# Garib Unnayan Sangstha (Gus)

# Security Policy

## APPROVED BY 11 - 03 - 2021

## Table of Contents

# Introduction

Kurigram district is a neglected and undeveloped area of the country in Bangladesh. 16 rivers, including the Brahmaputra and Jamuna, the major rivers of the country flowing across the wider area of the northeast of this district, resulting in floods, river erosions and other disaster districts, and floods every year, floods, rivers Due to breakdown, monga, cold wave and Tornado, hundreds of families are landless, homeless, and without resources. Because of the communication system and disaster, people of this region are deprived from all walks of life, factories are not in the same place, and other business commerce has not spread so much that there is no opportunity for local employment in the locality. There is no scope for employment throughout the year, as well as the natural disaster, especially the river erosion, and whistle thunderstorms, there is a chance of poverty in the daily life of the people living in poverty, and in the education and health sectors, the opportunities for poor people are reduced. Thus, the area is losing livelihood due to the loss of the environment and is being endured due to over exploitation of population and superstition. Location is very sorry they are family members There are many types of physical and mental tortures, including the lack of employment and fair wages, besides the lack of discrimination and bigotry, religious harassment, prejudice has been denied from all rights of women.

## Introduction of the Organization

Since 12 February 1998, some progressive youths Females and males together have been given good governance with the rights of poor women in the area. By organizing the poor people for establishment, a community base will be organized As a Organization (CBO), Garib Unnayan Sangstha (GUS) was established and as a non-political, non-profit volunteer and social welfare organization, the organization later took the registration from the Bangladesh Social Services Department in 2001, after the registration of the various socio-economic development of the poor Initiating and implementing development programs and registering from Bangladesh NGO Affairs Bureau in 2006 After adoption, the expansion of various development programs for the socio-economic development of the poor people. The organization is currently implementing the benefits of various services and funding activities with the assistance of different donors, including humanitarian assistance during various disasters. Our Organization signed the Charter for Change (C4C) Endorsers And the native is foreign Connected to different networks.

Our organization since 1998 Different Donors E.g. Food & Agriculture Organization of the United Nations (FAO),Islamic Relief-Bangladesh (IRB), UNDP, WFP, Oxfam Bangladesh, World Bank through DPE, IDB through DAE, Royal Danish Embassy and Khan Foundation, GIVEWATTS East Africa Limited, NGO Forum, Department of Public Health & Engineering (DPHE),BRAC Education Program ,The Hunger Project, Directorate of Environment, Upazila Health Complex, Rajibpur, Kurigram, Grameen Shopno, Gano Shakhsarota avijan, WBBTrust, Bangladesh folito pusti, Through its various trainings the various policy update processes of the organization. National and international level Gain membership of different networks And communicate directly with donors and job opportunities have been created. Our Organization signed the Charter for Change (C4C) Endorsers and the natives foreign Connected to different networks. Country level to Global level. That includes local level coordination platform such as Humanitarian Actors Platform in Kurigram (HAP-Kurigram, COVID-19 District &Upazila) Comity Member, ADAB, FNB, NGO Forum, Rajibpur Rowmari NGO Network, Sujan, Konna Shishu Advocacy Forum, Red Crescent Societies Bangladesh, KNA; at national level GUS engaged with Need Assessment working group, Cash Working group, food Security Cluster, National Alliance of Humanitarian Actors Bangladesh (NAHAB), Localization Working Group; at international GUS is connected with Charter 4 Change (C4C) Endorsers, NEAR, Alliance for Empowering Partnership (A4EP), GIVEWATTS East Africa Limited, Smart Response, Global Giving, MYCORPS MISSION 8 @ SOUTH ASIA II. These platform and network created a wider space to the GUS as well as increased their visibility towards the humanitarian actors in the country level and Global level that upholds their voice and space in the humanitarian sector. the native is foreign Connected to different networks.

***We believe in working Our Organization according to the core Humanitarian Principal.***

## Purpose

The purpose of the security policy is to record and communicate the guiding principles and responsibilities that form the governing framework for security risk management.
The policy provides managers and staff direction and guidance to enable Gus programme objectives to be effectively implemented while at the same time protecting (to the extent possible) Gus employees, reputation and assets from harm.

## Complementarily with other Governing Frameworks & Codes

Several governing frameworks guide Gus program and operations management and shape Gus' overall behavior and approach to its work. The security policy forms part of the set of governing codes and agreements that Gus willingly commits to.
The security policy is complementary to the following governing frameworks:

- Gus Code of Conduct
- Gus Security Protocol
- Gus Single Management Structure Agreement (SMA)
- People in Aid Code of Good Practice
- The Code of Conduct for The International Red Cross and Red Crescent Movement and NGOs in Disaster Relief
- OI and Security Crisis Management: Recommendations of the OI Security Network Working Group
- Guidance Note: Obtaining Authorization to Use Armed Escorts/Guards: An Exception to the OI Security Protocol
- SCHR Position Paper on Humanitarian Military Relations

Where necessary the governing frameworks are referenced in the policy. However the complementarily noted above is not intended as a cross-referencing guide to readers. Complementarily refers to the **security policy forming part of a specific set of governing references**, and as such communicates policy positions and principles that are aligned with, supportive of, or analogous with the other codes and agreements.

