# Safety and Security Incident Information Management (SIIM) for Staff

READY to go Mobile Guide

Learn how to report a safety and security incident to your organization.

## Security Incidents

## Safety and Security Incidents Can Happen Anywhere

Safety and security incidents can happen at any time and in any working environment. Relief and development professionals and volunteers operating in insecure settings and in emergency or crisis response are often at risk of experiencing a safety and security incident.

Incidents may involve accidents, threats, violence, or crime which can have lasting physical and emotional effects on everyone involved. Every organization has a duty of care obligation to protect, respond, and support their staff before, during, and after a safety and security incident.

# Why Should You Report an Incident?

It is critical for all staff to report safety and security incidents. Your organization can only act if they know about an incident. Reporting an incident will enable your organization to respond immediately, help reduce the impact of the incident, and take actions to prevent incidents from happening in the future. Even if the incident does not seem critical to you or does not directly affect your organization, reporting it could help inform key decisions about operations and programs in your organization.

**Reporting Incidents Helps You…**

- Process and understand what happened
- Receive support (additional medical care, counseling, legal action)
- Learn how to mitigate risks and make informed decisions regarding personal safety and security at work
- Learn how to prevent similar incidents from happening in the future
- Better understand security procedures and how to support other colleagues

**Reporting Incidents Helps Organizations…**

- Respond to the incident and provide immediate assistance to everyone involved
- Learn from the incident to better prevent, prepare for, and respond to future incidents
- Meet duty of care obligations by improving the safety and security of employees and others
- Understand the operational context to inform key decisions for security measures and improving access to communities
- Inform strategic decision-making for programming, safety and security, human resources, finance, and advocacy
- Identify and address underlying structural and systemic issues, discrimination, and/or bias that may have caused the incident or an employee to be a specific target
- Determine inclusive ways to improve the safety and security of diverse profiles of staff, taking into consideration how personal characteristics may make individuals vulnerable to different internal and external threats

# What is an Incident?

Each organization will have their own policy on what safety and security incidents need to be reported by staff and specific reporting procedures to follow. Consider the different aspects of an incident to help you report it and support your organization with learning from and responding to the reported incident.

### Defining an Incident

An incident can be an event in which:

- Employee safety or security was compromised
- A dependent or other third party was injured/harmed during organizational activities
- Organizational property or assets were stolen, damaged, or put at risk
- There was interference with programming and operations
- The organization's independent work was compromised
- The organization's reputation was put at risk or damaged

### Internal vs External

An incident can involve and/or affect…

- The organization
- Employees
- People outside the organization (partners, other NGO staff, community members, the public)

### Critical vs Non-critical

Incidents can be critical and non-critical:

- **Critical incident** = the organization's response requires using additional measures and resources beyond normal organizational procedures. Examples: kidnapping, death
- **Non-critical incident** = the organization's response uses normal organizational procedures. Example: road traffic accident with no injury or severe damage

## Impact

An incident can impact:

- The safety, security, and wellbeing of yourself, colleagues, and/or others
- Your organization's ability to:
  - Conduct operations
  - Deliver aid and services
  - Achieve its objectives

## Accident vs Intentional Act

An incident can be an accident or an intentional act:

- **Safety incident** = an accident
- **Security incident** = an event that was caused intentionally by a third party to inflict harm on an individual, the organization, or other actors, or to negatively impact the delivery of aid

