

**SAFETY & SECURITY MANAGEMENT PLAN**

**Updated by:**

Safety and Security:

Date:

**Approved by:**

Leadership:

Date:

*This Safety & Security Management Plan template provides a framework that has been developed by humanitarian safety and security professionals. Significant elements of humanitarian safety and security management remain outside the control of* ***the Forum*** *or any individual staff member, and, accordingly, adherence to this Safety & Security Management Plan cannot guarantee that no harm will be suffered.* ***The Forum and*** *its affiliated entities have no responsibility or liability for the use of this SSMP template.*

***\*For internal distribution only\****

1. **INTRODUCTION**

**Purpose of the Plan**

This Safety and Security Management Plan (SSMP) is designed to maximize staff safety and security and minimize risks to *(insert agency)* staff, assets, and reputation within the context of *(insert agency)* areas of operation. Safety and security can only be realized when staff are aware of the threats in their context, take steps to mitigate them, and know how to respond appropriately. Safety and security in the Resettlement Agency (RA) and affiliate context is designed to mitigate risk in support of program delivery. Ultimately, this means a client centered approach to all we do. To this end, the core values of the social work profession are listed below.

**National Association of Social Workers (NASW)**

The mission of the social work profession is rooted in a set of core values. These core values, embraced by social workers throughout the profession’s history, are the foundation of social work’s unique purpose and perspective:

* Service
* Social justice
* Dignity and worth of the person
* Importance of human relationships
* Integrity
* Competence

This constellation of core values reflects what is unique to the social work profession. Core values, and the principles that flow from them, must be balanced within the context and complexity of the human experience.

**Scope of the Plan**

The SSMP is intended for use by all *(insert agency)* staff.

**Distribution of Copies**

All *(insert agency)* staff should be aware of the existence of the SSMP and its contents. Staff should be informed by their supervisors about relevant parts of the plan that will affect their daily work. They should also be kept informed of any changes to the plan, including any changes to security phases.

All leadership and safety and security personnel should keep a copy of the plan and laminated copies should be available for easy access by staff. When the plan is updated, it will be redistributed to staff.

**Decision-Making Process (May Vary by Agency)**

The *(insert leadership title)* is ultimately responsible for all aspects of safety and security management at all *(insert agency’s)* domestic locations. Thus, the *(insert leadership title)* will have ultimate authority regarding safety and security management. The *(insert leadership title)* will ensure that at all domestic locations have:

* An effective safety and security management system in line with *(insert agency)* safety and security management policy and standards is established and maintained.
* Appropriate Security Risk Analysis (SRA) is done as warranted by the context in to determine the appropriate security threat levels.
* Adequate budget provisions are made for safety and security management.

**The structure of the decision-making process related to security is:**

* Safety and security oversees SRAs according to *(insert agency)* standard practices to determine threat levels and makes recommendations to the *(insert leadership title)* for consequent actions.
* If the *(insert leadership title)* is absent, their deputy will assume the safety/security responsibilities of the *(insert leadership title).* If both the *(insert leadership title)* and their deputy are absent, operations leadership will assume policy related safety and security related responsibilities.
* All staff members have a responsibility for safety and security and should quickly communicate any security-related information to the safety and security team, the program lead/their supervisor.
* If a safety/security crisis arises when the *(insert leadership title)* is not available, the deputy or or operations lead, together with safety and security, are responsible for deciding any change in threat level, and coordinating response(s) as the situation requires.
* In terms of security crises, the program lead will report via safety and security and the *(insert leadership title)* will assume control if required by the crisis.

**Review**

This SSMP will be reviewed at least bi-annually and updated based on any changes in the operating environment. This is because security planning is a continuous process and threats in the operational environment may change over time. The plan should also be reviewed after any major event affecting the security situation faced by *(insert agency)* staff or operations.

**Use of the Plan**

This SSMP should be read in conjunction with current security documents to gain an accurate picture of the evolving security situation. This plan is one part of a broader security management system that includes ongoing internal review by the Senior Management Team (SMT), safety & security staff and focal points, and external communications with RA and affiliate partners.