## Applicability and Policy Implementation

The security policy applies to Gus organizations (as independent legal entities and employers), and their employees. In certain circumstances, and depending on the nature of the relationship, the policy may apply to associated personnel. The security policy shall be routinely implemented as part of program or operational management activities.
The Gus Security Protocol outlines the architecture by which security will be managed. It is acknowledged that the local operating context will influence how the security policy is put into practice; however the principles contained in the policy shall be reflected in local security and/or crisis management plans and procedures.

## Security Management Approaches

Security must be actively managed, not just planned for, and is most effective when fully integrated into program management. Managers must ensure security of persons and programs is given a high priority, through objective setting, the performance management cycle, work planning/scheduling and other relevant management tools. Security management approaches are informed by an understanding of the local context and based upon the outcomes risk assessments. Generally approaches are not mutually exclusive; the key is to adopt the right mix in a given context.
**Acceptance** approaches reduce or remove threats by gaining widespread acceptance (political and social consent) in the community for Gus' presence and activities. Building positive relationships and promoting understanding of Gus through establishing our legitimacy as an impartial and independent humanitarian actor, achieves this. This identity must be communicated clearly to all parties. The success of an 'Acceptance' approach depends on many factors including staff behavior, staff diversity, type, design and implementation of programs, community participation, choice of partners and proactive creation and maintenance of relationships.

**Protection** approaches aim to reduce risk by reducing vulnerability, through protective devices and operating procedures. Protective devices can be communications equipment, reliable vehicles, use or non-use of Gus' branding (e.g. displaying the logo), or perimeter protection for premises. Operating policies and procedures include locally based security management plans and standard operating procedures (SOPs), including evacuation plans, equitable staff policies, and other program management policies and procedures relevant to the local context.

**Deterrence** approaches aim to reduce risk by containing or deterring the threat by applying a credible counter-threat (e.g. suspension or withdrawal of activities, or the use of armed guards *in exceptional and authorized circumstances only*, or calling for military intervention. This approach is generally to be considered as a last resort, and is decided according to specific procedures and authorization levels.

## Risk Attitude & Risk Tolerance

Almost every operational activity presents threats to personnel and assets. Guided by the humanitarian imperative, Gus' risk attitude is aligned with its mission statement. GUS will **always assess and communicate the level of risk** in a given context and take informed management decisions to accept or avoid these risks.
The humanitarian imperative is reiterated in the security policy as a reminder to employees that acting in a safe and secure manner enables Gus to meaningfully uphold the rights of this fundamental principle.
Risk assessments aim to provide information in sufficient detail in order for managers and other employees to take informed decisions. Gus' risk assessments shall take account of the following minimum considerations:

- The specific operating context and regional influences
- The foreseeable threats to personnel and programs
- The impact foreseeable threats may have on Gus' personnel and programs
- The factors that expose or make Gus vulnerable to these threats
- The available options to treat the risks presented by these threats

Gus' **0** Tolerances to take risks will **always take account of program objectives and the importance of what is to be achieved,** as well as the impact of other strategic factors (e.g. impact of key relationships, donor interests, etc). Risk owners will decide on a case-by-case basis whether the specific program objectives and intended outcomes justify accepting the assessed level of risk. It is important to note that Gus works in some of the most challenging, hazardous and dangerous environments. When humanitarian needs are high, Gus may accept a higher level of risk. In such situations an even greater emphasis on security management is essential.

### Principles

In the context of the Gus security policy, **principles** contain the overarching rules and beliefs that govern Gus's approach to security management. The principles are intended to provide clarity to certain policy positions and guide risk management decisions and actions

## Duty of Care & Security of Personnel

Security of personnel (whether employees or others) shall always remain a higher priority than the protection of material assets, the preservation of programs, the expression of advocacy objectives, or the protection of Gus's reputation.
Gus' duty of care is exercised through the application of the security policy, and other management policies and procedures. The systems developed to manage duty of care include (but are not limited to) informing employees about work-related risks, preparing employees to manage and treat risks, and seeking to ensure post-incident care (e.g. counseling for victims, their families, and/or colleagues) is available to employees.

## Risk Ownership & Delegation

Security management is a line management responsibility in Gus. All Gus employees and the various governing boards and executive officers are risk owners. Risks owners are defined as *"the persons with the decision making authority and accountability to manage risks.*

The exact level of risk ownership, accountability and responsibility of these individuals or collective bodies will vary depending on their assigned roles, and may be influenced by national laws or regulations concerning legal liabilities.

