



БЛАГОДІЙНА ОРГАНІЗАЦІЯ «БЛАГОДІЙНИЙ ФОНД «СТАБІЛІЗАЦІЙНИЙ СУПОРТ СЕРВІСІЗ»
CHARITABLE ORGANIZATION «CHARITY FOUNDATION «STABILIZATION SUPPORT SERVICES» 04053, Україна, м. Київ, вул. Січових Стрільців, 1-5
ЄДРПОУ 40567253, р/р 26008500242960 банк ПАТ «Креді Агріколь Банк», МФО 300614

Incident Reporting Procedure

Document Information	
Document Version	1.0
Applies to those who work on our behalf	<i>Employees, consultants, volunteers</i>
Prepared by	Toro Solutions
Approved by	Dermot Hamilton
Issued date	2020
Review date	Within two years of the issue date





Contents

1. Introduction	3
1.1. <i>Purpose</i>	3
1.2. <i>Procedure Review</i>	3
2. Procedure	3
2.1. <i>Why should we report incidents?</i>	3
2.2. <i>What is an incident?</i>	3
2.3. <i>Incident Reporting Process</i>	4
2.4. <i>Incident Database</i>	5
Appendix 1 – Incident Report Form	6
1.1. <i>Headline Information</i>	6
1.2. <i>Incident Information</i>	6
1.3. <i>Incident Review</i>	8



1. Introduction

1.1. Purpose

The document identifies why incidents should be reported, defines what an incident is, outlines the four steps of incident reporting, discusses the incident database and includes our incident report form. This procedure does not include the reporting of safeguarding incidents, which should be reported under the separate Safeguarding Framework.

1.2. Procedure Review

To meet with best practice and safety and security risk management developments and any changes in applicable law, we agree to review this procedure, and any other relevant documents or practices that govern and regulate incident reporting, every two years as a minimum.

2. Procedure

2.1. Why should we report incidents?

All incidents and near misses that involve anyone working on our behalf should be reported to a Senior Person. This is important because it:

- Ensures that immediate support can be provided to the affected individual(s) to reduce any remaining risks to them or others.
- Allows us to identify any trends or patterns of incidents we are exposed to and to determine whether any remedial action to prevent future reoccurrence of similar incidents is warranted or whether the security environment is deteriorating or improving.
- Provides us with a measurable indicator of whether existing policies and procedures are sufficiently reducing risk or whether alternative approaches require exploration.
- Ensures that we continue to learn from past incidents that have been reported and managed.

2.2. What is an incident?

The following table details all the threats, that we consider to be incidents. However, any incident that occurs either at work, or outside of work, should be reported.

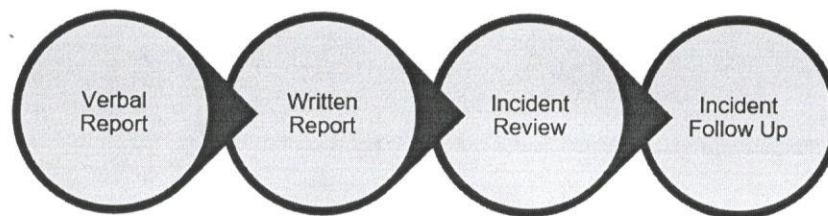
Incident Affecting:	Threats
Those working on our behalf	<ul style="list-style-type: none">• Vehicle accidents• Workplace accidents that cause physical or mental harm or injury• Threats of harm (made in any format)• Arrest and detention• Ambush• Personal attack or assault, attempted assaults• Abduction/kidnap• Bombing and other explosives• Landmine accidents• Physical surveillance of team• Natural disasters and diseases• 'Near miss' incidents



	<ul style="list-style-type: none"> • Traumatic or highly stressful events • Abuse of power situations • Any other situation that causes physical or mental harm or injury
Our data, systems and information	<ul style="list-style-type: none"> • Ineffective security controls • Information or system access violations • Uncontrolled system changes • Malfunctions of hardware or software • Human errors • A malware infection • Lost or stolen portable storage media or other computing equipment • The exposure of personal or private information relating to our organisation
Our finances or assets	<ul style="list-style-type: none"> • Thefts of funds • Theft or deliberate damage of equipment and other property • Bribery or attempted bribery • Extortion or attempted extortion
Our reputation	<ul style="list-style-type: none"> • Negative accusations made in public • Negative social media posts • Negative news stories • Accusations from partners, governments or the others in our sector
Our operations	<ul style="list-style-type: none"> • Disruption to our projects due to insecurity • Incidents targeted at our organisation • Deteriorating security situation
Our policies	<ul style="list-style-type: none"> • Non-compliance with any policies or procedures

2.3. Incident Reporting Process

The following process must be followed, after an incident has taken place:



Roles you can contact in case of an incident:

Role:	Name	Contact
Operations Director	Olga Ivanova	oivanova@stabilizationsupportservices.org
Programme Manager	Valeriia Vershynina	vershynina@radnyk.org
Human Resources	Kateryna Morhun	kmorhun@stabilizationsupportservices.org

2.3.1. Verbal Report (Immediate)

Any person working on our behalf who is involved in, observes, or is informed of any incident affecting them or others with them, should verbally report the incident to a Senior Person immediately (or as soon as it is safe to do so).

