**Reference:** CRITICAL INCIDENT MANAGEMENT WITHIN FEDERATION OPERATIONS

**Annex:** **H**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Document authorization** | | | | |
| **Stakeholder** | **Name** | **Position** | **Signature** | **Date approved** |
| Author | Reynette Royer-Thomas | Country Cluster Support Team – Port of Spain (CCST)  CADRIM Coordinator |  |  |
| Document authorizer | Jorge Zequeria | Coordinator, Security and Safety, IFRC Americas Regional Office (ARO) |  |  |
| CADRIM Document Stakeholders | Reynette Royer-Thomas  Chamara Hollingsworth  Tamara Lovell | Coordinator  Admin/Finance Assistant  DRM Coordinator |  |  |
| NS Document Stakeholders | Winston Waithe  David Griffith  Danielle Toppin | President  Head, Disaster Management Dept.  Project Coordinator, Zika |  |  |
| Regional Document stakeholders | Lorenzo Violante  Josephine Shields-Recass | Head, Policy Strategy and Knowledge Unit (PSK), ARO  Head, CCST – Port of Spain |  |  |

**Definition of a Critical Incident**

A situation that threatens or has impacted on the safety/security of Federation personnel, assets or operations to the extent that there is the potential for significant disruption or even incapacity to continue to operate.

The term **situation** is used in the definition so as to be sufficiently broad to encompass, specific situations e.g. accidents with serious or multiple injuries, violation of status agreement, kidnapping, a major disruptive event such as a hurricane, building fire or pandemic, or the death of a Delegate.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Minor Critical Incident** | **Significant Critical Incident** | **Major Critical Incident** |
| **Description** | Incident that causes minor disruption to CADRIM’s operations e.g. any accident without serious injury, theft. | Incident that causes significant disruption to CADRIM’s operations e.g. death of (a) staff member(s), accident with serious or multiple injuries, property damage, burglary [[1]](#footnote-1) etc. | Incident that jeopardizes CADRIM’s operations or incapacitates it. e.g. serious deterioration in security situation, multiple loss of life, violation of status agreement, major equipment loss, office fire, pandemic etc. |
| **Management Approach** | Senior IFRC Officer on site manages the incident, and, Head, CCST, Director of Region and Geneva Senior Management Team (SMT) advised through incident reporting procedures. | Senior IFRC Officer on site, Head, CCST manage incident with advice (and if required, direction) provided by Director of Region and Geneva SMT. | Incident managed through Geneva  Field teams provide information and act on direction from the Critical Incident Manager  A support team may be deployed in the case of a field incident. |
| **Reporting**  **Requirements** | Written incident report [[2]](#footnote-2) submitted within 24 hours | Immediate verbal report via telephone;  Written incident report submitted within 24 hours;  Written and oral reports submitted in keeping with decisions taken related to incident response and follow-up. | Immediate verbal report via telephone;  Written report submitted within 24 hours;  Regular written and oral reports submitted in keeping with a timeline developed by the incident management team |

**NOTIFICATION AND RESPONSE PROCEDURE**

The notification and response procedure for significant and major incidents is as follows:

Secretary General and Geneva SMT (Including Security Unit) Informed / Advised / Consulted

INCIDENT

Senior IFRC Officer/CADRIM Coordinator on site Advised,

DG, BdsRC advised,

notified

Head, CCST Advised /Consulted

**Key Initial Information Requirements**

* **I**ncident type (e.g. kidnap, death, serious assault, loss of assets, pandemic)
* **C**ontext
* **E**xact location
* **C**asualties
* **R**esponse by Federation, by Government, Movement partners
* **E**mergency Response action taken so far
* **A**ssistance required
* **M**edia interest
* Critical Incident Manager appointed
* Critical Incident Management Team established to manage incident / Situation
* Critical Incident Manager appointed
* Critical incident Management Team established to manage incident / Situation
* Critical Incident Manager appointed
* Critical Incident Management Team established to manage incident / Situation

1. **Immediate Response:**

The document below outlines the basic procedures to be followed in response to a critical incident within/involving CADRIM.

1. Incident reported to Senior IFRC Officer on site/Senior IFRC Officer in country.
2. Senior IFRC Officer on site/Senior IFRC Officer in country (or his/her designate) calls until one is reached, who then informs the others on this list:
   * Head, IFRC Country Cluster Support Team (CCST) in Trinidad – Ariel Kersens +1-868-722-3662
   * Deputy Director, IFRC Americas Regional Office (ARO) - +507-6677-6520
   * Director of IFRC Americas Regional office (ARO) - +507-6670-7377
   * Security Unit in Panama - +507-6949-5546
   * Security Unit in Geneva - +41-79 217 33 71
   * Head, Disaster Management Department, Barbados Red Cross (BdsRC)
   * (BdsRC) Director General or President (if DG is not accessible/available)
3. Senior IFRC Officer on site/Senior IFRC Officer in country (or his/her designate) contacts local authorities in the area (Royal Barbados Police Force, 211, BdsRC, Department of Emergency Management, Barbados Fire Service 311, etc.) and requests assistance.
4. Senior IFRC Officer on site/Senior IFRC Officer in country (or his/her designate) generates SMS Alert of incident to all BdsRC human assets in order to minimize additional staff members’ exposure to danger.
5. Senior IFRC Officer on site/Senior IFRC Officer in country (or his/her designate) commences collecting information on the incident to advise the Head, CCST.
6. Senior IFRC Officer on site/Senior IFRC Officer in country (or his/her designate) informs Insurance Provider, Head, CCST and family members (as applicable).
7. Head, CCST and Senior IFRC Officer on site form Critical Incident Management Team (CIMT) including identification/ appointing of a Critical Incident Manager (CIM), who directs resources as needed.
8. The CIMT takes over all line and operational responsibilities of the incident (as per the process outlined below), report directly to the Head, CCST who retains overall authority.
9. **Critical Incident Management Process:**

The Critical Incident Management Process (CIMP) usually includes five stages as per the diagram below:

**Stage 3**

Analyze the available options

**Stage 1**

What has happened?