## Classification

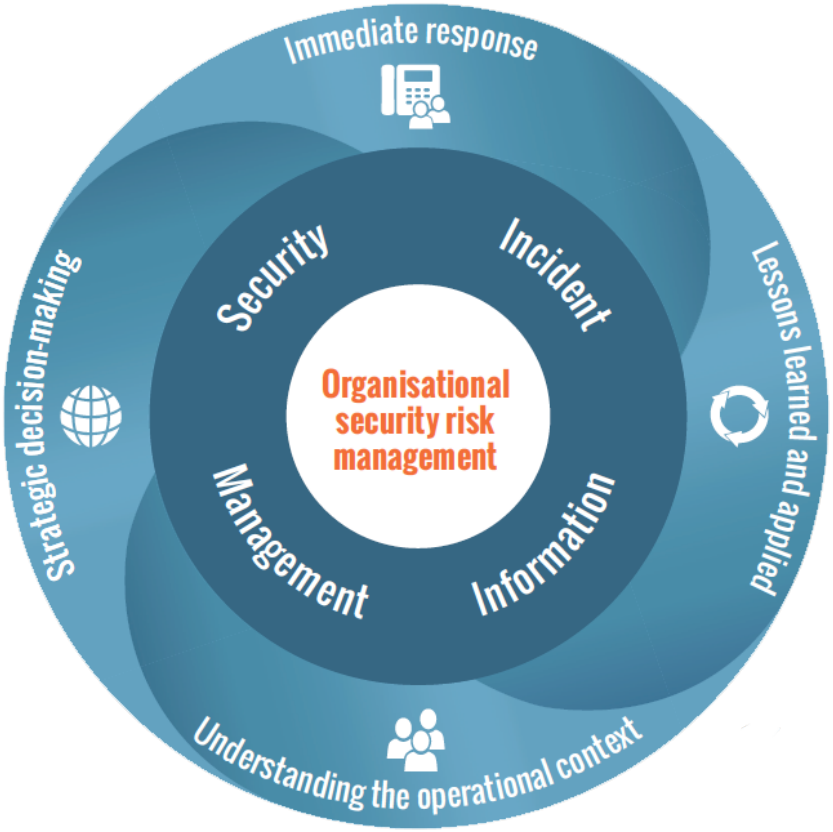
Your organization will use a classification system that clearly defines different types of incidents. This classification will help safety and security colleagues analyze the incident and compare it with similar incidents to draw out lessons to be learned.

# What is Safety and Security Incident Information Management?

Safety and security incident information management (SIIM) is the process of collecting and using information related to incidents to inform organizational decision-making. Safety and security incident information management allows organizations to:

1. Respond immediately to an incident.
2. Learn from the incident to improve staff safety and security.
3. Improve the organization's understanding of the operational context to support the delivery of programs.
4. Make informed strategic decisions across all departments of the organization.

Incident reporting enables organizations to meet these four objectives to improve the safety and security of staff, operations, and safe access to communities in need.



# How to Report an Incident

## Know How to Report an Incident

Your organization will have its own requirements and procedures for reporting security incidents. It is critical that you understand how to make a report BEFORE an incident takes place.

Your organization should provide you with clear guidelines on how to report an incident and set expectations on how they will use the information in the report to take next steps.

# Step 1: Report Immediately

Report the incident to your organization as soon as it is safe for you to do so. If you are involved in a critical incident, you may need to contact the authorities, but this will depend on the context and your organization's policy. If you are involved in a non-critical incident, your organization may ask you to complete a formal incident report instead of reporting the incident directly to the security focal point.

Follow your organization's reporting procedures to ensure that you and anyone affected by the incident receives the support they need. Make sure to provide your organization's focal point with critical information about the incident so they can respond effectively and immediately. Remember the 6 'Ws': **WHO** was involved, **WHAT** happened, **WHERE** did the incident happen, **WHEN** did the incident happen, **WHAT** actions have been taken so far, and **WHAT** help is needed.

Consider these questions when reporting a safety or security incident to your organization.

**Who was involved?**

Give the names, job titles, and information about staff and everyone involved in the incident.

**What Happened?**

Describe the details of the incident including any injuries, damage or loss.

**Where did the incident happen?**

Be specific about the location where the incident took place by providing the address, GPS coordinates, recognizable landmarks nearby, and/or describe how you arrived at the destination.

**When did the incident happen?**

Give the day and time when the incident occurred. The sooner you report an incident, the faster your organization can provide support and safeguard others.

**What actions have been taken so far?**

Explain if you have received help from anyone or a medical team, or if you have provided first aid to anyone.

**What help is needed?**

Be clear about the severity of any injuries and if you need your focal point to call the police, an ambulance, or provide transportation.