**The SSMP shall be shared with all *(insert agency)* staff, who are required to abide by the policies and procedures as set forth herein and to sign the acknowledgement of understanding document, which is attached.**

1. **SITUATIONAL AWARENESS**

Situational awareness is crucial for the early identification of threats and the sound development of responses.

**The (Insert Agency) Mission**

The agency has *(insert number)* of staff. The agency is based in *(insert location).* There are *(insert number)* of facilities. Key partners include *(insert partners).*

*(Insert agency)* currently implements *(insert program)* activities in the following geographic area *(Insert geographic areas).* *(Describe scope of programs).*

**Context Analysis – (insert location)**

*(Insert agency)* currently implements directly in areas of *(insert location).*

Sound safety and security management planning starts with robust context analysis. To that end, please describe the threat environment within which your staff, assets, reputation, and clients during the delivery of services face potential harm.

In order to conduct the context analysis, consider using a combination of open source, as well as primary and secondary research.

**Threat Assessment**

The threats within the *(insert agency)* area of operations vary. Threats may differ based on geographic location, local program operations, and the parameters of deliverables**.**

The points below are potential threats.

(List Potential Threats)

* (Example) Field visits – When operating in the field, staff may come across clients who become escalated. Other areas of concern can include criminality, an unfamiliar environment, and a lack of preparedness.

* (Example) Transporting clients – When transporting clients, staff may not have a properly functioning vehicle, necessary supplies, may be transporting at night, and may not be familiar with the client or area they are traveling.

1. **SECURITY THREAT RATINGS**

The *(insert agency)* Safety & Security Threat rating system is used to rate threats from various categories according to their likelihood of occurrence and their likely impact on *(insert agency)* staff programs, assets, and clients during program delivery. They are ranked on a scale of 1 to 5 where 1 or 2 (Green) signifies a low threat to *(insert agency)* staff, programs, assets, and clients during program delivery, while 4 or 5 (Orange or Red) signifies a high threat. The definitions of the five color-coded levels of the Threat Rating system are detailed below. Higher threat ratings warrant higher levels of staff and organizational preparedness and response.

**Threat Rating Scale**

|  |  |
| --- | --- |
| **THREAT** | **DEFINITION** |
| **VERY LOW = 1** | Rare or limited threat occurrence. Minimal effect on staff, programs, assets, or reputation. Very small or no probability. Frequency may range from once every 5 to 10 years**.** |
| **LOW = 2** | Threat occasionally occurs. Little effect on staff, programs, assets, or reputation with minor operational disruptions. Small probability. Frequency may range from once every 6 months to a year. |
| **MEDIUM = 3** | Occasionally, multiple threats occur. Poses modest threat to staff, programs, assets, reputation, or operations but disruptions are temporary and manageable. Frequency may range from once every month to 3 months. |
| **HIGH = 4** | Frequent multiple threats occur. Poses frequent but contained threat to staff, programs, assets, or reputation causing some interruptions to operations. Frequency may range from weekly to twice a month. |
| **VERY HIGH = 5** | Continuous multiple threats. Poses constant and severe threat to staff, programs, assets, or reputation causing frequent interruptions or suspensions of operations. Frequency may range from twice a week to daily. |

