Crisis Communication Plan

(Your Agency Information Here)

## Provided Courtesy of OnSolve

the market leader in cloud- alerts based communication and collaboration tools capable of delivering critical notifications and.

Executive Summary 3

Glossary 3

Cautions 3

The Team 4

Team Members 4

Team Activation Procedures 4

Team Assembly at Crisis Communications Center 4

Threat Assessment 5

Define Crisis and Incident Scenarios 5

Assemble Collateral Materials 6

The Audiences 7

Identify Audiences 7

Establish Notification Process/System 7

Set Up Monitoring Channels 7

Create Your Voice 8

Name and Train Spokespersons 8

Create Quick Response Press Releases 8

Create Press Release Templates 8

Crisis Communications During an Incident 9

Emergency Response 9

Communications Team Activation 9

Situational Assessment 9

Refine Messaging 9

Procedures for Event Duration 10

After the Crisis 11

Crisis Communication Plan Maintenance 12

Test 12

Train 12

Plan Review 12

Executive Summary

(Include the agency’s mission statement)

(Explain the agency’s responsibilities)

(Tell about the purposes of the Crisis Communication Plan. Examples include:

* Keeping communications effective with employees and stakeholders
* Being readily available to news media
* Quicker assessment of messaging needed
* Extending empathy to affected people
* Keeping information secure
* Keeping audit trails intact
* Having multiple channels of communication
* Eliminating dependency on paper
* Quicker crisis communication response times
* More accurate messaging and better control of messaging
* Maintaining trust
* Purposes unique to your organization

(Explain how the CCP fits in with the agency Disaster Preparedness Plan and tell how it streamlines inter and intra-agency coordination. Also include descriptions of what constitutes a crisis and what constitutes an incident.)

Glossary

(Define words, phrases and acronyms used throughout this document.)

Cautions

(Reinforce the importance of proper early reporting to other authorities (fire, police). Include cautions about withholding and delaying information. Here is also where you include notes about truthful disclosures and how to report information breaches and dishonest disclosures.)

1

The Team

Team Members

(Name the team members. Include title, functional responsibilities, and other desired pertinent information that helps to identify them and that supports them in their role.)

Team Activation Procedures

(Describe scenarios when the team is activated and tell how that happens. If using an emergency notification system, tell how and where it is maintained, who initiates its use and other information on activating it. Provide any identifiers for the team notification feature. If using other types of notifications, name them and describe how they function and who initiates.)

Team Assembly at Crisis Communications Center

(Tell exactly how the team should know where to assemble once notified. Tell parameters for using an alternate location. Explain the initial communications setup so team members know what tools they will have available. Tell how team members can get communication tools if those described are missing, or if they need additional resources. Tell the locations of supporting materials like brochures, and fact sheets. Also indicate names of people primarily responsible for keeping communications tools and collateral materials up to date and available. Include other directions that provide a complete description of the team assembly area/s. Assign responsibility for maintaining the materials needed in the communications center.)

2

Threat Assessment

Define Crisis and Incident Scenarios

(Explain the process you use to define crises and incidents requiring a communications response. Specify the responses for each scenario. To be most thorough, describe potential cascading events and sub scenarios, and plan responses to them.)

| Scenario | Sub or Cascading Events | Collateral Resources | Response |
| --- | --- | --- | --- |
| Bomb Threat | 1. Public Panic
2. Multiple Escape Injuries
 | 1. Building Exit Plans
2. Employee Locator
 | IPAWSEmergency Notification SystemOn-site Triage AnnouncementsMedia Talking PointsSpokesperson |
| Tornado Touch Down |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Assemble Collateral Materials

(During the threat assessment you specified collateral materials that are used as additional information to support your efforts and to provide information to your audiences. Now, you list and assemble those here. Include locations and who is responsible for maintenance and updates. Specify the digital location of the materials.)

* Brochures
* Fact Sheets
* Contact Information
* Materials that simplify explanations about the agency, its mission, its leadership
* Materials that help with explanations and evacuations, like blueprints and building directories
* Agency wiring diagrams
* Inter and intra agency relationship diagrams

3

The Audiences

Identify Audiences

(Create a detailed list of all audiences you’d likely need to include in messaging. This is based on your threat assessment, but there are audiences that will be universally appropriate to include. A starter list might include:)

* Other public agencies
* The public
* Insurance and banking
* News Media
* Businesses
* Elected officials
* Regulators
* Affected persons
* Affected community

Establish Notification Process/System

(Explain the notification processes and the systems to use. An emergency notification system should allow you to contact people in multiple ways so if one contact method doesn’t work, you can continue trying to reach the person using other contact methods. You need to set up a system that helps you to quickly and easily select specific groups of people for notification. Your notification system should be easy to test, so you can regularly confirm the contact information of the people who have opted in. This is also the place to list the people who have access to the IPAWS, and to explain its capabilities and use cases that align with your agency responsibilities and your threat assessment.)