Risk ownership and the subsequent security management responsibilities shall be communicated in official Gus records including but not limited to employment contracts, job descriptions, terms of references, minutes of governing or executive body meetings, explicit instructions and delegations of line management, or official agreements and policies.

## Informed Consent & Right to Withdraw

Via their respective line managers, employees shall be informed of the foreseeable risks related to their role and their place of work. By accepting the assigned duties after having been provided with relevant information, the employee is generally deemed to have provided their informed consent to accept these risks and the risk treatment options and processes implemented by the employer.

Employees may decline to undertake an assigned duty if their individual risk tolerance is lower than that of their employer. Likewise employees may withdraw from a location for the same reason. If withdrawing from a duty station for security reasons, employees shall immediately inform their line manager and as soon as practical record the reasons for the withdrawal. Such cases shall be subject to procedural review by the employer.

## Individual Obligations & Self Generated Risks

Gus employees are obliged to work with their employers to manage risks, and are responsible for taking reasonable and meaningful actions to manage their own safety and security. Individual behavior is key to an employee's own safety and security as well as that of the organization, co-workers and the effect on program objectives. It is very important that each and every employee accepts this responsibility, and understands that failing to adhere to security plans and other behavioral guidelines can put other people at risk. Negligent actions that create self-generated risks are likely to lead to dismissal or other disciplinary action.

## Gender and Security

Men and women can be, and often will be affected differently by specific threats. Likewise men and women may perceive or understand risk differently because gender influences an individual's vulnerability to certain threats. Gus' security policy recognizes gender as a potential vulnerability factor when assessing risks. Likewise gender may influence specific risk treatment options, and used to reduce the risk of harm (e.g. deciding to deploy or not deploy only men or only women to a certain context for a specific program objective). Risk assessments, local security management plans and subsequent risk treatment options shall explicitly communicate how gender is considered within the local context.

## Non-Discrimination & Equality of Risk Treatment

A specific threat may produce different levels of foreseeable risk between different groups working in the same operating context. Gus' risk attitude and approach to security management is non-discriminatory and shall ensure risk treatment options produce (to the extent possible) equal protection for employees and associated personnel. This may require different risk treatment approaches, strategies, procedures or resources for specific individuals or groups even if these individuals or groups are working in the same operating context on the same program.
While risk treatment may sometimes appear unequal (e.g. different rules between national and international employees), the resultant level of acceptable risk is the intended outcome of a non-discriminatory approach to security management that aims to be applied without distinction or discrimination of any kind.

## Privacy of Information

Gus should act responsibly to ensure personal and other information is used, stored or disposed of appropriately, and should have regard to relevant regulatory requirements Local SMPs may also need to address privacy or data protection in terms of electronic networks, and/or hard copy files.

## Individual Employees

Gus employees are responsible for:

- Complying with all security policies, procedures, directions, instructions, regulations or plans
- Taking care of their own safety and security and of the staff they manage
- Actively contributing to the development and maintenance of security management policy and procedures
- Ensuring their behavior is in line with Gus' governing frameworks
- Reporting security incidents up and down their management line

## Line Managers - Generic

Line managers are responsible for:

- Ensuring their staff and associated personnel have access to security management policies, plans and procedures
- Monitoring compliance to security policies, plans and procedures by their staff
- Reporting security incidents up and down their management line
- Identifying staff security training, learning and development needs and ensure access to the training (including appropriate planning and resourcing)
- Reporting organizational security management performance on a regular basis to governing bodies

## Responsibilities:

### Line Managers - Directors & Associate Actors

In accordance with the GUS Security Protocol, Director and Associate organization are **responsible for ensuring an appropriate security management system is in place** for their respective offices and/or programs. This obligation will involve a combination of the listed responsibilities for individuals, line managers and directors as contained in the policy and other governing documents. In addition Director and Associate Director are to work with the Leadership Team (where applicable) to ensure that minimum standards are met for program management, human resources, finance, security, and health and safety.

In addition to the above, Director and Associate Director are responsible for:

- Effectively delegating specific security management roles, tasks and functional responsibilities (whether to security-specific employees or others)
- Leading and managing the review and updating of local SMPs
- Contributing to establishing a local security information networks

## Other Directors & Executive Officers

Directors and Executive Officers are responsible for:

- Ensuring full implementation of GUS security policy
- Ensuring security management needs are identified and effectively communicated in program proposals and reports
- Ensuring adequate resources are made available to address security management needs
- Ensuring a crisis management process is developed, implemented, and periodically tested
- Holding line managers and employees to account for individual behaviors and attitudes towards security risk management
- Reporting on an annual basis to governing bodies (e.g. boards or councils, donors, etc.) Gus' security management performance