**Stage 5**

Debrief

**Stage 4**

Implement chosen response option

**Stage 2**

Analyze the situation

**Stage 1: Establishing What has Happened**

The first action must be to identify whether there ***is any immediate action required to protect life, liberty, or physical person. Any action so identified must be taken.***

Verifiable information must be established outlining the details of the incident and a comprehensive incident log is to be initiated. This log would include the chronology of events, a record of all phone calls, and notes of all meetings. All related documents must be recorded and filed.

**Stage 2: Analyse the situation**

What do you need to do?

What has been done?

What do you need to know?

What do you know?

The primary aim of this stage is to identify the problem and the parameters surrounding it:

* RC Movement actors involved (ICRC, IFRC) and current status (locations, operational agreements in force, etc)
* Security issues
* External actors involved
* Country context – current situation (disaster, conflict etc.), infrastructure (transport, medical, food and water, sanitation), capability of Government, status and capability of NS in country, status of Federation in country, limitations on ability to act/or and operate.
* Legal issues
* Medical issues
* Communications issues
* Media issues
* Determine the end-state objective (injured person evacuated, body repatriated, hostage released)

The CIMT must also decide:

* Whether any programme activities should be suspended due to risks to personnel, and/or whether personnel should be withdrawn to a more secure location.
* If additional support personnel should be deployed to any field location to assist.
* What information should be circulated internally and externally.
* What are the situation’s limitations or issues re: confidentiality.
* If any additional personnel or external specialists should be included in the CIMT.

CIMT members may be assigned specific roles/tasks and responsibilities for managing relations with specific stakeholders.

**Stage 3: Option Analysis**

|  |
| --- |
| At the start of this stage, the following questions must be asked:   * Is this situation covered by existing contingency plans? If so, can they be implemented? * Is the situation severe enough to warrant the activation of a business continuity plan? * Does the Federation have the internal expertise to manage the incident – if not, where can this be accessed? |

If there are no existing current contingency plans or no existing continuity plans that can be adapted, then a response plan must be developed. This requires the identification and analysis of options to reach agreed-upon end-state objective(s). During this stage the following should pertain:

* Only options and factors that contribute to the identified end-state should be discussed and analysed.
* Options should have technical input from all members of the CIMT.
* If technical input is required that is not available from within the CIMT then external advice must be obtained.
* All options must be tested against:
  + Fundamental Principles
  + Code of Conduct
  + Limitations imposed by country context
  + Resources available to implement
* Preferred option is identified by CIMT and presented for approval and action of the Head, CCST, the Americas Director of Region and BdsRC Director General.

When considering options and having identified the preferred option, the CIMT must always consider the fluid nature of the situation and the potential implication this might have. The question ‘**What if -?**’ (- something changes or something new happens) should constantly be tabled.

**Stage 4: Implementation**

The CIMT’s role is to monitor the response plan’s implementation and to be prepared to adjust actions and related plans as required.

Implementation of the preferred option should be guided by a detailed plan. This should:

* Clearly define the objective(s)
* Assign clear roles
* Detail clear coordination aspects – timings, reporting requirements, interaction with other players – ICRC, Bds RC and/or external agencies
* Define a clear command and control framework
* Detail a protocol to govern the flow of information related to the incident. The CIMT needs to ensure that Federation Media and External Communication Department, ICRC and BdsRC are kept informed. There will be need for control over information to the press/media and information sharing with our stakeholders. This might involve information black outs or preparation of press briefings, media statements and internal information sharing within the BdsRC.

**Stage 5: Follow Up/Debrief**

It is absolutely necessary to ensure that support is provided to those directly affected and/or closely involved with the situation. The ranking IFRC officer co-ordinating the operation/ DG BdsRC may request of the Head, CCST either that a PSP team be deployed to the CADRIM, or that specific individuals be referred for psychosocial support.

After the incident has been resolved a debriefing process is to be implemented. In the first instance, the incident and situation surrounding the incident are to be fully investigated to determine why it occurred, whether it could have been prevented and how to prevent it in the future. Secondly, the debriefing is to examine how the incident or situation was managed, in order to determine what can be learned and whether the manner in which it was managed could be improved. This process is to work through the incident chronologically, examining the actions taken at each stage.

* Confirm that the incident log and sequence of events are accurate
* Were the actions taken appropriate?
* Were the existing procedures followed and are these procedures appropriate or do they need changing?
* Lessons should be identified and recorded
* Are there any follow-up requirements: e.g. counselling, asset acquisition, legal/ insurance-related?

A post-incident report is to be produced and forwarded to senior management. This must include the Head, CCST and the Director General BdsRC.

1. burglary with entry” comprises burglary where the building was successfully entered, regardless of whether something was stolen or not; “burglary with loss” comprises burglary where a building was successfully entered and something was stolen;“burglary with no loss” comprises burglary where a building was successfully entered but nothing was stolen; “attempts” comprises incidents where there is clear evidence that the offender made an actual, physical attempt to gain entry to a building (for example, damage to locks, or broken doors) but was unsuccessful [↑](#footnote-ref-1)
2. Security incident reporting procedures are outlined in the Security Section of the Fed Net - go on Fed Net-secretariat-security and then incident reporting. [↑](#footnote-ref-2)