Crisis Management Policy

For the Christian Reformed Church in North America (CRCNA)

(Revised May, 2018)
(Resonate added MLC approved VII D Feb 2019)

PROLOGUE

No matter what the circumstance, God holds our lives and our times in his hand. We live in a broken, sin-filled world in which natural disasters and human violence happen and present serious dangers to human life and safety. God requires that we not harm or recklessly endanger ourselves (Heidelberg Catechism Q & A 105) and that we protect others from harm as much as we can (Heidelberg Catechism Q & A 107). The CRCNA Crisis Management Policy was written and approved in the spirit of and with the assurance of these facts.

When people enter God's service in public ministry, they do so having first professed a commitment to devote their lives to God. Most of the time, Christian workers and families in domestic or overseas postings walk through careers encountering the quiet and rough waters and the green and scorched pastures we accept as routine in a world awaiting Christ's full shalom. Yet the mystery of God's preserving grace can numb us to expect safety. Today, more and more frequently in a world with perforated borders, instant electronic communication and conflicts even between people of faith, we walk through the valleys that contain the shadow of death, and sometimes death itself.

In such a volatile world, it is incumbent on offices, agencies and educational institutions of the Christian Reformed Church to provide conditions of reasonable safety for personnel and their families. Thus, the Council of Delegates of the CRC directs the Ministry Leadership Council and the Crisis Management Policy Team to maintain standards and strategies commonly referred to as *Crisis Management Policy*. This policy should by no means be understood as an attempt to eliminate all risk nor as unconditionally guaranteeing staff safety.

The policy must be understood and implemented with full awareness that Christian ministry workers must be willing, often due to unforeseeable conditions and circumstances, to take and face physical risks and to develop the spiritual courage that may be needed to accept the risk to physical life and personal well being. At the same time, and equally important, is the stated caution that one may not recklessly endanger one's own life or the lives of others.

I. Introduction to this policy statement and its appendices

A. Purpose

To establish a CRCNA policy for all denominational personnel (employees, volunteers, their accompanying spouses and dependent children), particularly those who serve in places where political conflict, natural disasters, terror and terrorism are a real and present danger.

B. Status

All denominational personnel must follow the policy as a condition of their service within the CRCNA.

C. Scope

The policy is herewith stated so that all may know in advance the proper and appropriate responses to crises with particular, although not exclusive, attention to acts of terrorism (e.g., kidnapping, ransom demands, extortion, hostage-taking, or civil unrest). Because of the uniqueness of each situation, as well as the complexity of circumstances within which events may occur, no policy can anticipate every situation. In cases of ambiguity, those assigned responsibility for the implementation of this policy are authorized to make decisions within the spirit of the policy as stated below. Toolkit Item 4 provides an overview of the process upon notification of a crisis.

D. Application

All CRCNA personnel, especially those whose ministries require constant or frequent exposure to the risks anticipated in this policy should become familiar with, and retain a copy of, this policy as well as any guidelines, procedures, or related items that the Crisis Management Policy Team (CMPT) may adopt to implement it.

E. Implementation

All questions, exceptions, and matters relating to the implementation of this policy shall be referred to the Crisis Management Policy Team.

II. Definitions

A. Crisis: A situation occasioned by an unplanned event or set of events that may disrupt, endanger or destroy CRCNA's personnel, property, systems, information, or reputation.[1]

B. Denominational personnel: CRCNA employees, volunteers, board members, and their accompanying families[2] and guests, or anyone with official reporting and or other accountability lines to the CRCNA.

III. Purpose and Composition of Teams

A. *Crisis Management Policy Team (CMPT)*

1. Membership: Those serving in the following positions by virtue of their offices:

- The executive director of the Christian Reformed Church (ED - convener).

[1] Adapted from notes taken by Gary Bekker from a presentation by Alexander Tabb, Managing Director of Kroll Worldwide, at the ORC Missionary Roundtable October 10, 2002.

[2] "For CRCNA employees, *family* includes all legal dependents recognized by CRCNA Human Resources. For international personnel, local entities are asked to specify which individuals and family members are included in contingency plans.

- The director of Resonate Global Mission
- The co-directors of World Renew.
- The Canadian Ministries Director
- The Director of Timothy Leadership Training Institute
- The director of Back to God Ministries International.
- The director of finance and operations.

Representatives from Calvin College and Calvin Theological Seminary are invited to participate.

2. Responsibilities:

a. The CMPT has ongoing responsibility to make sure that . . .

- Policies are provided, reviewed, and updated as necessary.
- All persons serving under the auspices of the Christian Reformed Church in North America or any of its entities are thoroughly knowledgeable with all aspects of this policy.
- All such persons fully comply with the provisions of this policy.
- The positions of Risk Assessment and Monitoring Coordinator and [Crisis] Training Coordinator are staffed, appropriate administrative support is given (so that these positions form the Crisis Preparedness Team), and a network of decentralized monitors is identified to assist the Crisis Preparedness Team. (See Appendix D)
- Permission from the ED is obtained for any requested exception to this policy.
- The ED is notified immediately by any person or agency of any pending or existing situation that might necessitate implementing this policy. Upon notification, a process of action is followed as suggested in Appendix H.
- The ED convenes the CMPT as soon as possible upon receiving information that invokes this policy and makes sure that appropriate action is taken. (See Appendix H)

b. The CMPT has the following responsibilities in particular situations:

1) If the CMPT judges that a crisis is in the making, or when a crisis has not yet occurred but there are indicators of a crisis, the CMPT may form a <u>Monitoring Team,</u> consulting with the Risk Assessment and Monitoring Coordinator as appropriate..

2) If the CMPT declares that a crisis has developed, the CMPT shall nominate not fewer than three (3) persons for appointment to an <u>Event Response Team</u> (ERT). The CMPT shall submit its recommendation to the ED, who shall make the appointments on behalf of the BOT. Once the ERT is appointed, the CMPT is informed by the ERT of progress and any notable changes in the situation.

B. *Crisis Preparedness Team (CPT)*

1. Membership: Includes the Risk Assessment and Monitoring Coordinator, the Training Coordinator, and the person providing Administrative Support (See also Appendix D); internal and external consultants may be included.

2. Mandate: To coordinate CRCNA work in three areas:

A. Regionally distributed security monitoring (see also Appendix D).
B. Compliance of CRCNA personnel with CRCNA crisis management and travel policies.
C. Preparedness for crisis of CRCNA information, human resources, communication, and electronic systems.

3. Accountability: To the CMPT through the CRCNA Executive Director, including authority to recommend appointment of monitoring and event response teams.

C. *Monitoring Team (MT)*

1. Purpose and Rationale: The Monitoring Team is a team of people appointed by CMPT at its discretion to monitor and give advice to CMPT regarding security concerns on any topic, place, or event. A Monitoring Team is used in situations that may not require an ERT but where there are indications a crisis may be pending. If the situation escalates to a level where CMPT judges an ERT is required, members of the Monitoring Team may become part of the ERT, but the Monitoring Team's assignment ends when the ERT is appointed. Note: An individual agency may also form their own Internal Monitoring Team and provide notice of its establishment and its reports to the CMPT.

2. Appointment: The primary criteria for appointment to the Monitoring Team is the ability to gather information and evaluate the situation. It would be helpful for at least one team member to have former field experience.