## Security Working Group (SWG)

The SWG is a forum where Gus affiliates share security information, exchange ideas and discuss proposals to achieve a coordinated approach to security management.
The group is responsible for:

- Exchanging security information to encourage better security management practices
- Providing support and advice to line managers on the development of security procedures and plans for each all.
- Coordinating and following up on Gus' participation to external security networks
- Agreeing on Gus' representation to national security networks
- Facilitating learning and exchange experiences
- Making proposals and recommendations regarding security management coordination within the collective Gus membership
- Coordinating with Gus security focal points (SFP) on security management issues

## Governing Bodies (e.g. Boards, Councils, etc.)

Governing bodies are responsible for:

- Providing explicit governance and oversight of security management performance
- Holding directors and executive officers accountable for security management performance

## Security Levels

Gus' security management actions shall be guided by assessing foreseeable risks in a given operating context. The overall risk shall be allocated a measurable security level and the security levels shall be communicated in local security management plans, and be subject to regular review.

## Security Management Plans

Security management plans (SMP) must be available in all Gus offices. SMPs shall be subject to periodic review to ensure the information remains current. SMPs shall be accessible to all employees and associated personnel working in the operating context relevant to the plans. SMPs and all associated documents must be translated into the appropriate working language.

## Security Incident Reporting

All security incidents, including minor incidents and near misses, must be reported immediately via line management or other locally defined reporting lines. Security incident reports shall be shared as widely as possible within Gus and its implementing partners,

and when appropriate, shared with others (e.g. United Nations organizations, other INGOS,NGOs, local authorities, etc.)

## Evacuation, Relocation & Hibernation

In the context of the Gus security policy, *"evacuation, relocation and hibernation"* are processes intended to move persons to a safer location, or remain in a sustainable safer location. Security management plans shall explicitly address evacuation, relocation and hibernation needs, relevant to the local context. Such plans will communicate decision- making authority (as reflected in other governing documents referenced in the policy), delegation of responsibilities, the criteria for which persons shall be moved and when, and the processes for evacuating, relocating and hibernating. In accordance with the Gus Security Protocol, Directors and Associate Directors of the managing affiliate are responsible for leading and managing evacuation, relocation and hibernation activities.

## Implementing Partners

Partners are responsible for their own security management. If necessary Gus may assist partners to build their own local capacity to effectively exercise this responsibility. This assistance may include training, information sharing, mentoring, provision of security management resources, or a combination of these. Directors shall decide if assistance to partners is necessary, and the extent of any such assistance. Gus shall consult with partners on context and risk analysis and share security management information with them (as appropriate to the local context). The partners are encouraged to report incidents to Gus. Gus will not expect implementing partners to work at locations that we consider too insecure or unsafe to work ourselves unless the risk transfer is clearly demonstrated as acceptable to both parties.

## Use of Armed Protection

Armed protection is only compatible with Gus principles and programs in exceptional circumstances. Generally the use of armed protection is an absolute last resort option to reduce risk.
Gus *Guidance Note: Obtaining Authorization to Use Armed Escorts/Guards: An Exception to the OI Security Protocol (April 2019)* states:

*"Exceptions to the protocol may be considered and authorized, according to the process outlined, when there is a compelling programme reason, when the threat is largely banditry, not political, when an acceptable provider is available and when the deterrent will be effective. Exceptions may be sought for a specific time period (if long-term, it must be reviewed annually at a minimum), for a specific project or for a specific one-off activity. However, in extreme and time critical situations, the use of armed escorts for emergency relocation and evacuation may be authorized by the most senior staff member present."*

## Engaging with Armed Actors

Gus' relationships with armed actors are guided by the *SCHR Position Paper on Humanitarian Military Relations (January 2018)*. Gus will engage with any third party it

Deems necessary in order to achieve stated programme objectives. At times this may include engaging (having indirect or direct contact) with armed actors. Such contact with armed actors shall only be pursued after consideration of the associated risks and when it is reasonably assessed the desired outcomes will support programme objectives.

## Crisis Management

The security policy aims to help reduce the likelihood of a crisis event affecting Gus' personnel or programs. Specific crisis management systems form part of Gus' overall security management approach, and are designed to address foreseeable events such as abduction or kidnapping.

As necessary Gus will develop and implement management systems to address context- specific issues that may present a crisis. Gus' crisis management systems include all-level crisis management plans and although contextual, will aim for the following priorities and objectives:
Crisis Management Priorities:

1. Safety of employees and associated personnel
2. Reducing programmatic and operational disruption
3. Protecting Gus' reputation

Crisis Management Objectives:

1. Resume usual programs and operations as quickly as possible, or
2. Transition to an alternative means of programs and operations, or
3. End programs and operations in a given context

## 4.No Ransom or Other Concession

Gus does not pay ransoms, or concede to other demands from belligerent parties who threaten Gus employees or associated personnel. When appropriate, in serious incidences when employees are the victim of kidnap (or similar circumstance) Gus will support the work of relevant police forces (or other authorities) with the legal jurisdiction to act on such matters.