**Alert Levels**

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat Level** | **General Indicators** | **Security Management Responses** | **Individual Actions** |
| **Level 1 (Normal)** | -Secure situation within the area.  -No outward signs of significant social disruption or instability.  -Crime is within normal limits.  -Free and unrestricted movement of staff always.  -No observable threat to *(insert agency)*  -Program activities continuing as normal. | -Develop and maintain strong relations with individuals, community leaders, and law enforcement.  - Maintain liaison with other agencies.  -Apply standard operating procedures.  -Maintain emergency personnel files for all staff. | -Each individual staff member is responsible for their own security, safety, and health.  -All staff should proactively monitor the security situation and report any incidents or concerns to their line manager.  -All staff must carry their photo ID card. |
| **Level 2 (Tense)** | -Significant political, economic, and social unrest is present.  -High crime.  -Some restrictions on the movement of staff in certain locations.  -Program activities carrying on as normal but with a need for extra care and diligence. | -Notify all staff of the increased security level.  -Establish regular staff security meetings.  -Ensure all staff movements are monitored, and all field travel is limited to daylight hours.  -Review and reinforce security measures and procedures.  -Consider establishing guards at *(insert agency)* offices. | -All staff should avoid traveling alone, especially at night.  -All staff should routinely communicate their movement plans, or any changes, to their supervisor/colleagues. |
| **Level 3 (Insecure)** | -Substantial deterioration in the security situation.  -General lawlessness, incidents of rioting or looting reported.  -Staff movement and presence in particular areas, or at times, is restricted.  -Program activities restricted. | -Ensure staff is briefed weekly on security developments and incidents  -Ensure all staff movements are strictly monitored, including time of departure, estimated time of arrival and persons traveling.  -Ensure all travel to the field is authorized by *(insert agency)* leadership.  -Ensure regular secure back-up of computer files. | -All staff should maintain regular contact with the office. |
| **Level 4 (Dangerous)** | -Violence against staff and indiscriminate violence e.g protests.  - Credible threat against NGOs/social workers.  -All staff movements are restricted.  -Program activities restricted to essential activities or suspended. | -Consult with leadership regarding suspension of activities.  -Ensure staff are updated on the security situation (daily). | -All staff should await further instruction.  -All travel and movements must be authorized by leadership. |
| **Level 5 (Untenable)))** | **-**Security deteriorated to such an extent that it is considered unsafe, or impossible, to operate. Active threat.  -No movement of staff at any time.  -Program activities suspended | **-**Suspend all program activities and close offices.  -Maintain constant contact with leadership. | -No movement. |

1. **SAFETY & SECURITY POLICIES**

This section outlines the safety and security policies and procedures that are to be adopted.

**Compliance with *(insert agency)* Safety and Security Management Policy and Standards**

*(Insert agency’s)* Safety and Security Management Policy and Standards have been created to minimize safety and security risks to all staff while maximizing the impact of *(insert agency’s)* programs. Staff should familiarize themselves with *(insert agency’s)* safety and security policy and standards and adhere to them. The Safety and Security Management Policy and Standards can be found on *(insert location).*

***(Insert agency),* Safety & Security Policy Statement**

*(Insert existing policy, sample below if necessary)*

*(Insert agency)* is committed to minimizing safety and security risks to staff and ensuring staff are given training, support and information to reduce their risk exposure while maximizing the impact of program deliverables. *(Insert agency)* seeks to provide safe and healthy working conditions for all staff, mindful that each individual staff member also has responsibility for achieving this.

**Acceptance as Security Management**

Acceptance is the cornerstone of effective security management in the RA and affiliate program delivery contexts. *(Insert agency)* recognizes that staff safety and security is, to a great extent, best assured when *(insert agency)* and staff are well integrated into the local community and valued for their contributions to the social welfare of immigrants and refugees. Therefore, *(insert agency*) will always strive to build and maintain acceptance from local authorities, partner agencies, communities and other stakeholders for its presence and the work the organization performs*. (Insert agency’s)* overall approach, program design and behavior of staff will be based on the acceptance approach and principles of transparency, accountability, respect, and participation.

**Staff Roles and Responsibilities**

* Safety & security is everyone’s job: staff will actively participate in and contribute to maintenance of safety and security measures, awareness of security risks, team security, and coordination with partners.
* *(Insert agency)* staff will always strive to maintain vigilance regarding changes to the operational environment that might increase their organization’s exposure to threats.
* All (Insert agency) staff are responsible for the impact their actions have on the safety and security of their fellow staff, and for (Insert agency) programs, reputation and assets under their management and care; and will, when possible, reasonably support the safety and security of clients during the delivery of services.
* All *(insert agency)* staff should exercise common sense to ensure their own safety and security.
* All staff are responsible for reporting any safety and security incident or near-miss incident to safety and security/their supervisor as soon as possible.
* All *(insert agency)* staff will have access and orient themselves to the safety and security policy, standards, procedures and supporting tools and guidelines. These will be included in the initial orientation and briefings for all staff and a signed acknowledgement will be kept by Human Resources.
* Failure to follow the policy, procedures and standards may increase the risk of harm to staff, *(insert agency)* assets; and may reduce acceptance of *(insert agency)* by partner organizations, communities, and beneficiaries.
* All *(insert agency)* staff must comply with *(insert agency)* safety and security policy and standards. Failure to comply, including failure to report breaches of this policy, standards and procedures may result in disciplinary action up to and including dismissal and/or cancellation of the contract.
* *(Insert agency)* staff have the right to decline to undertake a field visit, activity, or travel without suffering disciplinary action if they feel the risk to their personal security is unacceptable, except for when instructions are given for the purpose of avoiding a dangerous situation and reducing risk.

