellite communication system
- GPS tracking of staff in the field: Process ongoing with staff sensitization on value and utilization and development of tools with limited permissions and defined processes

Responses to Questions

- How do you protect your staff and, in IDinsight's case, contracted surveyors, from violence in the field?
        - We have built acceptance in the communities through engagement with community gatekeepers (village heads, barbers, TBAs) who provide us information
        - We provide ongoing training to our staff on preventive actions to reduce the chances of incidents and actions to take in case of an incident
        - The Security Unit utilizes multiple sources to obtain information which is fed to the Operations Unit through Field Managers
        - Field Officers review the security situation in their destination before moving to the clinic or settlement for activities and if in doubt, reach out to their Field Manager to determine their travel route and whether it is safe to visit
        - Ongoing contingency plan development will provide information on escape routes and safe places in settlements in case of incident while on the field
    - Where do you source your information about security risks, and who decides if a place is safe enough to visit?
        - We get our information from a variety of sources, including community stakeholders (such as community heads), local security enforcers, communities, networks, publicly

        circulated information, and membership access to information from local and international sources
        - The Security Unit and Field Managers decide whether a given locality is safe enough to visit
    - How often do you review your own security procedures and information sources?
        - The activities of the Security Unit are reviewed by the National Coordinator weekly, including basic review of the security procedures and information sources
        - Monthly Security Reports including MOSS Audit findings and Security Dashboard are reviewed by the COO on a monthly basis
        - Key security procedures were created with the help of experienced security consultants; new procedures are reviewed by Michael O'Neil, a security consultant, on an ongoing basis
        - A comprehensive security review was done in Q2 this year and the next one is expected in Q2 of 2020
- How do you prevent staff or contractors from paying bribes, e.g. paying off a group for protection in an otherwise dangerous area?
    - The Anti-Bribery and Anti-Corruption Policy communicates the organization's zero-tolerance policy to giving or receiving bribes
    - This is communicated to staff in their Employee Handbook that is shared upon employment and during onboarding
    - Expenses are tracked and signed off by at least two sources other than the submitter - locally by the Line Manager and outside of Nigeria through the Console Unit so it is difficult to use organizational funds for unauthorized purposes