SAFETY AND SECURITY POLICY – AIPP

Endorsed by Executive Council in July 2022, subject to be adopted by General Assembly (GA)

Asia Indigenous Peoples Pact (AIPP)
Chiang Mai, Thailand

INDEX

BASIC GLOSSARY

Duty of care: the legal and moral obligation of an organization to take all possible measures to reduce the risk of harm to those who work for an organization or are operating on its behalf.

Security: freedom from risk or harm resulting from violence or other intentional acts.

Safety: freedom from risk or harm because of unintentional acts (accidents, natural phenomena, illness).

Threat: declaration or indication of an intention to inflict damage, punish or hurt (recent or immediate)

Vulnerability: any factor which makes it more likely for harm to materialize or result in greater damage

Risk: refers to the possibility of events, however uncertain, that will result in harm.

Capacities: are the strengths and resources to mitigate the risk and improve the security.

Acceptance: generation of a safe operating environment through the consent, approval and cooperation of individuals, communities, and local authorities.

Deterrence: risk reduction by containing the threat with a counter threat (eg, armed protection, diplomatic political or media pressure).

Protection: risk reduction by reducing the vulnerability of the organization (eg, fences, guards, walls).

Safety and Security Committee: Support the development of the organization's security risk management framework and ensure there are agreed policies and guidelines in place. Provide advice to the management line if required.

IPHRDs (Indigenous Peoples Human Rights Defenders) - Refers to individuals, Indigenous Persons Women Human Rights Defenders, Youths, Person with Disabilities, and other intersectional groups, groups and associations working to protect their lands, environment and human rights and the fundamental freedoms of peoples and individuals.

1.- PURPOSE AND SCOPE OF THE POLICY

The Asia Indigenous Peoples Pact (AIPP) is an independent organization committed to promote and work for the respect, recognition and protection of human rights, particularly indigenous peoples' rights, environment protection, social justice, peace, and democracy.

Indigenous Peoples Human Rights Defenders (IPHRD) face serious risks all over the world for their work to protect their communities, peoples and environment. Due to the nature of their work, they often become targets of actors who seek to discourage, discredit and disrupt their activities

This Policy defines the reference framework for the implementation of the safety and security management for AIPP members, network and partners related to the work of IPHRD in actions for the protection or defense of human rights, which may include civil and political rights, collective rights, transparency, anti-corruption, environmental rights, economic, social and cultural rights.

Its ultimate purpose is to allow operations in all contexts in which it works, including the most dangerous, and to minimize disturbances derived from security incidents through the establishment of common standards and tools in accordance with the identity of the organization and its strategic orientation.

Given how sensitive this area of management is, the approval and modification of the policy is responsibility of the General Assembly (GA) and the final validation will require the involvement of the highest decision-making levels, including the Executive Council.

This policy aims to:

(i) Minimize the risks for the members, communities, material, goods, assets, and activities of the organizations to acceptable levels.

(ii) Establish incident management mechanisms in the event they occur, to minimize the consequences of such incidents

(iii) Guarantee continuous reflection on this issue at the institutional level, so that it translates into the improvement of the proposed mechanisms based on context changes and the occurrence of incidents

To achieve these objectives, the security policy:

- Defines the specific functions of the members of the organization in matters of security management, decision levels and responsibility
- Establishes the principles that govern security management in the organization in relation to its vision, mission, and values
- Defines a common procedure for security and safety management valid for each member.
- Establishes principles of action for specific situations
- Defines the requirements at the organizational level for security management to be effective.

This policy, as a reference framework, applies to all AIPP networks, members and partners and its organs including consultants, volunteers, and field trainees.

It does not concern the partner organizations that will be governed by their own security policies and protocols, although the coherence of the latter with this policy will be a criterion to take into account when being selected as AIPP partners.

2.- SAFETY AND SECURITY PRINCIPLES

Indigenous Peoples' Human Rights Defenders in Asia are taking legitimate actions to protect the rights of individuals and their Collective rights as well as the environment. Security and Security take on particular importance since they continue to suffer attacks at the hands of both State and non-State actors, which impact upon their physical, digital, and psychological integrity and often further affect their friends and families and communities. Therefore, the protection of personnel is of utmost importance to the organization and teams to avoid undue risks in meeting the Organization vision, mission, and goals

- **Informed Consent -** IPHRDs must be aware that they are potentially exposed to risks and provide them tools to prevent them and have effective mechanisms to manage possible incidents
- **Shared responsibility** - managing and reducing the risks to staff is a shared responsibility involving all levels within the organization.
- **Acknowledgement of risk** - managing security will not remove all the risks. Individual IPHRD need to appreciate that they are still exposed to risk.
- **Primacy of life** - IPHRD safety is of the highest importance to the organization, IPHRD should never place themselves at excessive risk to meet programs objectives or protect property.
- **Proportionate risk** - the risk to IPHRD must be constantly assessed and should be proportionate to the need for, and benefits of, certain activities, and to the ability of the organization to manage these risks.
- **Equitable security** - some IPHRDs may be more vulnerable to certain threats than their colleagues. These individuals must be informed of the risks, but security restrictions/measures should not discriminate against individuals based on their personal characteristics.
- **Right to withdraw** - all IPHRDs should have the right to withdraw from or refuse to take up work in a particular area due to security concerns.
- **No right to remain** - the organization has the right to suspend activities or withdraw staff from situations that it considers to be too dangerous.