## Training, Learning & Development

Gus will take continued actions to build the security management capacity of its National workforce. Employees (and where assessed as relevant and appropriate, associated personnel) will have access to security-related training and professional development opportunities during their employment term as appropriate. Security management training strategies shall be determined and communicated to all relevant parties. These strategies must include an assessment of current security skills and competencies, gaps between current skills and those required due to assessed risks, resources, and explicit reference to budgets sufficient to meet training needs.

# Annex A: Gus Code of Conduct

## *Introduction*

As one Gus (*any Gus Affiliate and / or Gus national throughout the country)* we are a strategic network of organizations working together nationally to find lasting solutions to poverty and injustice. We share a common vision, common philosophies and, to a large extent, common working practices. We all have the same brand values, the same passion and commitment. We have joined forces as an national confederation because we believe we will achieve greater impact by working together in collaboration with others.

Together we are working towards a world in which people can live with dignity, have their basic needs met and their basic rights respected, and have the ability to control their own lives.

As we work to achieve our ambition and vision of 'a just world without poverty' we should always remain true to our core mission, aims and values. This Code of Conduct will help you live by them by providing guidance in the face of ethical dilemmas you may experience. It shows you what to do when a situation is complex by providing standards and values for you to follow and how to protect against situations that may damage you or Gus. It also seeks to ensure that employees avoid using possible unequal power relationships for their own benefit.

The rules and guidelines contained in this Code of Conduct, together with your employing affiliate's policies and procedures and the terms and conditions of your employment (as outlined in your employment contract or your collective agreement if applicable), provides a framework within which all Gus employees, regardless of location, undertake to discharge their duties and to regulate their conduct. They also support Gus in our role in implementing, monitoring and enforcing these standards.

The Code does not exempt anyone and in accordance with the relevant employing affiliate's policies and procedures, any breach may result in disciplinary action (including dismissal in some instances), and in some cases could lead to criminal prosecution.

In accepting your appointment you undertake to discharge your duties and to regulate your conduct in accordance with the requirements of this Code, thereby contributing to Gus' quality of performance and reputation. The code describes what Gus expects from its employees and what the employees can expect from Gus.

Whilst recognizing that local laws and cultures differ considerably from one country to another, Gus is an national Non-Governmental Organization (NGO) and therefore the Code of Conduct is developed from national, International and UN standards.

***This Code is subject to relevant international human rights law, wherever the employee is employed and shall be read in a manner that is compliant with that law. Standards & Values***

## As an Gus employee I will:

### *1. Uphold the integrity and reputation of Gus by ensuring that my professional and personal conduct is demonstrably consistent with Gus' values and standards.*

I will seek to maintain and enhance public confidence in Gus by being accountable for the professional and personal actions I take and ensuring that I manage the power that comes with my Gus position with appropriate restraint.

Whilst observing the requirements of the Code of Conduct, I will also be sensitive to, and respectful of, local customs and culture, even if the norms and values in that cultural context

Differ from the Code of Conduct. I will if necessary seek (and will receive) support and advice from Gus.

I will not work under the influence of alcohol or use, or be in possession of, illegal substances on Gus premises, vehicles or accommodation.

***2. Treat all people with respect and dignity and challenge any form of harassment, discrimination, intimidation or exploitation.***

I will contribute to a working environment characterized by mutual respect, integrity, dignity and non-discrimination.
I will ensure that my relationships and behavior are not exploitative, abusive or corrupt in any way.
I will respect all peoples' rights, including children's rights, and will not engage in any form of abuse or sexual exploitation of children (as defined in the Child Protection Policy), or of any persons of any age.
With beneficiaries, I will not exchange money, offers of employment, employment, goods or services for sex nor for any forms of humiliating, degrading or exploitative behavior.
I will use my best endeavors to report any such behavior or malpractice in the workplace by others to my line management or through recognized confidential reporting systems.

***3. Perform my duties and conduct my private life in a manner that avoids possible conflicts of interest with the work of Gus.***

I will declare any financial, personal, family (or close intimate relationship) interest in matters of official business which may impact on the work of Gus (e.g. contract for goods/services, employment or promotion within Gus, partner organizations, beneficiary groups).I will advise Gus of any intention to seek a nomination as a prospective candidate or another official role for any political party or public office to clarify whether any conflict, or perceived conflicts, with my duties with Gus may arise.
Even when the giving and acceptance of gifts is normal cultural practice I will reject monetary gifts or inappropriate gifts from governments, beneficiaries, donors, suppliers and other persons, which have been offered to me as a result of my employment with Gus. Where the giving and acceptance of gifts is normal cultural practice, I will ensure that such gifts are within the limits of reasonable judgments and in accordance with procurement policies and I will report gifts to the line management and where appropriate hand them onto Gus.