Set Up Monitoring Channels

(Explain the platforms and systems you will use for listening to your audiences. On the digital front, these might include social media analytics tools and automatic searches using Google Alerts, or search agents and bots. Tell about person-to-person efforts you use to connect with your various audiences and to stay in touch with them in non-crisis times.)

4

Create Your Voice

Name and Train Spokespersons

(List experts and spokespersons according to their specialties. Tell how they fit in with your threat assessment scenarios. Explain the training modules you’ve set up covering best practices for communicating with the various audiences. List the training modules you’ve set up for experts and spokespersons that directly relate to the threat scenarios they would be called in for. Include a training schedule and rehearsals so experts and spokespersons can regularly practice their roles. Show the physical locations for all these assets and specify who is responsible for monitoring and maintaining them.)

Create Quick Response Press Releases

(List the short, early response press releases you’ve written up for each of the threat scenarios. List any standard templates with fill-in blanks that you’ve created to use across multiple incidents. These acknowledge the incidents without much detail, so audiences know your awareness of events. List these asset locations, and who is responsible for maintaining them.)

Create Press Release Templates

(List the press release templates you’ve created for the threat scenarios and that anticipate the information you would need to release. List these asset locations, and who is responsible for maintaining them.)

5

Crisis Communications
During an Incident

Emergency Response

(Specify the actions to take for the members of the crisis communications team at the onset of a crisis or incident. This is when gleaning information about the team’s crisis center and agency assets are critical. Establish processes for creating a timeline of events, and for gathering information about first response and conditions of agency people and property. Specify backup options for the team if team members are missing, injured or not able to perform their duties. Outline activities team members might perform to help preserve life and property. Depending on the length and severity of the crisis the team might not get activated. Specify chain of command within the team so leadership is always clear regardless of the number of team members available. Reveal other plans and specify other actions for the team members during the very early stage of a crisis.)

Communications Team Activation

(Define timeframes for activation and team member requirements for various threat scenario intensities. Describe shelter-in-place practices. Include other procedures like special notifications that are unique to your organization.)

Situational Assessment

(Detail the processes to use when assessing the incident from a communications perspective. Specify the order of notifications to the various audiences, and the conditions requiring press releases, spokesperson talking points and collateral materials that match the threat scenario. Outline process for disbanding and reassembling if the team itself comes under threat.)

Refine Messaging

(Outline team process for deciding what messaging to use and the venues to use to disseminate information and messaging. Describe an example scenario and show how the messaging is adjusted to the scenario and then to the various audiences. Specify spokesperson activities based on the incident threat level.)

Procedures for Event Duration

(Define the team objectives for the remainder of an incident. Address team staff levels based on changing threat levels. Outline response times for new messaging and process for tracking and assessing the situation. Outline scenarios for disbanding the team as threats go down. Detail how information and data is saved for post incident analysis.)

6

After the Crisis

(Provide the details and locations of data and information that arose from the incident. Detail how the information and data is handled, chain of custody and persons who participate in analysis. Assign responsibility for preserving and archiving information and data. Detail the various reports and timeframes for completion. Set up templates for sorting information that single out problems and highlight what worked. Assign functional responsibilities for addressing problems and for incorporating what went right into best practices. Set up reviews with the entire team for brainstorming on how to improve and to recognize successes.)

7

Crisis Communication
Plan Maintenance

Test

(Create exercises to test the team’s response, accuracy and timeliness. Set up testing schedule and exit evaluations. Assign responsibilities for creating, reviewing and maintaining exercise scenarios.)

Train

(Set up training for new team members and refreshers for veteran members. Establish a training schedule. Assign responsibilities for assessing training needs and creating training modules. Set up regular review of training by team members to identify weaknesses and strengths.)

Plan Review

(Set up functional responsibilities and schedule for plan review. Name stakeholders in review, evaluation and revision of the crisis communication plan. Establish review of CCP functions within the broader ICS.)

SOURCES:

http://www.dpworkshop.org/workshops/management-tools/disaster-preparedness/communication

https://www.bernsteincrisismanagement.com/the-10-steps-of-crisis-communications/

http://www.niu.edu/newsplace/crisis.html

https://icma.org/articles/crisis-communication-planning-e-book-local-government