All IPHRDs must be advocated about the organization's vision, mission, and values and to act in accordance with the fundamental principles that the organization upholds.

To comply with the mandate, it is necessary to equip the defenders with mechanisms and tools that not only facilitate the fulfillment of its objectives, but also protect them from any situation that implies a threat to themselves, to the individuals and their communities with whom and for whom they work.

- **Security strategy**

The security strategy is based on the organization's approach to mitigating risks. AIPP will adopt mainly as a default security strategy for the risk reduction the Acceptance. Its objective is to provide a good understanding to external stakeholders of the organization’s mandate and objectives, to promote and ensure mutual understanding and respect between the organization, defenders, networks, partners and members. and thus, reduce our exposure to potential risks.

In any case, security management must adequately combine acceptance, protection, and deterrence strategies, based on the results of the threat and vulnerability analysis.

3.- ROLES AND RESPONSIBILITIES

Managing risks to IPHRDs is a shared responsibility. Embedding good security risk management requires clearly defined roles and responsibilities, and structures that have sufficient capacity to provide and maintain effective support.

The AIPP Safety and Security Committee[1] is ultimately responsible for security management.

- Supervises the content of the policy and the guidelines
- Supports managers in implementing and monitoring the security risk management framework.
- Support in any decision related with the response to incidents

The Responsible of each organization:

- Ensures the implementation of the Security and Safety Policy and Guidelines or any other protocol or plan necessary in the geographical area under its responsibility.
- Is responsible for analyzing the context, defining the specific local risks, and establishing the response measures and the necessary means with the support of the AIPP Security Committee.

Every IPHRD is responsible for complying with all security policies and guidelines.

- Will be asked to accept the security risks related to the activities as a personal responsibility, therefore, they should be informed.
- Will report all security incidents appropriately.
- Will know and respect Organization´s Codes of Conduct as an integral part of this Security and Safety Plan.
- Must know and consider the social, cultural, economic, and political characteristics of the context in which they work and ensure their behavior does not increase risk to themselves and/or others

4.- SECURITY AND SAFETY MANAGEMENT

The security management in AIPP is defined in the "Security and Safety Guidelines" and will be adapted into a security and safety plan for each AIPP member country, based on a regular context monitoring and risk assessment.

Security management cannot be standard, but must be based on a prior analysis that results in the following phases:

• Identification of threats present in the context and the organization's vulnerabilities to those threats. Therefore, risk is defined as the exposure of the organization (personnel, premises, operations, including beneficiaries) to these threats.

• Risk analysis and assessment (Risk level = probability x impact / capabilities) and choice of security strategy.

• Implementation of mitigation measures: such as rules and procedures, equipment, training, and awareness.

• Acceptance of residual risk as the last stage to analyze the extent to which the organization is still

[1] Attached in Annex 1, Terms and References for AIPP Safety and Security Committee

exposed to a certain risk once mitigation measures have been implemented.

The frequency with which the risk analysis must be updated is defined in the security plans, but at a minimum it is recommended that it be reviewed once a year. In any case, in addition to scheduled updates, a significant change in context or the appearance of a new threat should prompt a review of the risk analysis.

It is recommended that all AIPP networks, members, and partners, have a Security Plan that includes context analysis, risk assessment, mitigation measures and contingency plans.

5.- MONITORING OF INCIDENTS. CRITICAL INCIDENT MANAGEMENT

IPHRDs should regularly report and monitor incidents to determine where and how security situations are changing, why contexts are changing, and what these changes mean for staff safety. It is important to maintain an agile system to monitor incidents that will help other colleagues avoid similar incidents and react appropriately to changes in the operating environment.

Incident reporting procedures should define which incidents have to be reported, to whom and through what mechanisms.

A security incident is any situation or event that has caused or that may cause damage to personnel; associated employees; third parties; a significant change in programs/activities, or considerable damage/loss to the reputation of the organization.

Attempts should also be reported as these are a useful record and can be used to inform people about potentially harmful incidents, manage incidents more effectively (e.g., through effective communications such as warnings) and to help people understand changes in the safety and security environment.

In the case of an incident, the responsibility for security management rests with the safety and security committee. However, in the event of an incident that involves serious threats to the organization, in addition to operations and / or individuals, the responsibility rises to the Responsible of each organization

In the case of Critical Incidents (kidnapping, disappearance, or death). The AIPP Security Committee must have defined a Crisis Management Team (CMT) and specific procedures that detail how to handle all types of critical incidents that pose a level of threat such that the defined management line does not have full capacity to deal with.

6.- REFERENCE DOCUMENTS

The application of this policy should be in line with the following sources:

The international legislative framework

- Universal Declaration of Human Rights

The national legislative framework

- protection laws for human rights defenders in each of the countries

AIPP internal documents:

- AIPP Gender Policy - Sept 2016
- AIPP Finance-Manual - Feb 2020
- AIPP Anti-Corruption Policy -Nov 2006
- AIPP Security Guidelines –