I will assure that assistance by Gus is not provided in return of any service or favor from others.

I will act against any form of corruption and not offer, promise, give or accept any bribes.

***4.Be responsible for the use of information, equipment, money and resources to which I have access by reason of my employment with Gus.***

I will use my discretion when handling sensitive or confidential information.

I will seek authorization before communicating externally in Gus's name and will avoid any unintended detrimental repercussions for me or Gus.

I will appropriately account for all Gus money and property, (e.g. vehicles, office equipment, Gus-provided accommodation, computers including the use of internet, email and intranet).
1. Protect the health, safety, security and welfare of all Gus employees, volunteers and contractors.
I will undertake and act on appropriate risk assessments.
I will comply with local security management guidelines and be pro-active in informing management of any necessary changes to such guidelines.
I will behave in such a way as to avoid any unnecessary risk to the safety, health and welfare of myself and others, including partner organizations and beneficiaries.
2.Promote human rights, protect the environment and oppose criminal or unethical activities.
I will ensure that my conduct is consistent with the human rights framework to which Gus subscribes.
I will use my best endeavors to protect the natural environment and work in a sustainable way.
I will contribute to preventing all forms of criminal or unethical activities.
I will inform Gus of any relevant criminal convictions or charges I have had prior to my employment in which Gus may have a legitimate interest.

I will also notify Gus if I face any criminal charges during my employment that may impede my ability to perform the duties of my position subject to national legislation.
I will adhere to following policies and procedures (see list below) that support the above Standards:

- Child protection
- Anti harassment and bullying
- Disciplinary procedures

In accepting my appointment I undertake to discharge my duties and to regulate my conduct in accordance with the requirements of this Code thereby contributing to Gus's quality of performance and reputation.

## Annex B: Gus Security Protocol

(As reviewed March 2021)

### Vision

Gus recognizes that working in complex environments may entail staff being present in insecure and violent contexts. Affiliates undertake to reduce the risk of operating in such environments by effective security management.

Close collaboration of Affiliates in the management of security will lead to effective and efficient programme delivery, as well as seeking greater safety and security of staff and assets. This protocol outlines the architecture by which this vision will be realized through provision of principles, standards and guidance.

The Gus Security Protocol is mandatory for all countries and all Affiliates.

### General agreements

1. Staff safety and security is a higher priority than the protection of material assets, the preservation of programmes or the expression of advocacy objectives.
2. Affiliates recognize the impact that their staff behavior, actions and programmes may have on Gus' overall reputation and brand, and hold each other accountable.
3. Security management is an integral part of programme management and as such subject to systematic and methodical discussion at all levels.
4. The right of individual staff to withdraw from insecure situations is supported by all Affiliates.
5. In our humanitarian work, affiliates work according to the principles in the Code of Conduct for The International Red Cross and Red Crescent Movement and NGOs in Disaster Relief.
6. Affiliates agree not to use armed guards and that staff will not carry or take up arms. However, the exceptional use of armed guards may be authorized by the Executive Director (ED) of the Managing Affiliate (MA), following a collective risk analysis
7. and decision by all Affiliates present. The ED will advise other Affiliate ED's present of the specific circumstances of the authorization.
8. Affiliates agree not to make statements or undertake activities that could compromise Gus' standing as an independent party, based on Gus' policies and principles, and sign-off systems and procedures.
9. Affiliates will respect the confidentiality of what has been shared with them.

### Global agreements

Affiliates must have a Global Security Policy and a Crisis Management Plan in place. The Gus Security Network Working Group monitors compliance on an annual basis, on behalf of the PDG.

The Global Security Policy should be proportionate to the Affiliates mandate, programme and mode of operation. It should clearly articulate the expectations the Affiliate has of its employees and the responsibility the Affiliate assumes on behalf of its employees.

The Crisis Management Plan establishes arrangements and resources required to manage a critical security incident that is so complex or acute (such as kidnap) it cannot be managed adequately within the normal scale of operations.

The plan provides a framework for necessary steps during such a crisis and its immediate aftermath.

**agreements**

1. The Executive Director (ED) in consultation with the Associate Directors , and managers from other Affiliates present in that all program, is responsible for ensuring an appropriate security management system is in place.
2. The system includes a countrywide Security Management Plan (SMP) (format in Gus Security Management Formats) that applies to everyone in country. The creation and maintenance of the SMP is a consultative, participatory and collaborative effort to ensure ownership and compliance. The SMP must be reviewed every year or more frequently if the security context changes significantly.
3. The process for the establishment and review of the SMP consists of the minimum following steps: consultation, drafting, formal feedback, approval, dissemination and communication.