***(Insert agency)* Safety and Security Management Standards**

* Standard 1: An effective communications plan is established and functioning communications equipment for all administrative offices and service delivery sites is maintained.
* Standard 2: Effective safety and security management systems are in place, enabling programs and ensuring access to vulnerable populations while mitigating safety and security risks.
* Standard 3: An SSMP with appropriate contingency plans are developed and maintained, with contingency plans being practiced annually.
* Standard 4: All facilities are managed and equipped to operate safely and securely.
* Standard 5: All staff received safety and security training, orientations, briefings appropriate to their roles and as determined by the assessed risks in the operational environment.
* Standard 6: All safety and security incidents are reported to the designated safety and security personnel/supervisor in a timely manner (not exceeding 24 hours) and follow-up actions are carried out in accordance with the relevant procedures.
* Standard 7: Effective crisis management systems are in place to respond to any critical event in accordance with *(insert agency)* crisis management policies, procedures and templates.

***(Insert agency)* Staff Safety and Security Training Requirements & Resources**

**Recommended Trainings:**

All staff must complete the Resettlement Agency Safety & Security Focal Point Forum (RA SSFP “The Forum”) webinars. These trainings include: active threat response, trauma informed de-escalation, safety & security basics/situational awareness, setting boundaries with clients, physical site security, and offsite safety and security. Webinars that are relevant to key Standard Operating Procedures (as defined by the threat environment) and contingency plans are also recommended. Yearly crisis management planning and training with leadership is also recommended.

**Fire & Electrical Safety**

Basic incident response and reporting procedures are explained to all staff. There must be occasional unannounced fire drills which will test emergency evacuation procedures. Fire extinguisher training is recommended.

**Disaster Preparedness**

An overview of the office procedures for specific events/incidents is in the Emergency Preparedness/Response Plan. These procedures are explained to all staff during induction and reiterated dependent upon the threat context.

**Information Sharing (internal, external, representation on safety and security fora)**

The SSFPs are responsible for gathering, reviewing and sharing safety and security information from various sources – including open source and verified news/media outlets.

**Facilities Description**

If necessary, one can use the provided checklist (**Annex 1**) to conduct a basic security inspection. For more detailed inspections, it is recommended to utilize a licensed vendor or professional.

**Facilities safety procedures (fire safety, exit drills, first aid kits, etc.)**

**Preventive measures concerning fire**

* All premises should have working fire extinguishers.
* All offices should have an appropriate fire alarm system (verbal or air horn).
* Exit drills are conducted at least twice a year.

**Fire: Prevention and general information**

* Fire prevention is everyone’s responsibility. *(Insert agency)* has a no smoking policy in offices and vehicles worldwide.
* Smoke detectors should be fitted in all offices.
* Each staff member is responsible for knowing the fire escape routes/exits closest to her/his office and residence. These exits should be marked and clear of debris.
* Each office is to hold a fire drill practice on a quarterly basis and report when completed.

**Field Visits**

Field movement procedures can be found in the SOPs. Staff are required to abide by authorization, safety, and movement tracking procedures without exception.

**Communications: Telephone**

* The internet is used as a primary means of communication with emails and Skype being quick and effective.
* Mobile phones are also used as a primary means of communication.
* What’s app is also used for creating groups for emergency communication.

**Incident Reporting and Response**

Every member of *(insert agency)* is obliged to report any security-related incident. While some incidents may seem insignificant, analysis of ongoing patterns and trends can only be accomplished when every incident is reported promptly, and complete information is provided to safety and security.