3. Responsibilities: The responsibility entails gathering information from the field and other sources and sharing it with both the CMPT and the normal field administrative structures.
   - The field would be required to relay all circumstances and information available at the country level to the Monitoring Team, and the MT to the field.
   - The MT recognizes that the field has additional burdens during the crisis situation and wants to relieve some of those burdens.
   - The MT would have access to additional information that the field may not be able to access.
   - The MT would be in frequent communication with the field and provide regular updates to the CMPT.

4. Accountability: Working with the Risk Assessment and Monitoring Coordinator (and his/her network of decentralized, regional monitors), the MT shall be accountable to the CMPT.

5. Advisers: The Monitoring Team may seek the advice of non-MT CRCNA personnel and include these advisers in MT meetings. These advisers would not have voting rights.

6. Status: Early in the situation, the MT should develop criteria to use in deciding whether to recommend that the CMPT escalate their status to that of an ERT or move back to the normal administrative structure.

D. *Event Response Team (ERT)*

1. Role: The CMPT is the only CRCNA entity responsible for nominating an ERT and for advising an ERT in its work on a crisis, as appropriate. All other organizational groups or entities affiliated with the CRCNA are required to refer all crisis-related information to the ERT once it has been appointed. No

action related to a crisis can be taken without the ERT's authorization, and no public statements related to the crisis can be made without the ERT's authorization.

2. Appointment: At least three (3) people appointed by the ED on behalf of the BOT ordinarily upon the recommendation of the CMPT. Primary criteria for appointment are the ability to manage the crisis at hand. CMPT members may serve on an ERT by way of exception. If they do serve on an ERT, their membership on CMPT will be suspended until the CRCNA-BOT has accepted the evaluation of the crisis management for which the ERT was appointed. The memo template for team appointment is found in the Toolkit, Item 1.

3. Responsibilities: The ERT has exclusive responsibility for managing the crisis at hand. The ERT shall exercise its responsibility until the crisis is declared to be over by the CMPT ordinarily upon the ERT's recommendation. Because the ERT has exclusive responsibility for managing the crisis at hand, all other organizational groups or entities affiliated with the CRCNA are required to refer all crisis-related information to the ERT once it has been appointed. No action related to a crisis may be taken without the ERT's authorization, and no public statements related to the crisis may be made without the ERT's authorization. This arrangement is intended to buffer the CMPT and the rest of the CRCNA from the crisis event so that the mission of the CRCNA can continue during the crisis.

4. Advisers: An ERT may seek the advice of non-ERT CRCNA personnel and include these advisers in ERT meetings. However, the ERT chair will make clear to the advisers and to ERT members that the advisers participate as guests, not as voting members of the ERT.

5. Accountability: ERT shall be accountable to the ED. The ERT shall also give regular updates to the CMPT of progress (at least weekly) and any notable changes in the situation.

IV. Risk assessment

A. Policy: All CRCNA entities are required to conduct and maintain adequate and timely tactical and strategic risk assessments. Strategic risk assessments are to be conducted at least every two years by each agency and denominational office. Tactical risk assessments are to be conducted at the beginning of a new project, partnership or country ministry and at least every year thereafter. Both types of risk assessment are necessary for a comprehensive and accurate understanding of risks and dangers facing the organization. A scale useful for risk assessment is found in Appendix A.

- *Tactical assessment* analyzes the present situation and identifies threats and vulnerabilities that are present here and now; and
- *Strategic risk forecasting* anticipates future risks and predicts both the probability and consequences of unwanted events occurring.
- Note: Risk Assessment and Monitoring Coordinator is responsible for monitoring of the assessments.[see Appendix D]

The frequency of strategic and tactical risk assessments is to be increased if:

- The assessed risk/threat level is such that field, regional, or denominational leadership determines that a more frequent risk-assessment schedule is appropriate. See Appendix A: Levels of Risk
- There is significant change in political or economic situations. See Appendix B for policy on political involvement of CRCNA personnel in foreign countries.

B. Policy: All CRCNA entities are required to establish procedures that regularly monitor the travel of staff and ensure that safety and security concerns are considered when trips are approved.

Core Standards:

1. Each CRCNA entity shall establish a central location that collects itineraries and archives them so that there is 24/7 access by multiple people.
2. Each CRCNA entity shall ensure traveling staff communicate with and get informed approval from supervisor and designated senior leadership regarding:
    a. Advice from CRCNA Country Monitoring Teams, including Event Response Teams
    b. Awareness of Canadian and US government alerts for country of destination
    c. Pre-approval from insurance for their monitored countries
    d. Notification of CRCNA staff who reside in the country of destination

V. Contingency plans

A. Each entity of the CRCNA, including executive offices, agencies, and support services is required to develop contingency plans and keep them current for threats and dangers that are reasonably foreseeable and potentially threaten the safety of personnel and expatriate guests or threaten to disrupt their work. Educational institutions such as Calvin College and Calvin Seminary are exempted from this requirement since they have their own accountability systems that cover this need. Specialized ministries are required to make contingency plans but it may not be necessary to have all aspects that agencies address due to the different nature and scope of their work.

B. All such plans shall address:

- Evacuation of personnel (both local and countrywide). Appendix C states policy covering evacuation of national personnel outside of Canada and the USA.
- Management of major assets (real estate, vehicles and equipment) through a crisis.
- Information management during a crisis.

C. CRCNA entities with international operations are required to use a risk assessment software program such as CCI's EZRA program or an approved equivalent. If a category of foreseeable threat or danger is not included in the risk assessment software, the contingency planner will address that threat or danger by another means.

Canada/USA-based CRCNA entities will take into account at least the following threats and dangers. If an entity's planner judges that a particular item on the list is not a foreseeable threat or danger to that entity, the planner may request an exemption from addressing it from the DDM.

Abduction
Accidental death
Airplane crash
Bomb threat
Disease (severe) exposure
Earthquake
Explosion
Terrorism
Tornado
Exposure to toxic substance
Business interruption
Violent act
Threat of violence
Hurricane
Kidnapping
Hostage taking
Motor vehicle accident
Robbery/theft
Suicide
Food contamination
Fire
Political instability
Flood
Sabotage

VI. Training

Policy: To provide security and crisis-management training to all personnel. The training program is led by the [Crisis] Training Coordinator (see Appendix D). The type and degree of training shall be commensurate with the assessed risks and dangers the member is exposed to, as well as being commensurate with the member's organizational responsibility for the safety and security of other personnel and organizational assets. All personnel shall receive training in at least the following areas:

- All CRCNA crisis policies and procedures (see Appendices) that pertain to their roles.
- Evacuation procedures – appropriate to the location of their workplace.
- Basic personal safety and security – appropriate to the location of their workplace.

Designated personnel are asked to sign a form (Toolkit Item 2) indicating their awareness of risk and commitment of follow policy.

VII. Information and Communication management during crisis

A. The Crisis Communication Guidelines (from the Employee Handbook) provide the first considerations:

When any member of CRCNA staff becomes aware of a significant issue or potential crisis that could affect the denomination or its ministry, the following questions should be considered in assessing the situation:

1. Does this compromise our values?
2. Does this go against or jeopardize us from achieving our mission?
3. Does this put our brand promise/reputation/image at risk?
4. Has this violated an organizational or ministry policy?
5. Will there be a significant impact on our ministry?
6. Will the media be interested in the situation?
7. Will the situation cause concern to CRC congregants or churches and church leadership?
8. Will our agencies and other ministries "catch heat" from churches, donors, etc.?