   The most recent approved version must be posted on Sumas. After presentation of the final draft, Implementing Affiliates (IA) are given a reasonable period to provide feedback. The non-provision of feedback within the stated timeframe implies approval. Approval is given by the CLT, and subject to the MAs approval mechanism. The above process should be clearly documented in the CLT minutes.
4. As part of the SMP, the ED is also responsible for ensuring the development of security levels according to the agreed five levels system (format in Gus Security Management Formats). Although the security levels headings are fixed, the indicators and actions must be made context and risk specific. A security levels document must also be developed for field offices, which is specific to that particular context, and is approved by the ED.
5. Where possible the ED consults in order to set the appropriate security level. However, the ED has the express right to set the security level including the evacuation of staff for all offices. The decision is binding on all Affiliates and they must comply.
6. Lowering the security level is subject to the MAs mechanism as described in their security policy.
7. The right of Affiliates to withdraw from locations because of insecurity, prior to such a decision by the ED, is supported by all Affiliates.
8. Certain tasks may be delegated to an IA for practical reasons, but the responsibility cannot be delegated.
9. If field offices exist, location specific plans must be developed and maintained by the appropriate Affiliate. The ED ensures quality and consistency with the overarching SMP.
10. Each Affiliate is responsible for staff that they manage and is responsible for ensuring that staff and visitors comply with the security management system.
11. Affiliates share responsibility to feed into the security management system, including joint context analysis, risk assessment and risk mitigation measures.
12. Non-present Affiliates, wishing to visit a country, must have authorization from the MA, and must abide by the authority of the MA and the SMP.
13. Affiliates must meet the minimum standards outlined in this document. Where Affiliates global security policy imposes other standards on specific issues, these may be met in addition to the minimum standards.
14. The ED is held accountable by their line manager, and the Programme Governance Group (PGG), and has the right and duty to report any concerns about the functioning of security management to the PGG chair.
15. Should Affiliates disagree about security management issues they take their concerns to their line management, who will deal with them bilaterally or take the concerns to the PGG.
16. If issues cannot be resolved by the PGG, they should be escalated to the PDG.

17. Despite the process outlined above; urgent decisions, such as described in point 5, may be taken by the ED and are binding. Escalation to PGG, PDG or bilateral line management may take place simultaneously, but the urgent decision is binding and applied immediately.

**How to meet agreements**

1. Context analysis and risk assessment must be undertaken jointly, and must be a collaborative, consultative effort.
2. The choice of security approaches (for example, acceptance, deterrence and protection) is based on joint context analysis and risk assessment.
3. Roles and responsibilities for security management must be defined and assigned to named individuals. A clear explanation of the relationship between the PGG, CD, and PD's must be documented in the SMP.
4. Information is shared between Affiliates, and mechanisms to do so are institutionalized. The ED ensures that information is gathered from, and shared with, other actors (such as NGO`s, INGOs, UN, partners, local authorities and other stakeholders) and is crosschecked and analyzed.
5. The security levels chapter of the SMP is developed in detail, including program specific indicators and relevant actions to take at each level. Specifically this will include definition of essential and non- essential staff.
6. The ED oversees security learning and development needs, and coordinates efforts to provide joint training initiatives.
7. Resources for managing security, including provision for learning and development, should be budgeted for.
8. The ED is responsible for ensuring the development of a current, agreed Welcome Pack (format in Gus Security Management Formats).
9. Incident reporting and analysis – in addition to meeting line management reporting requirements; all security incidents must be shared with all Affiliates. (format in Gus Security Management Formats)
10. Each Affiliate is responsible for ensuring security briefings are conducted and for monitoring the security of all their staff and visitors. The ED should be notified of all visitors and new staff.
11. Partners are responsible for managing their own security. Affiliates need to ensure that staff and partners are clear about their specific roles and responsibilities regarding security management.

## Annex C: Security Levels

| | Indicators | Actions |
|---|---|---|
| 1 | Normal:<br>Situation calm<br>Low level of crime | All staff aware of current security management plan General precautions against crime<br>Emergency supplies in place (see evacuation plan) Evacuation plan in place |
| 2 | Precautionary: Situation less stable, higher risk of sporadic violence, possible threats against staff High level of crime<br>Increased military presence<br>Increased demonstrations | Contingency plans updated, staff aware of hibernation and evacuation sites<br>Emergency supplies checked Higher<br>security awareness by staff |

| | | |
|---|---|---|
| 3 | Restricted Movement/Restricted Programme: Increase in tension Increased demonstrations, with violence and anarchy Indications that military/belligerents are mobilizing Threats/demonstrations directed at national organizations Violence in project areas | Security updates every 2 days<br>Staff movements restricted<br>Programme activities may be partially suspended<br>Hibernation/evacuation points agreed with other NGOs<br>Curfew<br>All incidents reported immediately<br>No additional staff to travel into the Eligible<br>dependents may be evacuated |
| 4 | Partial Evacuation/Hibernation: Increased tensions and violence, including in locations near offices Increased violence in project areas Harassment/violence directed at national organizations Lootings Security forces unable to maintain law and order | Security updates daily/or more often<br>Essential/low risk staff only to report to work<br>Initiate evacuation/hibernation plan<br>High-risk &/or non-essentialnationalstaffto evacuate<br>Daily contact with line management Programme<br>activities likely to be suspended |
| 5 | Office Closure and Suspension of activities: Unacceptable level of risk Direct threats/attacks on national organizations/staff and or property Inability to continue programmes Large-scale mobilization of belligerents Indiscriminate violence, looting and destruction | Closure of office. See evacuation Plan<br>Closure of all programme activities |