**What is a reportable incident?**

A reportable incident is defined as any event, situation, or occurrence that causes, or has the potential to cause harm to staff, assets, reputation, or clients during the delivery of services. Reportable incidents include, but are not limited to:

* All vehicle accidents (even minor ones)
* Physical or sexual harassment
* Attacks or assault, sexual assault, or attempted assault
* Theft or attempted theft of funds, goods, vehicles, or other assets
* Break-ins or burglary
* Credible threats of harm to staff or property or patterns of hostile acts, even if it seems minor. This should include foot or vehicular surveillance (being followed by an individual or a vehicle)
* Serious medical emergency or injury
* Death of staff
* Suspension of activities
* Temporary closure of office
* Incidents involving other agencies
* Negative media exposure

Every member of *(insert agency)* shall report anything that can be defined as an incident. Staff members should immediately report through the proper channels any incident involving serious medical emergency, injury, crime, or vehicle accident. If there is an imminent threat that poses life threatening circumstances, please do not hesitate to call 911. Written incident reports are to be prepared as soon as possible after the immediate verbal report. Reports should be made to safety and security within 24 hours of the incident. As soon as possible, safety and security will compile information on the incident to determine immediate actions and corrective measures required. Safety and security will submit all reports and recommended measures to the *(insert assigned decision maker).*

An incident should be reported in the following format:

* When did this happen?
* Where did this happen?
* What happened?
* Who is involved?
* How did it happen?
* Why did this happen?

Staff should provide regular updates as the situation changes. The information provided may save someone’s life.

A generic incident reporting form can be found in **Annex 2**

**Safety & Security**

Safety & security should be immediately notified of any ongoing incident.

Someone will compile information on the incident to determine whether immediate action and corrective measures are required, translate, and forward all reports and recommended measures to *(insert leadership title)* for review and approval. Upon approval, safety & security will disseminate warnings to all staff by the most effective means possible. These will be analyzed for completeness and relevance. Persons forwarding incomplete reports will be contacted by safety and security to obtain the missing information.

Incident reports will be analyzed by safety and security to determine:

* Trends and patterns
* Potential for escalation

For incidents reported after the fact, Safety & Security will brief the (Insert Agency Leadership) with analysis and suggested corrective measures. Staff briefings will be organized on control measures to be taken by the office, as deemed appropriate by the (Insert Agency Leadership).

Safety & Security maintains incident reports for a minimum of two years. Reports will be kept in a safe location with a special file designated for security issues. All incidents reported via (Insert Agency) online form will be held electronically.

**Weapons and firearms prohibitions on (Insert Agency) premises and in (Insert Agency) vehicles**

The presence of firearms, weapons of any type or armed personnel in any (Insert Agency) premises or vehicle is prohibited *unless there is an immediate threat to life, or the proper approval procedures have been followed* to allow protection of (Insert Agency) staff and property.

1. **CONTINGENCY PLANS**

**Vehicle Accidents**

The possibility of vehicle accidents can be limited by safe driving, but of course they cannot be avoided entirely. If staff are involved in an accident, it’s important to handle the situation correctly. If mishandled, it can quickly change from an unfortunate accident into a security risk. The following procedures should be followed to mitigate the effects of an accident.

* Assess the situation. Quickly discern the attitudes and behavior of people around the accident site to ensure that you are not at risk.
* Stop or not? Do not leave the scene of the accident unless your safety or that of your colleagues is jeopardized, and then only to move to the nearest police station or known safe location
* Aid if someone is injured, provide immediate care and assistance as appropriate.
* Report it. Contact your office and report the incident. If appropriate, contact the police immediately and cooperate as required.
* Do not discuss compensation! If issues regarding settlement to victims for death or injury, vehicle damage arise, get advice from senior management when approaching an accident involving other vehicles, consider the safety and security of the vehicle and occupants before responding.
* Remember insurance. Adhere to procedures required by the insurance company regarding vehicle accidents. If feasible, take photographs of the scene and record the names and contact information of those involved, witnesses, and responding authorities. In most cases Insurance will require a police report.

**Natural Disaster Response**

Fill in (Insert Agency’s) policy.

**Office Intrusion**

Fill in (Insert Agency’s) policy.