If the answer to any of these questions is "yes," the matter must be brought to the attention of the Executive Director, CRCNA.

The Executive Director will evaluate these questions with the following criteria in mind:

1. Could this be detrimental to our ministry on a large scale?
2. Is there potential for negative media exposure?
3. Will this damage our relationship significantly with one or more key audiences: donors, employees, local church leaders, classis, congregants, or partners?
4. How will this event or issue play out over the next several days, weeks, months? Does this change the impact it could have on our ministry?

If the answer is "yes" to any of these questions, then the Executive Director will alert the Crisis Communications Task Force and activate the Crisis Communications Process.

B. Crisis Communications Process Points/Crisis Communication Task Force

1. Any information regarding a potential crisis should be forwarded immediately to the Director of Communications.
2. The Director of Communications will immediately inform the Executive Director (or designee) as well as agency heads for whom the potential crisis may have impact.
3. The Director of Communications, in consultation with the Executive Director, will determine if a Crisis Communication Task Force needs to be formed to handle the situation. If a task force is not needed, the Director of Communications will communicate the issue and resolution to the ED and agency directors as appropriate.
4. If a Crisis Communication Task Force is necessary, the Director of Communications will form the task force, drawing from the following departments:
    a. CRC Communications team
    b. Advancement group
    c. Ministries Leadership Team
    d. Specialized Ministries leadership group
    e. Agency/Institution Communications staff
    f. Denominational Office
5. The Director of Communications will serve as the link from the Crisis Communications Task Force to the Executive Director or designee.
6. The Crisis Communications Task Force is fully empowered to assess the crisis, develop a solution and implement the solution, using the Crisis Management Guidelines as a tool for determining the magnitude of the crisis and the best solution.
7. A solution should be determined and activated within 24 hours of identifying the crisis.
8. When a solution has been determined, the following should be alerted:
    a. Executive Director or designee
    b. Ministries Leadership Team
    c. Specialized Ministries leadership group
    d. Presidents of Calvin College & Seminary
    e. CRC Communications team
    f. All employees (optional, depending on the crisis)
    g. Churches/stakeholders
9. Regular updates will be provided to the Executive Director or designee as needed after the solution has been determined and while the action plan is underway.

C. Crisis Communication When an ERT is Functioning.

1. Information relating to a crisis shall be carefully and strictly directed and controlled by the ERT.

    - Incoming communications such as background information, suggestions about resources and assistance, ideas for resolution, and so forth, shall be forwarded to the ERT.
    - Outgoing information shall be monitored to prevent the release of confidential information, to prevent exacerbation of the situation or the creation of secondary crises, and to control the spread of rumors. Individual crises vary greatly in the level of monitoring necessary, and the ERT or MT shall develop communications guidelines for the specific situation (working with the Crisis Communication Task Force if one has been established.

2. All information, intelligence, ideas, suggestions, and so forth that relates to a crisis be directed to the ERT or MT at the earliest possible time. Any member of the organization with such

information or with suggestions for the ERT shall forward the information or suggestions immediately to the ERT.

3. The MT or ERT shall establish guidelines for outgoing information and public statements (working with the Crisis Communication Task Force if one has been established). The ERT communication guidelines shall apply to statements to internal constituencies (other members, families, and so forth) as well as external constituencies (the media, extended family, home churches, government agencies, and so forth). Options include but are not limited to:

- All information released and all public statements made about the crisis shall be approved by the ERT prior to being disseminated.
- The MT or ERT shall develop guidelines for official statements that missionaries involved could send out with their own short introductions.
- No member of the organization outside of those authorized by the ERT is authorized to make any statement that relates in any way to an ongoing crisis.

4. The CRCNA Director of Communications shall serve as an adviser to the ERT on decisions involving internal and external communications**,** and if a Crisis Communication Team has been established, the CRCNA Director of Communications shall be the link between Teams.

D. **Guidelines for outgoing information and public statements during times of security risk.** The CRCNA has policies to guide communications even in places where there is no security risk. See the "social networking and media policy" of the Employee Manual, for example, to be reminded that as an employee of the CRCNA, "*your online presence reflects on the CRCNA.*

"Be aware that your actions captured via images, posts, or comments may appear to reflect those of the CRCNA. Before creating online content, employees should consider some of the risks and rewards involved, and recognize that conduct that adversely affects job performance, the performance of other employees or otherwise adversely affects CRCNA may result in disciplinary action."

While these policies apply at all times, there are some times and some places where CRCNA employees work that may involve more security risks than others. Staff are reminded to prioritize personal safety as well as the safety of colleagues and partners in the region. In addition to the general guidelines, we also recommend that staff use the following guidelines depending on the level of risk where they are working. The Communications Protocol Levels (below) are to be assigned by CRCNA regional leaders, in coordination with any Crisis Monitoring Team (MT) or Event Response Team (ERT).

Communications Protocol Level A (no risk)

- Remember that your content reflects on the CRCNA and your ministry
- Remember to get permission before using people's photos or names publicly
- Remember to protect the privacy of children and only use their names and locations with guardian permission

Communications Protocol Level B (minimal risk)

- All guidelines from Level A

- Be careful about publicly criticizing the government or government policies
- Be aware of specific "hot button" issues in the region and avoid drawing unnecessary attention to yourself or your program

Communications Protocol Level C (steady level of risk at all times, in some places or related to some topics)

- All guidelines from Levels A and B
- Alert your supervisor or country leader about all planned outgoing communication (blogs, newsletters, prayer letters, etc) so that someone can provide guidance about what is shared and monitor what goes out
- Be careful about mentioning evangelism and conversion stories; if the government is suspicious about Christianity, overtly religious communication should be avoided
- Do not mention location of staff offices or programs
- Check with staff and crisis management team before mentioning staff members or their family by name

Communications Protocol Level D (specific situation has led to increased risk in some locations or related to some topics)

- All guidelines from Levels A, B, and C
- Adhere to communications guidelines provided by MT or ERT
- Do not mention staff members or their family by name
- Do not mention the location of staff in the country or those who may have left
- Utilize pre-approved statements from MT or ERT and Crisis Communications team in staff newsletters, blogs, and emails.

Communications Protocol Level E (high level of risk)

- All guidelines from Levels A, B, C, and D
- No staff outside of those authorized by the MT or ERT may make any sort of public statement about the ongoing crisis (this includes any form of digital communication: blog post, social media post, email message)
- All public communication must be cleared by the MT or ERT and crisis communication team before they are sent out or posted online.

Additional Information - the CMPT has 6 Levels of RISK, see below. Note that these levels of risk do not directly correlate to the Communications Protocol Levels. Your CRCNA regional leaders and the Crisis Monitoring Team or Event Response Team will alert you to both the risk level and communication protocol level to which you should adhere.