**Keep in mind...**

- Always report an incident as soon as possible, even if you are unsure about your organization's reporting procedures.
- The safety and security of everyone involved is the main priority at this stage.
- If the incident is ongoing, provide updates as needed.
- You can provide more detailed information later in the Formal Incident Report.

# Step 2: Complete a Formal Incident Report

After an incident takes place, complete a **Formal Incident Report** for your organization as soon as possible.

**What is the purpose of the formal incident report?**

This report will gather detailed information about the incident to help your organization learn how to prevent and improve the response to similar incidents in the future.

**What information is collected in the formal report?**

The formal incident report will include detailed information about what happened, the events leading up to the incident, actions taken following the incident, the personal characteristics and/or circumstances of those involved in the incident, and any other relevant information.

**Who completes the report?**

You may be asked to complete the report yourself or your organization's security focal point may interview you and complete the report with your help. This is a factual exercise, not an emotional debrief. Try to be as clear and factual as possible about what happened so trained colleagues can use the information to investigate the circumstances around the incident.

**How will the information be used?**

The information you share about an incident can be used by your organization in a number of ways, including informing decision-making around safety and security and other important aspects of your organization's work. If you are concerned that the incident might have been caused as a result of your actions or a mistake you made, you may feel the need to not be completely honest about what happened. Before deciding to withhold any information, ask your security focal point about the potential consequences of reporting.

## Step 3: Learn from the Incident

After completing the Formal Incident Report, take time to reflect on what actions you or others could have taken, if any, to avoid the incident. Accidents and mistakes do happen, so it is important for both individuals and organizations to learn from incidents to prevent and avoid similar incidents from occurring again. Remember that the purpose of learning from an incident is to reflect and prepare for the future and not to assign blame.

**How will the information be used?**

Take time to think about the actions you and others involved took before, during, and after the incident. Consider if there were any actions you or your organization could have taken to prevent or avoid the incident. Think about how you will apply lessons learned from the incident to prevent similar incidents from occurring in the future. Remember that the aim of reflecting on lessons learned is to identify practical and procedural solutions for the future that increase resilience. It is important that you do not blame yourself for the incident – accidents and mistakes do happen, and you are never to blame for the harm someone else has caused you.

**Were you a target?**

Structural, institutional, and personal prejudice can make some people more vulnerable and put them at greater risk than others to particular threats. Your safety and security colleagues may ask you questions about your personal characteristics and individual circumstances (ethnicity, personal status, gender identity) to determine if you might have been targeted based on who you are or how others perceive you. If you feel uncomfortable disclosing this personal information, ask how the information will be used and kept confidential. If you feel that underlying structural and systemic issues, discrimination, and/or bias are a factor that may have led to the incident or made you a specific target, inform your safety and security colleagues about these issues as they also may not be aware of these risks or their own unconscious bias.

## Step 4: Inform Decision-making

The information you share in your report about the incident will help inform decision-making in your organization.

**How will we apply what we have learned from the incident?**

The information you share in your report about an incident will help inform and improve your organization's decision-making process regarding:

- Contextual analyses
- Risk assessments
- Security and safety procedures
- Policy
- Operations
- Programming

# Example Scenario: Reporting a Carjacking Incident

Here is an example scenario for reporting a carjacking incident.

### Reporting Immediately

You and an international staff member visiting from HQ are involved in a carjacking incident while traveling to a field location. The perpetrators take your organization's vehicle and leave you and your colleagues on the side of the road. You and the other passenger are uninjured, but the driver was assaulted and needs medical assistance. You call your organization's focal point over the phone to report the incident.

### Providing Key Information

Try to communicate clearly, focus on the facts, and provide key information:

- **WHO WAS INVOLVED**: You provide the names, job titles, and other key information about the people involved in the incident: the national driver, you (a national program manager), and the HQ-based international staff member.
- **WHAT HAPPENED**: You explain the carjacking event and how the perpetrators took the car. You clarify that you and your international colleague are unharmed, but the driver was assaulted and needs medical assistance. The losses include: the vehicle, your international colleague's passport and laptop containing sensitive information about their personal identity, the organization, and the local community.
- **WHERE THE INCIDENT TOOK PLACE**: Since you do not have the exact address of where you are and your GPS is not working, you describe the route you took so far and mention that there is a river nearby.
- **WHEN THE INCIDENT HAPPENED**: You provide the day and time the incident took place.
- **WHAT ACTIONS HAVE BEEN TAKEN SO FAR**: You mention that two people on the road have stopped to help the driver get medical assistance.
- **WHAT HELP IS NEEDED**: You ask the focal point to arrange emergency medical assistance for the driver, and to send a vehicle for you and your colleague.