1. **ANNEX**

**Annex 1 (Security Inspection Checklist)**

**The Office Perimeter Score:**

**Narrative:**

|  |  |  |
| --- | --- | --- |
| **Infrastructure:** | **Yes / No / N/A** | **Description** |
| 1. Clearly defined property lines | ☐Yes ☐No ☐N/A |  |
| 1. Are there spots where someone can hide? | ☐Yes ☐No ☐N/A |  |
| 1. Adequate perimeter lights | ☐Yes ☐No ☐N/A |  |
| 1. Is there anything that can be climbed to gain access to the office? | ☐Yes ☐No ☐N/A |  |
| 1. Blind spots | ☐Yes ☐No ☐N/A |  |
| 1. Is the office located in a high crime area? | ☐Yes ☐No ☐N/A |  |
| 1. Is the area regularly patrolled by law enforcement? | ☐Yes ☐No ☐N/A |  |

**CCTV Score:**

**Narrative:**

|  |  |  |
| --- | --- | --- |
| **Infrastructure:** | **Yes / No / N/A** | **Description** |
| 1. CCTV System | ☐Yes ☐No ☐N/A |  |
| 1. Access to CCTV | ☐Yes ☐No ☐N/A |  |
| 1. Exterior CCTV Cameras | ☐Yes ☐No ☐N/A | # Of cameras: |
| 1. Interior (office) CCTV Cameras | ☐Yes ☐No ☐N/A | # Of cameras: |
| 1. Entrance (building) CCTV Cameras | ☐Yes ☐No ☐N/A | # Of cameras: |
| 1. Hallway CCTV Cameras | ☐Yes ☐No ☐N/A | # Of cameras: |
| 1. Trained CCTV user operated | ☐Yes ☐No ☐N/A |  |
| 1. CCTV Operator 24/7 | ☐Yes ☐No ☐N/A |  |
| 1. CCTV Operator equipped with alarm | ☐Yes ☐No ☐N/A |  |
| 1. Back up recording (7 days min) | ☐Yes ☐No ☐N/A |  |
| 1. Functioning in dark | ☐Yes ☐No ☐N/A |  |
| 1. Effective interlocking coverage (blind spots) | ☐Yes ☐No ☐N/A |  |

**Access Control Score:**

**Narrative:**

|  |  |  |
| --- | --- | --- |
| **Infrastructure:** | **Yes / No / N/A** | **Description** |
| **Exterior Access Control** |  |  |
| 1. Multiple entry/exit points | ☐Yes ☐No ☐N/A |  |
| 1. ID card access control | ☐Yes ☐No ☐N/A |  |
| 1. Escape door | ☐Yes ☐No ☐N/A |  |
| 1. Self-closing security doors | ☐Yes ☐No ☐N/A |  |
| 1. Do you have “deterring” signs such as firearm carry, search policy, property surveillance? | ☐Yes ☐No ☐N/A |  |
| 1. Professional guards at front desk | ☐Yes ☐No ☐N/A |  |
| 1. Adequate number of guards. | ☐Yes ☐No ☐N/A |  |
| 1. Are the guards armed? | ☐Yes ☐No ☐N/A |  |
| 1. Can you use the elevator without a fob or ID? | ☐Yes ☐No ☐N/A |  |
| 1. Do you have to sign in? | ☐Yes ☐No ☐N/A |  |
| 1. Are access points limited? | ☐Yes ☐No ☐N/A |  |
| 1. Is the main entry clearly identified? | ☐Yes ☐No ☐N/A |  |
| **Parking** |  |  |
| 1. Purpose built parking area | ☐Yes ☐No ☐N/A |  |
| 1. Can cars park near the building? | ☐Yes ☐No ☐N/A |  |
| 1. Is there heavy vehicle traffic? | ☐Yes ☐No ☐N/A |  |
| **Interior Access Control** |  |  |
| 1. Robust main door | ☐Yes ☐No ☐N/A |  |
| 1. Self-closing main door | ☐Yes ☐No ☐N/A |  |
| 1. Dedicated main reception | ☐Yes ☐No ☐N/A |  |
| 1. ID card access control | ☐Yes ☐No ☐N/A |  |
| 1. A separate waiting room for guests | ☐Yes ☐No ☐N/A |  |
| 1. Escape door | ☐Yes ☐No ☐N/A |  |
| 1. Segmented rooms | ☐Yes ☐No ☐N/A |  |
| 1. Neighbors on the same floor? | ☐Yes ☐No ☐N/A |  |