Levels of Risk (as outlined in the CRCNA Security Manual) The following levels of risk may prevail:

- Level 1 – All personnel, living or traveling, encounter some normal risk such as parasites, tropical diseases, lax law enforcement, poor driving conditions, poor medical care, and so forth. This level would not include immediate political threats.
- Level 2 – This level involves situations where there is political unrest involving armed conflict, suspension of citizens' rights, and a breakdown of the normal safeguards that govern a civilized country. This may also include strikes, demonstrations, troop movement, and a general intimidation of the people by the government forces or rebel groups.
- Level 3 – This level exists when physical violence invades the "living space" of the person involved. It involves a risk that someone may "stumble into" a dangerous situation by mistake, ignorance, or imprudence, as when travel occurs at night in an area known to be the scene of armed conflict.
- Level 4 – This level involves situations where a member of a class of people is generally threatened. This may include all foreigners, all people working in a certain geographic or subject area, all those thought to be "against" one faction or another, or those who are at risk because of their identification with a type of work, such as a multinational organization. This grouping may be especially vulnerable to kidnapping.
- Level 5 – This level includes situations in which a person is specifically targeted for a threat, either directly (via a phone call or letter) or indirectly through actions (harassment by police, robberies to ransack files) or by rumors that intimidate, inhibit normal work patterns, and so forth.
- Level 6 – During a time of civil war, everyone lives in a high-risk environment. Under such circumstances there is no really safe position.

Any risk above level 1 demands an assessment of the advantages and disadvantages of evacuation of personnel and/or families. When levels 5 and 6 occur, staff can ordinarily no longer be effective in their work, and the risk of injury or death to them is clear. Therefore, at these levels staff will be evacuated.

VIII. Member care

A. The CRCNA recognizes that personnel who undergo traumatic events, as well as others associated with these events, can suffer emotional reactions that may become destructive if untreated.

B. Those involved in traumatic events will receive evaluation and, if necessary, intervention from mental-health professionals.

- This evaluation and intervention will be conducted confidentially with the objective being the treatment of existing trauma and the prevention of future trauma associated with the crisis.

- Personnel who are directly involved in a crisis shall receive initial and follow-up evaluations from a qualified Christian mental-health professional.
- These evaluations shall occur as soon as possible following a crisis and again six to twelve months following the crisis (unless otherwise specified by the mental-health professional).

While an ERT may note that member care is needed, it is the responsibility of the agency for which the personnel is serving to make sure that it is provided and to provide the necessary resources.

IX. Policies governing specific situations

A. Kidnapping, hostage-taking, or other extortion

1. Negotiation with kidnappers and hostage-takers

The CRCNA recognizes that hostage negotiations are a specialized and potentially dangerous activity. The CRCNA distinguishes between negotiations and payments or concessions in cases of kidnapping and hostage-taking. It is understood that negotiations can be conducted without necessarily obligating the organization to making payments or concessions that violate the values and policy of the CRCNA. It is also understood that negotiations, if they can be effectively and competently conducted, are the strategy of first choice in cases of kidnapping and hostage-taking.

In cases of kidnapping or hostage-taking of CRC members, personnel, or members of their families, their safe return shall be a priority of the organization. All reasonable effort consistent with the policy and core values of the CRCNA will be made to achieve their safe return. These efforts include hostage negotiation as a strategy of first choice. In cases where the CRCNA has the opportunity to negotiate for the safe return of hostages, advice and assistance is available and will be sought from Crisis Consulting International (See ~~Appendix J~~ the Tool Kit for more information). The liaison for the kidnappers will be the appropriate law enforcement authorities in U.S. or Canada or CCI.

Prior to their travel, all personnel traveling under the auspices of the CRCNA to countries other than Canada and USA are required to provide *"proof of life"* information to their designated contact and to their supervising CRCNA entity.

Note: Toolkit Item 5 provides the Proof of Life template; Toolkit Item 5 provides a First Contact Checklist in the event of a kidnapping

2. Payment of ransom and yielding to extortion

Because the CRCNA places a high value on the safety of its members, personnel, and their families, in cases of kidnapping or hostage-taking the CRCNA desires to take all reasonable steps to secure the safe release of the hostage(s).

In situations of kidnapping, hostage-taking, or other extortion no ransom shall be paid or concession made that is reasonably likely to cause or contribute to the probability that future similar events will occur.

An ERT is responsible for determining whether or not a proposed payment or concession complies with both the letter and spirit of this policy. If the ERT cannot reach a consensus with respect to a proposed concession, or, if a proposed concession would likely be viewed by the broader Christian community as violating the spirit of this policy, the proposed payment or concession shall be referred to the ED for decision before the proposed payment or concession being agreed to is made.

3. Family relocation

In cases of kidnapping and hostage-taking, family members will be relocated from the country of occurrence as soon as possible. This relocation will normally be to the home country of the family. In specific cases, the ERT may waive this policy if doing so is in the best interests of the crisis-management effort.

In cases where family relocation is ordered, the CRCNA will make ongoing support and assistance to the family a priority. This will include, but not necessarily be limited to, support in finding appropriate housing, school transfers, ongoing financial support, and similar matters. This will also include establishing a system to provide, regular, timely and accurate information to the family on the status of the case and the work of the ERT. This support will also include ensuring that adequate pastoral; emotional; and psychological help, including that of trained professionals, is provided.

4. Notifications to governments

In cases of kidnapping and hostage-taking, ideally the CRCNA, the embassy, and local governments should be contacted as soon as possible. The CRCNA recognizes that the local (host) government has authority and responsibility for such crimes that occur within the country. The CRCNA is also aware that the home government (government of citizenship) of the hostage(s) has a legitimate interest, and perhaps even legal jurisdiction, in these foreign kidnappings or hostage-takings of their citizens. However, it is recognized that in some of these cases, and in some countries, the involvement of governments may conflict with the objectives and values of the CRCNA.

The CRC will cooperate with legitimate government inquiries and activities in cases of kidnapping and hostage-taking when doing so is judged to be in the best interest of the hostage(s) and the CRCNA. The decision whether, when, and how to make such notifications to government agencies rests with the ERT.

B. Evacuations from host locations

1. Evacuation authority

Ultimately, the ERT has the authority to determine when and how an evacuation decision is to be made. This does not negate the possibility that an individual or family may decide that the safety and security levels of their situation are such that they no longer can work productively, whether or not there is an ERT appointed. When they make such a decision to leave after every effort to consult their supervisor prior to doing so, this is not considered an evacuation but an approved departure from duty from location of service. (See Appendix C concerning evacuation of national personnel.)

The process that an ERT takes to come to a decision for evacuation may involve a review of several factors including: the perspective of those closest to the situation and the information they have available that may not be known to personnel closest to the situation. Occasionally there may be a difference of opinion between personnel or between field and ERT when evacuation is necessary. In the end, the ERT decision shall prevail.

Decision-making authority to evacuate a particular individual or family ultimately rests with the ERT. However, a family or individual may decide to leave their place of work prior to an ERT decision when they deem unsafe conditions exist.

2. Evacuation criteria

The intention of this policy is to address those components of evacuation planning and decision-making that can be identified before a crisis occurs. Experience shows that training and contingency planning ahead of time will oftentimes make the difference between successful and safe evacuations and those that endanger members and result in unnecessary organizational disruption.

Each local entity will prepare and maintain evacuation plans for all personnel serving under its jurisdiction for when the risk level rises above level 1 (as defined in Appendix A). Copies of these plans shall be submitted to the home administrative offices of the agency involved (both Canada and the United States) and to the office of the DDM, where a reference copy will be maintained. These plans shall be reviewed, updated, and revised as needed—at least every year unless the CMPT grants an exemption from annual updating. If an exemption from annual updating is approved, the updating shall be done every second year. At a minimum, these plans shall include:

- A description of how the local entity will determine whether an evacuation is necessary, specifically identifying the decision-making authority and criteria to be used to make such a decision.
- A description of the notification system ensuring that all personnel receive necessary information before and during an evacuation.
- A description of the procedures the local entity will use, such as: means of transportation, evacuation routes and alternate routes, staging and destination sites, and communications procedures.
- The ready availability of cash in local currency, but also in U.S. currency or Euros, sufficient to cover costs to reach a safe destination (such as transportation, meals and lodging, and other anticipated expenses).