## Annex D: Security Management Plan Template

Front page: title, date, author and review date
Chapters:

1. Introduction: purpose and scope of the document and its relation to other documents. First principles such as right to withdraw, duty to contribute to security etc.
2. Context Analysis (summary)
3. Internal Analysis. An overview of the joint Gus program, including partner activities.
4. External Analysis. General analysis (history, gender, religion, culture, infrastructure, demographics etc) conflict analysis, crime analysis, actor mapping, incident mapping.
5. Risk Assessment; threat identification and analysis, vulnerability analysis, threshold of acceptable risk.
6. Security approaches: the balance between acceptance, protection and deterrence and an explanation of implementation methodology.
7. Roles and responsibilities.
8. Standard Operating Procedures (may include vehicle and travel, communications, personal behavior, conflict survival, site protection etc).
9. Contingency Plans (may include hostage taking, sexual assault, gunfire, carjacking etc).

10. Evacuation Plan.
11. Incident reporting and analysis. (Definition of security incident, reporting structure, explanation of how lessons will be learned).
12. Security levels: built on the generic system of levels (section 4 of the security policy), a context specific overview describing the security levels, and related indicators and actions.
13. Annexes (contact numbers, maps, medical evacuation procedures, etc).

## Annex E: Crisis Management Plan Template

Front page: title, date, author and review date

1. Introduction
2. What Constitutes a Crisis?
3. Management and Decision Making
4. Crisis Management Team (CMT)
    a. Immediate Actions of Crisis Director
    b. Immediate Actions of CMT
    c. In the Event of an Abduction
    d. Individual CMT Member Actions
5. Incidents Involving Gus Affiliates or Other Agencies
    a. Gus Affiliates
    b. Other Organizations
    c. Partners or Community Volunteers
6. Human Resources
7. Family Liaison
    a. Delivering the Bad News Message
    b. Family Liaison Contact
8. Communication
    a. Media Communications
    b. Internal Communications
9. Information Management
10. Emergency Operations Room (EOR)
11. Post Crisis

| | | |
|---|---|---|
| 3 | Restricted Movement/Restricted Programme: Increase in tension<br>Increased demonstrations, with violence and anarchy<br>Indications that military/belligerents are mobilizing<br>Threats/demonstrations directed at national organizations<br>Violence in project areas | Security updates every 2 days<br>Staff movements restricted<br>Programme activities may be partially suspended<br>Hibernation/evacuation points agreed with other NGOs<br>Curfew<br>All incidents reported immediately<br>No additional staff to travel into the Eligible dependents may be evacuated |

| | | |
|---|---|---|
| 4 | Partial Evacuation/Hibernation: Increased tensions and violence, including in locations near offices Increased violence in project areas Harassment/violence directed at national organizations Lootings Security forces unable to maintain law and order | Security updates daily/or more often<br>Essential/low risk staff only to report to work<br>Initiate evacuation/hibernation plan High-risk &/or non-essential national staff to evacuate<br>Daily contact with line management Programme activities likely to be suspended |
| 5 | Office Closure and Suspension of activities: Unacceptable level of risk Direct threats/attacks on national organizations/staff and or property Inability to continue programmes Large-scale mobilization of belligerents Indiscriminate violence, looting and destruction | Closure of office. See evacuation Plan<br>Closure of all programme activities |

## Annex D: Security Management Plan Template

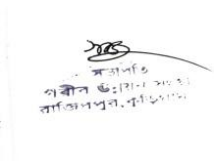
Front page: title, date, author and review date
Chapters:

14. Introduction: purpose and scope of the document and its relation to other documents. First principles such as right to withdraw, duty to contribute to security etc.

15. Context Analysis (summary)

16. Internal Analysis. An overview of the joint Gus program, including partner activities.

External Analysis. General analysis (history, gender, religion, culture, infrastructure, demographics etc) conflict analysis, crime analysis, actor mapping, incident mapping. Analysis and Lessons Learn



Md. Abdul Latif
Executive Director
Garib Unnayan Sangstha (GUS)

Md. Sajedul Islam
Chair person- Board of Trustee
Garib Unnayan Sangstha (GUS).