**The Office Building Superstructure Score:**

**Narrative:**

|  |  |  |
| --- | --- | --- |
| **Infrastructure:** | **Yes / No / N/A** | **Description** |
| **Infrastructure & Hazards** | | |
| 1. Hardened Structure | ☐Yes ☐No ☐N/A |  |
| 1. Noticeable building weak points | ☐Yes ☐No ☐N/A |  |
| 1. Glass exterior walls | ☐Yes ☐No ☐N/A |  |
| 1. Dedicated safe room | ☐Yes ☐No ☐N/A |  |
| 1. Elevators (w/posted inspection) | ☐Yes ☐No ☐N/A |  |
| 1. Emergency lighting system | ☐Yes ☐No ☐N/A |  |
| 1. Elevators (w/emergency phone) | ☐Yes ☐No ☐N/A |  |
| 1. Well-constructed stairwell(s) | ☐Yes ☐No ☐N/A |  |
| 1. Hardened safe/valuables area | ☐Yes ☐No ☐N/A |  |
| 1. Blast film (anti-shatter) | ☐Yes ☐No ☐N/A |  |
| 1. Security alarm system | ☐Yes ☐No ☐N/A |  |
| 1. Hallway clear | ☐Yes ☐No ☐N/A |  |
| 1. Escape routes | ☐Yes ☐No ☐N/A |  |

**Fire Safety & First Aid Score:**

**Narrative:**

|  |  |  |
| --- | --- | --- |
| **Infrastructure:** | **Yes / No / N/A** | **Description** |
| **Fire safety** |  |  |
| 1. Multiple fire exits (unobstructed) | ☐Yes ☐No ☐N/A |  |
| 1. Windows with fire escape | ☐Yes ☐No ☐N/A |  |
| 1. Emergency exits marked | ☐Yes ☐No ☐N/A |  |
| 1. Fire emergency plan posted | ☐Yes ☐No ☐N/A |  |
| 1. Adequate fire extinguishers | ☐Yes ☐No ☐N/A |  |
| 1. Fire alarms (audible/response) | ☐Yes ☐No ☐N/A |  |
| 1. Smoke detectors/alarms | ☐Yes ☐No ☐N/A |  |
| 1. Sprinkler system | ☐Yes ☐No ☐N/A |  |
| **First aid** |  |  |
| 1. First aid boxes present | ☐Yes ☐No ☐N/A |  |
| 1. First aid boxes a/ reception | ☐Yes ☐No ☐N/A |  |
| 1. First aid boxes a/ guard post | ☐Yes ☐No ☐N/A |  |
| 1. Auto-electric defibrillator | ☐Yes ☐No ☐N/A |  |
| 1. Emergency kit for natural hazards | ☐Yes ☐No ☐N/A |  |

**Annex 2 (Incident Reporting Form)**

**Incident Reporting Form**

Instructions: Please complete this form for all incidents and near misses that have implications on the safety or security of staff, associated personnel, assets, or operations. This form should be completed by a staff member involved in the incident, a relevant line manager, or the local Security Focal Point.

1. Who is reporting this incident? Please include your name and position title.
2. What is your contact information? Please include email and phone.
3. What date did the incident take place on?
4. At what time did this incident occur? Estimate if you do not know the precise time.
5. Where did the incident take place?
6. Were you or your staff directly involved in this incident?
7. Was a client affected during the delivery of services?
8. What was the specific nature of this incident?

* Violent Crime (e.g., assault)
* Political Rhetoric and Violence
* Gender Based (e.g., sexual harassment/sexual assault/rape)
* Property Crime (e.g., theft)
* Traffic Incident
* Protest or Riot
* Concerning or Threatening Communication
* Trespassing
* Fire and Natural Disasters
* Public Health (e.g., illness/mental health)
* Negative Interaction with Law Enforcement
* Other

1. If possible, please provide a summary of the incident.