Each member or member and family shall prepare for two types of evacuation scenarios by identifying what would be taken with them and how they would accomplish an evacuation (e.g., method of transportation, routes, staging areas, and destination) for each of these circumstances:

- An evacuation with at least 24 hour's advance notice and in which a carload (persons and belongings) could be taken.
- An evacuation with one hour's notice and in which only those items that could be hand carried could be taken.

Each member/family's plan will be submitted to the local entity and maintained as an annex to that entity's evacuation plan.

C. Maintaining the security of CRCNA facilities

The CRCNA recognizes the need to continue the operation of its entities during an event that makes the normal use of facilities and equipment impossible or impracticable. All physical locations of CRCNA operations are to maintain plans to deal with both short and long-term facility impairment. These plans should include:

1. Plans for personnel and visitor safety at the time a catastrophic event occurs.
2. Arrangement for alternative work facility including the ability to support work from remote locations such as the employees' home, alternative office space, or other similar arrangement.
3. The maintenance of appropriate insurance coverage to enable restoration of ministry with reasonable financial impact.
4. Coordination with the Information Technology Department for the restoration and/or replacement of information and communication systems.

X. Post-crisis evaluation

It is the overall intention of this policy that:

- Every opportunity be taken to be better prepared and to improve the CRCNA's response to crisis situations so that the crisis can be resolved as rapidly and efficiently as possible. It is specifically not the intention of this policy to focus blame on any person.
- Each crisis be reviewed so that the strengths of the response can be identified, built upon, and repeated.
- Areas of weakness can be identified and remedied through allocation of resources, training, policy changes, or some combination thereof.

Within sixty (60) days of the resolution of a crisis or the completion of an ERT an evaluation of the incident must be conducted. The evaluation shall be made by an individual appointed by the ~~BOT~~ **Executive Director** and shall not be conducted by any person reporting directly to any other person whose actions in the crisis will be reviewed. A template for assigning such evaluation is found in the Toolkit Item 3.

The evaluation shall address causal factors in the crisis, initial response to the crisis, the performance of the CMT and the ERT, and the performance of all other denominational officials who had a part in the crisis. The evaluation shall address those areas of strength that should be repeated in a future crisis and those areas of weakness that should be remedied. The evaluation shall also identify any areas in which policy should be established or changed.

Revised November 2005
Updated September 2006
Revised February 2009
Revised May 2012
Updated February 2014
Updated September 2015
Updated May 2018

Appendix A: Levels of Risk

The following levels of risk may prevail:

- *Level 1* – All personnel, living or traveling, encounter some normal risk such as parasites, tropical diseases, lax law enforcement, poor driving conditions, poor medical care, and so forth. This level would not include immediate political threats.
- *Level 2* – This level involves situations where there is political unrest involving armed conflict, suspension of citizens' rights, and a breakdown of the normal safeguards that govern a civilized country. This may also include strikes, demonstrations, troop movement, and a general intimidation of the people by the government forces or rebel groups.
- *Level 3* – This level exists when physical violence invades the "living space" of the person involved. It involves a risk that someone may "stumble into" a dangerous situation by mistake, ignorance, or imprudence, as when travel occurs at night in an area known to be the scene of armed conflict.
- *Level 4* – This level involves situations where a member of a class of people is generally threatened. This may include all foreigners, all people working in a certain geographic or subject area, all those thought to be "against" one faction or another, or those who are at risk because of their identification with a type of work, such as a multinational organization. This grouping may be especially vulnerable to kidnapping.
- *Level 5* – This level includes situations in which a person is specifically targeted for a threat, either directly (via a phone call or letter) or indirectly through actions (harassment by police, robberies to ransack files) or by rumors that intimidate, inhibit normal work patterns, and so forth.
- *Level 6* – During a time of civil war, everyone lives in a high-risk environment. Under such circumstances there is no really *safe* position.

Any risk above level 1 demands an assessment of the advantages and disadvantages of evacuation of personnel and/or families. When levels 5 and 6 occur, personnel can ordinarily no longer be effective in their work, and the risk of injury or death to them is clear. Therefore, at these levels personnel will be evacuated.

volvement

Personnel working outside North America must use discretion in any involvement in the political processes of the host country. Their mission is to accomplish the purpose of the agency that sent them to the area. The purpose, integrity, and safety of all CRCNA personnel and their dependents may be threatened by involvement in the politics of a host country because one individual's personal actions are quickly linked to the organization to which the employee belongs.

Any person who is a CRCNA employee or volunteer:

- Will not in a premeditated manner jeopardize the CRCNA's work or endanger the lives of themselves or others through political involvement. Political Involvement includes activity that shows overt support for one political group to the detriment of the other.
- Will promote and maintain the effectiveness and integrity of the CRCNA's work by carrying out approved plans and strategies of the CRCNA.
- Will not be involved with intelligence-gathering activities in any way regardless of their purpose. Intelligence gathering would include covert actions such as getting and providing information on one of our partners for use by a political group

Appendix C: National Personnel* Evacuation

Even though expatriate personnel may evacuate, it is assumed that personnel contracted by the CRCNA and who are citizens of the country in which they work and in which a crisis has occurred, will stay in place – because they are in their own country. The following exceptions to this policy are recognized:

- National personnel's relationship to the CRCNA places them in specific danger;
- There is evidence that national personnel are specifically targeted with a threat endangering their life;
- A civil war, or collapse of governmental order, leaves them with no safe haven in their country.

In such exceptional situations, CRCNA personnel will, to the best of their ability, help national personnel to leave the area safely.

*As used here, *national personnel* does not include staff from local offices or partner organizations whose personnel budgets receive funding from CRCNA agencies.

Appendix D: Description of the Crisis Preparedness Team and the Role of Regional Monitors; Position Descriptions for Risk Assessment and Monitoring Coordinator, Training Coordinator, and Administrative Support Person

Crisis Preparedness Team

Mandate: To coordinate CRCNA work in three areas:

D. Regionally distributed security monitoring.
E. Compliance of CRCNA personnel with CRCNA crisis management and travel policies.
F. Preparedness for crisis of CRCNA information, human resources, communication, and electronic systems.

Accountability: To the CMPT through the CRCNA Executive Director, including authority to recommend appointment of monitoring and event response teams.

Composition: Risk Assessment and Monitoring Coordinator, Training Coordinator, and administrative support person as well as internal and external consultants as invited by the team.

Expectations: Monthly meeting of CPT and invited internal and external consultants; four to six interactions per year between CPT and Regional Monitors for updates from the Regional Monitors to CPT and from CPT to the Regional Monitors, and for discussions of security issues affecting CRCNA personnel (including volunteers). Where necessary or simply convenient, these meetings will be held or done electronically

Risk Assessment and Monitoring Coordinator: Responsible to receive and share as necessary information and requests from decentralized monitors. Primary connection for regional monitors and to the rest of the CRCNA for the Crisis Preparedness Team.