It is imperative to quickly establish the facts about the incident and determine its severity for possible escalation. This is done by ascertaining the following (in order):

- **WHO** is reporting the incident and **WHO** has been involved?
- **WHERE** is the individual(s) involved in the incident reporting from?
- **WHERE** did the incident occur?



- **WHAT** actions have been taken so far?
- **WHAT** actions are going to be taken?
- **WHAT** further assistance is required?

2.3.2. Written Report

Following the Immediate Verbal Report, it is the affected person's responsibility to document the incident in writing, within 48 hours. A written incident report states exactly what happened (as much as possible). The report should outline in some detail what happened, when, and how those involved responded, using the Incident Report Form¹.

Key information will normally include:

- Who reported the incident, and when?
- What happened, where and when?
- Who was involved and what was the impact on those affected?
- What assets were lost or damaged?
- Was our organisation directly targeted during the incident?
- Were any weapons used?
- What were the immediate actions taken?
- Who has been informed?
- What are the implications for those involved?
- What further actions should be taken?

The incident may also need to be reported to others outside of our organisation (e.g. donors, relevant suppliers, law enforcement and insurers).

2.3.3. Incident Review

Following an incident, we will conduct an incident review with all the individuals who were involved. Discussing the incident as a group will enable facts to be confirmed and changes in our procedures to be discussed. The incident review must be conducted within seven days of the incident.

Care should be taken if the incident involved any events that the individuals found traumatising. The incident review should not focus on discussing any feelings related to the incident or delving deeply into traumatic material. If any individuals express concerns about their, or others', psychological wellbeing, they should be referred to an appropriately qualified psychologist, for further assessment and care.

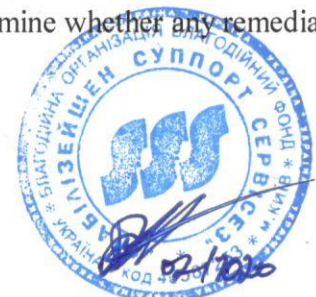
2.3.4. Incident Follow Up

A Senior Person must conduct a post-incident follow up to ensure the implementation of any changes identified during the incident review process. Incident follow ups should be conducted quarterly and use the Incident Report Form.

2.4. Incident Database

A Senior Person is responsible for maintaining the Incident Database which allows us to identify any trends or patterns of incidents we are exposed to and to determine whether any remedial

¹ See Appendix 1



PH



action to prevent future reoccurrence of similar incidents is warranted. The database also provides us with a measurable indicator of whether existing policies and practices are sufficiently reducing risk.

Appendix 1 – Incident Report Form

1. *Headline Information*

Incident Ref:	
Location:	
Date of Incident:	
Incident Type:	
Reported By:	
Avoidable / Unavoidable?	

2. *Incident Information*

Date & Time <i>Describe when the incident occurred as precisely as possible</i>	
Location <i>Describe where the incident occurred as accurately as possible</i>	
Description of incident <i>Describe the nature of the incident and events leading up to the incident, including:</i> <ul style="list-style-type: none">• <i>Who was involved?</i>• <i>Any witnesses?</i>• <i>What caused the incident?</i>• <i>The impact / material losses of the incident?</i> <i>Please attach sketches/photos when necessary.</i>	
If a data incident <i>Describe:</i> <ul style="list-style-type: none">• <i>The categories and approximate number of individuals affected</i>• <i>The types of personal data affected</i>• <i>The approximate number of personal data records concerned</i>• <i>A description of the likely consequences of the personal data breach</i>	



Was the incident specifically targeted? If so, at whom? <i>Please indicate if they were employees, consultants, or others</i>			
Actions taken so far <i>Detail any decisions and actions taken following the incident</i>			
Implications to others <i>Highlight possible implications of the incident for the safety, security, health and wellbeing of others working on our behalf</i>			
Is further assistance required?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Not Sure <input type="checkbox"/>

04



3. Incident Review

<p>Contributing factors: List what factors contributed to the incident occurring.</p> <p><i>Consider:</i></p> <ul style="list-style-type: none"> • Targeted or 'wrong place, wrong time'? • Threat environment/context changes • Profile of those involved (e.g. ethnicity, sexual orientation, gender, age, etc). • Profile of the people and organisation(s) affected • Behaviour at time of incident • Was there a breach in policy/procedure leading or contributing to the incident? 		
Remedial action required to prevent reoccurrence	Action owner	Completed?
		<input type="checkbox"/>
		<input type="checkbox"/>
		<input type="checkbox"/>
		<input type="checkbox"/>
		<input type="checkbox"/>
		<input type="checkbox"/>
		<input type="checkbox"/>
		<input type="checkbox"/>
		<input type="checkbox"/>
		<input type="checkbox"/>

81