### Completing a Formal Incident Report

A few hours after the carjacking incident, your organization's security focal point asks to interview you so that they can complete the Formal Incident Report form.

They ask you for detailed information about what happened, how the driver was injured, the purpose of travel, and any circumstances leading up to the incident, during the carjacking, and shortly after.

### Learning from the Incident

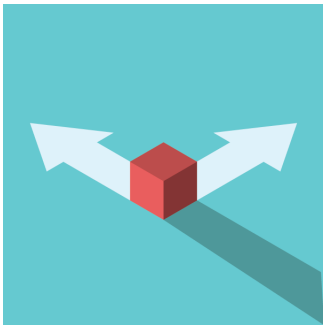
After analyzing the incident, your safety and security colleagues learn that:

- In the past three months, four other carjacking incidents have occurred in the same location.
- Each incident involved international staff members either from your organization or from other organizations in the area.
- All incidents occurred when the international staff members were visibly traveling in the vehicle and identifiable as foreign employees.
- The perpetrators of the incidents were identified as members of a particular armed group.

This information could explain why your vehicle was targeted in that location. Your colleague was sitting in the front of seat of the vehicle without tinted windows which made them easily visible and identifiable as a foreign employee.

Your safety and security colleagues also discovered that the driver is a member of an ethnic group with which the armed group has a history of conflict. Therefore, historical ethnic tensions in the area can explain why the driver was physically assaulted but the other travelers were left unharmed.

### Informing Decision-making



Your safety and security colleagues use the information provided in the report to inform further contextual risk assessments and to plan the following actions:

- Establish additional travel restrictions in the area where the incident took place.
- Include ethnicity in the organization's security risk assessments to identify and analyze risks that staff members from the same ethnic group as the driver may face in the operating context.
- Establish mitigation measures to reduce the risk of ethnic targeting, including setting up alternative work arrangements and travel routes for staff who may be at risk of ethnic violence.
- Provide training for organizational drivers on how to respond to a carjacking.
- Make it mandatory for international staff/foreign employees to travel in the backseat of vehicles with tinted windows.
- Share information about the incident (removing all identifiable information) with other organizations operating in the area so that they can take measures to protect their own staff.
- Have the IT team install additional software on organizational computers to make it difficult for thieves to access sensitive information.
- Ask program staff to inform community leaders and other authorities about the loss of sensitive data about the community and establish safeguards to protect these individuals from harm.
- If it is safe to do so, ask program staff to liaise with local leaders to try to open a dialogue with the armed group to improve the perception and acceptance of your organization, and improve your organization's access and security in areas where the armed group operates.

# Reporting Do's and Don'ts

## Reporting Do's and Don'ts

Consider these basic do's and don'ts when reporting a safety and security incident to your organization.

- **DO** know beforehand what types of incidents require reporting in your organization.
- **DO** report the facts as soon as it is safe to do so.
- **DO** be honest, clear, and precise.
- **DO** follow your organization's reporting procedure.
- **DO** reflect on what you could have done (if anything) to avoid the incident.
- **DO** ask how your personal information will be kept confidential.
- **DO** ask how you will stay informed about decisions and outcomes from the reported
- **DO** speak up if you are concerned about the reporting process and give advice on ways to improve it for other staff.

**DO NOT** delay reporting.

**DO NOT** leave out information.

**DO NOT** judge what is or is not important information to share.

**DO NOT** make immediate judgments about what happened or why.

**DO NOT** assign blame.

**DO NOT** be a detective and investigate the incident.

**DO NOT** assume that if the incident was caused by a mistake you made that you will be penalized. Ask about your organization's policy before deciding not to report.