1. Convene/lead the Crisis Preparedness Team.
2. Convene the Regional Monitors and the CPT for interaction between four and six times per year for updates from the monitors to the team and from the team to the monitors, and for discussion of security issues affecting CRCNA personnel (including volunteers). Where necessary or simply convenient, these interactions will be held or done electronically.
3. Monitor compliance with CRCNA Crisis Management Policy, including currency and completeness of field security planning, proof-of-life declarations, and the like, and report as necessary to supervisors and CMPT.
4. Receive and share as necessary information and requests from decentralized monitors.
5. Serve as the primary contact for our crisis management provider (currently CCI).
6. Receive and monitor information from security services and forward it to the appropriate staff and leadership as necessary.
7. Maintain awareness of risk assessment/crisis preparedness policies and practices by participation in entities such as: Concillium, Risk Management Network, the Faith-Based Working Group of OSAC – recommending changes to CRCNA policies and procedures as indicated.
8. Assist identifying and selecting of Emergency Response Team (ERT) members. Work with agency directors to identify staff. Identify people willing and able to serve as translators\interpreters. Work alongside ERT to understand policies and communication protocols. Make sure that all communication is sent through the ERT and that the ERT establishes clear communication protocols.

9. Maintain contact with/participating in the Risk Management Network, Concillium, the FBOWG of OSAC, etc.
10. Oversee risk assessments for occasional CRCNA international travelers (such as: personnel of Ministry Support Services; EIRC; any others).
11. Communicate operational CMPT decisions to CRC entities, offices, and personnel, including the appointment and discontinuation of Monitoring teams.

Training Coordinator: Responsible to arrange training as specified by CMPT.

1. Arrange general crisis management training on an annual basis for CMPT and ERT members.
2. Identify and provide risk assessment/crisis preparedness/crisis management training for staff on a regular basis.

Administrative Support: Support the RACPT in monitoring compliance of CRCNA personnel with CRCNA Crisis Management Policy, including currency and completeness of field security planning, proof-of-life declarations, training, and the like.

1. Maintain readily accessible sources of information needed by CPT and in a crisis, including emergency contact information for CMPT members and for personnel qualified to serve on an Event Response Team (ERT).
2. Maintain a readily accessible setof current country-specific security management plans, noting the date of the last update. . These plans should be consistent with CRCNA policy and updated on a bi-annual basis.
3. Maintain a record of the location and submission date of proof-of-life declarations as required for personnel who travel.
4. Ensure availability of GPTS units. (Note: GPS coordinates should be included in evacuation plans.)

Additional Information

1. INTERNAL CONSULTANTS: Personnel designated by the directors of Information Technology, Human Resources, and Finance and Administration; and the personnel administering the volunteer programs of World Renew and Resonate Global Missions.
2. EXTERNAL CONSULTANTS: Anyone invited by the team who agrees to serve, including: medical, cyber-security, and physical security professionals; people deeply knowledgeable in a particular geographic area or other area of interest.

Relationship of the Crisis Preparedness Team to the Decentralized, Regional Monitors

1. The Risk Assessment and Monitoring Coordinator will convene the Regional Monitors and the Crisis Preparedness Team for interaction between four and six times per year for updates from the monitors to the team and from the team to the monitors, and for discussions of security issues affecting CRCNA personnel (including volunteers). Where necessary or simply convenient, these interactions will be done through electronic-conferencing.

2. Experienced security monitors in the CRCNA system may be invited by the team to coach one or more decentralized monitors and to join team meetings as invited.

3. Regional Monitors Task List

    a. Monitoring -- to be done individually, or within an interagency pair or group as determined by the directors of World Renew and Resonate Global Mission
        i. Daily monitor security concerns in their region (see possible sources list).
        ii. Analyze security trends.
        iii. Communicate concerns to in-region staff, supervisors, and monitoring coordinator as needed (or where a high level of concern exists or a new situation involving a high level of concern arises).
        iv. Request Monitoring Team (MT) or Event Response Team (ERT) as needed.
        v. Serve on MT or ERT as appointed by CMPT.
    b. Assessment and Planning
        i. Work with Risk Assessment and Monitoring Coordinator to make sure strategic and tactical risk assessments are conducted as needed.
        ii. Work with the administrative person to make sure country security and evacuation plans are updated as need.
    c. Training
        i. Participate in training/sharing events for Regional Monitors—anticipated biannually.
        ii. Work with Training Coordinator to provide staff in their region receive adequate security training.

4. Regional Monitors and Information Flow
    a. All staff will be informed of Regional Monitors and their tasks (ED email to all staff; Director email to all staff) [even non-WR and Resonate staff need to know of this change so that they can answer questions and communicate appropriately when needed.]
    b. All regional staff will communicate high level concerns or new situations involving a high level of concern to the Regional Monitor.
    c. Regional Monitors will communicate concerns to in-region staff, supervisors, and monitoring coordinator as needed (or where high level of concern exists or new situations involving a high level of concern arises).
    d. Monitoring coordinator will communicate high level concerns or new situations involving a high level of concern to the Regional Monitor and to staff as needed. [e.g., Regional monitor not accessible, extreme level of concern].

Crisis Management Tool Kit

TOOLKIT Item 1: Appointment of an Event Response Team

MEMO of _________ TO CRCNA PERSONNEL LINKED WITH _______

In light of the crisis and insecurity in ______, the CRCNA's Crisis Management Policy Team has appointed an Event Response Team (ERT) consisting of the following persons at the following emergency contact numbers:

1.
2.
3.
4.

Please note the attached CRCNA policy that governs the authority of the ERT. This policy must be followed by all CRCNA personnel that include all personnel, visitors, and volunteers appointed by the CRCNA offices (Canada and USA). Personnel appointed by the (country/national) office are governed by (country/national organization) operational policies for crisis and security management.

As you will note, the "ERT has exclusive responsibility for managing the crisis at hand. The ERT shall continue to exercise its responsibility until the crisis is declared to be over by the CMT upon recommendation of the ER. All other organizational groups or entities affiliated with the CRCNA are required to refer all crisis-related information to the ERT once it has been appointed. No action related to a crisis can be taken without the ERT's authorization, and no public statements related to the crisis can be made without the ERT's authorization."

To honor this responsibility, I would ask that you note these points for your information and action:

a. Travel to and from ______ as well as within ______ by any official CRCNA personnel must be approved by the ERT. Those, who travel without approval and/or travel against the advice of the ERT do so at their own peril and take complete personal responsibility for their own actions. Formal discipline procedures may follow at the agency level.

b. ________ as chair of the ERT will serve as the primary communication link for all CRCNA personnel in Canada and USA. ___________ will serve as the first channel for relaying information from the ERT to CRCNA personnel in (country) as well as relaying all vital information from the personnel in (country) to the rest of the ERT as soon as possible, at least daily updates.

c. All CRCNA personnel in _______ are requested to forward all official communication regarding the security of their situation to the ERT and not give direct reports to constituents without prior approval of the ERT. They are free to contact persons that are close to them (relatives, friends) via email, phone etc. provided these contact persons agree that all content of this communication will be treated as confidential and not for public use or consumption. If a Crisis Communication Task Force has been established, the CRCNA Director of Communication and Marketing provides the link.

d. Commit all of this to PRAYER without ceasing, praying that God's peace and justice may reign in _______ again!

TOOLKIT Item 2: Awareness of Risk Document

Program Name

***CHRISTIAN REFORMED* __________________________**

AWARENESS OF RISK,

CRC CRISIS MANAGEMENT POLICY

AND

COMMITMENT TO FOLLOW POLICY

We believe that God holds the entire world in his hands but that does not mean that we can or will avoid all risks. While this is true regardless of where Christians live and work, the risks in different countries may be more varied and unpredictable. Regardless of what measures are appropriately taken to provide a safe climate and secure working conditions, risks remain.

The Christian Reformed Church in North America (CRCNA) and Christian Reformed ______________ ______________ have tried to be as prepared as possible for any event that would endanger the lives of its personnel, including short-term volunteers and guests. This preparation includes the development of policies that have been approved by the Ministry Leadership Council (under the direction of the Council of Delegates) of the Christian Reformed Church. I have been given a copy of these policies, understand them, and am aware that CRC – Crisis Management Policy will guide _______'s handling of any crisis event that may occur.

While I judge that necessary precautions have been taken to avoid harm and endangerment of life, I understand and accept that some risk will be present during my participation with (Program name). Furthermore, in the event of a crisis, I agree to allow the CRCNA Crisis Management Policy to mediate/ resolve any and all crises, to support without interference the CRCNA's implementation of these policies, and to refrain from engaging in secondary involvement or negotiations. I have also asked my family to act in the same way.

Name (please print) ________________________________

Signature _________________________________ Date _________

Revised November 2005
Updated September 2006
Revised September 2008
Revised May 2018

TOOLKIT Item 3: Instructions and format for post-crisis evaluation

TO: Post-Crisis Evaluator

FR: Executive Director of the CRCNA

DT:

RE: Instructions and format for evaluation of crisis designated ____________________

It is the policy of the CRCNA that within sixty (60) days of the resolution of a crisis an evaluation of the incident must be conducted. The evaluation shall be made by an individual appointed by the CRCNA-BOT and shall not be conducted by any person reporting directly to any other person whose actions in the crisis will be reviewed. Thank you for agreeing to accept the board's appointment to serve as post-crisis evaluator for the crisis designated ____________________.

Please note three goals that lie behind the CRCNA policy of evaluating a response to a crisis:

A. To enable the CRCNA to prepare better for a crisis and to improve the CRCNA's response to crisis situations so that a crisis can be resolved as rapidly and efficiently as possible. It is specifically the intention of this policy not to focus blame on any person.

B. To identify strengths of the response so that they can be built upon and repeated.

C. To identify areas of weakness of the response so that they can be remedied through allocation of resources, training, policy changes, or some combination thereof.

Please address your report to the CRCNA-BOT through the Executive Director of the CRCNA by ________ _________. If you need information, clarifications, or resources to conduct the evaluation, please contact the office of the Executive Director of the CRCNA.

Please use the following outline for your report. If for any reason you deviate from the outline, please identify in a single section, all questions, recommendations, and suggestions.

TO: Executive Director of the CRCNA

FR: Your Name, Evaluator for the Crisis Designated ___________________________

DT:

RE: Post-crisis evaluator for the crisis designated _________________________________

1. Introduction to this report.
2. Causal factors in the crisis.
3. Initial response by any and all CRCNA entities and personnel to the crisis.
4. Report on the actions of the CRCNA Crisis Management Team with regard to the crisis and your evaluation of the team's performance.
5. Report on the actions of the Emergency Response Team with regard to the crisis and your evaluation of the team's performance.
6. Report on the actions of all other CRCNA officials who had a part in the crisis and your evaluation of these officials' performance.
7. Areas of strength of the CRCNA and the CRCNA's preparation for and response to the crisis that should be repeated in a future crisis or that built upon to strengthen the CRCNA's capacity to respond to a future crisis.
8. Identification of areas in which policy should be established or changed.
9. Whatever you judge merits saying that does not fit elsewhere.
10. Specific questions, recommendations, and suggestions (even if stated previously).
11. Any appendices you judge necessary (such as: people and written materials you consulted).

TOOLKIT Item 4: Process for Responding to Crisis Notification

PROCESS FOR RESPONDING TO CRISIS NOTIFICATION

The following outline provides a series of steps to be taken during a crisis event:

1. Notification to the ED is given by agency or personnel of crisis event.

2. The ED convenes the CMT as soon as possible upon receiving information that invokes this policy and that appropriate action is taken.

3. Some events, such as the kidnapping of CRCNA personnel, clearly require a crisis response. Other events, such as those involving organizational reputation, may be more difficult to assess. The ED and CMPT will ask the following questions in their assessment of these events:

   a) Could this be detrimental to our ministry on a large scale?
   b) Is there potential for negative media exposure?
   c) Will this damage our relationship significantly with one or more key audiences: donors, employees, local church leaders, classis, congregants, or partners?
   d) How will this event or issue play out over the next several days, weeks, months? Does this change the impact it could have on our ministry?

4. When the CMPT makes the judgment that there is a crisis in the making or when the CMPT declares a crisis to have developed, the CMPT shall nominate persons, normally at least three members, for appointment to an event response team (ERT).* The primary criteria for selecting the persons to be appointed is their ability, based on the best information available, to manage the crisis at hand. The CMPT shall submit its recommendation to the office of the ED.

   The ED shall make the official appointment of ERT members ~~on behalf of the BOT~~. The ERT shall have exclusive responsibility for managing the crisis at hand and the ERT shall be accountable to ~~the BOT thro~~ugh the ED. This buffers the CMPT and the rest of the organization from the crisis event so that the mission of the organization can continue during the crisis.

TOOLKIT Item 5: SAMPLE PROOF OF LIFE MEMO

TO: ______________________ and _________________________________

FR: ______________________

DT:

RE: "Proof of Life" Questions **[*sample* questions – USE QUESTIONS THAT ONLY YOU, OR THAT ONLY YOU AND SOMEONE VERY, VERY CLOSE TO YOU CAN ANSWER.** The answers to these questions need to be the sort of thing that it would be hard for anyone to know, or learn, without getting it from you, the hostage. Be careful that the information is not posted on the web, etc. **Absolutely do not take this list with you.** Entrust it in a sealed envelope with someone very close to you, and if possible with the director of finance and operations.

1. What was the name of the dog [or other pet] you had as a child?
   Ans:

2. What was the name of your third grade teacher?
   Ans:

3. What was the name of your fourth grade teacher?
   Ans:

4. What was the name of your fifth grade teacher?
   Ans:

5. What was a distinguishing feature of your fifth grade teacher?
   Ans:

6. What was your mother's mother's father's family name [or anything else about your family that will be very hard to track down]?
   Ans:

7. If the person is married, ask and answer a question about something that happened between them that was hard on their relationship (the sort of thing that neither of them wants anyone else to know).
   Ans:

8. Anything else that would be hard for anyone to know, or learn, without getting it from the hostage. Be careful that the information is not accessible on the web, etc.

______________________________ ______________________________

Your signature Handwritten date

TOOLKIT Item 6: Crisis Consulting International Guides for Kidnapping Situations

Kidnap First Contact Checklist

NOTE: This checklist is NOT intended to serve as a plan for conducting a kidnap or hostage negotiation. Such negotiations should ALWAYS be conducted by or under the direction of trained professionals. Contact CCI for more information. This checklist is intended to be used by call-takers or others who may receive an initial call from a kidnapper or hostage-taker. It should be used to help recipients of such calls "get through" the call while setting the stage for the beginning of professional negotiations.

1. *Who should be prepared to receive a first call from kidnappers?*

   A number of people are potential recipients of these first calls. The kidnappers will generally make this first call in one of three ways: They will have already ascertained who they think they want to negotiate with and call there; they may ask the hostage who they should call; or, they may just instruct the hostage to call "someone" (a family member, someone from their organization, etc.). This means that a number of people need to be prepared to receive such a first call; including at least:

   a. *Whoever handles incoming calls at the office or workplace of the hostage (both in the host country and in the headquarters country).*

   b. *The hostage's supervisor, manager, department head, organization CEO (both in the host country and in the headquarters country).*

   c. *A partner or colleague of the hostage, especially one listed in mobile phone contact lists, etc.*

d. *Close family members of the hostage, both in the host country and back in the hostage's home country.*

2. *How should the recipient handle a first call from kidnappers?*

a. First, remain calm and control your voice and emotions (at least the external display of emotions). You may be talking to a kidnapper or to the hostage. Either way, their call is scripted and controlled and their first goal is to put you on the defensive and scare you. Remember that those are merely tactics – do your best not to show any response to anything unpleasant or threatening you hear. Kidnappers frequently use scare tactics to try to get the first call recipient to agree to things or make concessions that cannot later be accommodated. The more "reaction" a kidnapper gets to threats, etc.; the more he feels like that tactic works and the more often he will use it.

b. Keep a contemporaneous log of what was said (as close to verbatim quotes as can be accomplished), what background noises were heard, etc.

c. Do NOT ask for demands or deadlines to be repeated unless you really did not understand what was said. Asking for repetition can "set" the threat or deadline in the perpetrator's mind.

d. Do NOT agree to anything. Say that you are only answering the phone and that you don't have authority to make decisions. Say that you will pass on all of the information to someone who is authorized to speak to them. Try to avoid using the term "negotiator" unless they use it first – if they do, then tell them that you are only authorized to pass on what they tell you to the negotiator.

e. Ask how the hostage is – refer to him or her by name(s). Ask to speak to them. This will probably be denied, but you never know… If you speak to a hostage, ask:

i) *"Are you injured?" (Don't ask "how are you?" as that almost always gets a non-specific answer such as "fine" or "OK". If the answer to "are you injured?" is affirmative, ask followup questions to determine how serious the injury is and if any medical attention is being provided.*

ii) *"Is anyone else injured?" (if there are other hostages). If the answer is affirmative, ask the same followup questions.*

iii) *If more than one hostage was taken, ask if they are all together – try to use first names (e.g., "are you still with Paul and Jane?"). If the answer is negative, ask if he/she knows where they are.*

iv) *"Can you tell me who has you?"*

v) "Is it safe for you to tell me where you are?"

If you are not allowed to speak to a hostage, ask "is anyone hurt?" Keep the question open like this, as useful information may be gained by the response (if kidnappers were hurt, for example).

f. *Especially if you are being given complex or unclear instructions, you can ask for them to be repeated and you can say that you are writing them down to make sure you have it right. Except for threats, demands and deadlines, it is OK to read them back to the caller to make sure you've understood correctly.*

g. Try to determine a schedule for the next contact. Tell the callers that you need some time to contact the person authorized to talk to them, tell them what you've been told, and get them in position for a call. If the kidnappers do not suggest a time, or give you the option, suggest 24 hours from now (i.e., 24 hours from the time of this first call). That may seem like a long time, but for many reasons that is to our advantage.

2. If there are no demands, threats or deadlines offered by the caller, DO NOT ask anything about any of these topics. We'll hear soon enough, and time is on our side.

3. "All purpose help phrases":

a. *If there is a lot of screaming and yelling:*

i) "I'm sorry but its so loud that I cannot understand you well"

ii) "I'm sorry but there is a lot of noise in the background and I cannot hear you clearly"

b. *If there are threats that are being repeated or you are being asked specifically if you "heard" the threat:*

i) *"I understand what you said and I will pass that on. But I'm sure that a resolution is possible."*

ii) *"I understand what you said but I have no authority to do anything in this matter so I will pass on what you have said."*

iii) *"We are just starting this process so that (threat) is not necessary. I'm going to pass on everything you have said and the proper person will be speaking to you."*

c. *If the caller insists that you acknowledge a demand or make some kind of agreement ("you must do this RIGHT NOW or I will kill the hostage – DO YOU UNDERSTAND??!!"):*

i) *"Sir (unlikely that it will be a female caller) I understand what you have said and I am going to tell the persons in authority. I am not allowed to make any decisions at all – that is for the persons in authority, but I will make sure that they understand clearly everything you have said."*

ii) *"Because I have no authority, if I agreed with you I would be making an agreement I might not be able to keep and that would be disrespectful to you. I can only tell you the truth and that is what I'm doing. I have no authority to make any decisions but I will tell those who do exactly what you have told me."*

As you can tell, there is a general "theme" that runs through these statements, and it is repetitive. That is intentional and is designed to protect the call-taker, show respect to the kidnappers, and set the stage for the initiation of professional negotiations. It is perfectly OK to keep repeating a relevant statement as many times as necessary. Adding things like "I can only tell you the truth – I will not disrespect you by saying something I have no authority to complete" is fine.

4. *As soon as the call is completed, the person who receives the call should complete a history of the call. This is intended to capture as much information as possible while the call is still fresh in the person's mind. The template attached to this checklist is recommended for this purpose.*

5. *Beyond the scope of the first call, subsequent contacts should always be conducted by or under the direction of a professional hostage negotiator. One of the basic principles that will be used is to convey that negotiations will only occur for a living hostage, and that proof of that will be required. NOTE: There are specific tactics for conveying this message, and there are definitely right ways and wrong ways – even dangerous ways - to do it. This is* ***just one*** *of the reasons that professional assistance is needed.*

For more information, or for assistance in dealing with a kidnapping or hostage-taking, contact:

Crisis Consulting International

9452 Telephone Rd., No. 223

Ventura, CA 93004

United States of America

Telephone 805.642.2549 (staffed 24/7/365)

Facsimile 805.987.5192

Email info@cricon.org

Internet www.CriCon.org

CALL-TAKER’S NOTETAKING TEMPLATE

IMMEDIATELY AFTER RECEIVING THE CALL ANSWER THE FOLLOWING QUESTIONS:	
Name and telephone number(s) of staff member who received the call:	
What time was the call received:	
What number or line was called?	
Did the caller ask for a specific person, office, etc,?	
Was the caller male or female?	
How old did the caller sound?	
What language did the caller speak?	
Did you detect any accent? What accent?	
Could you tell the most likely nationality of the caller?	
Could you tell the most likely ethnicity of the caller?	
What was the emotional state of the caller? Calm? Excited? Angry?	

Frightened? Uncertain?	
What was the rate of speech? Slow? Normal? Rapid? Excited?	
What was the volume of the speaker’s voice? Soft? Normal? Loud?	
What was the voice quality of the caller? Nothing unusual? Slurred? High-pitched? Deep? Sincere? Rational? Irrational? Calm? Angry? Profane? Religious?	
Did the caller use any foreign words or terms? Technical words or terms? Slang or jargon?	
Did the caller’s voice sound familiar?	
Who is the person you know whose voice sounds most like the caller’s?	
Did you hear any background noises? Voices? Traffic? Other?	

Write down, as closely to verbatim as possible, what the person said; paying particular attention to any slang, unique phrases or unusual statements:

(use as many pages as needed)