



Social Media Crisis Management and Communication Plan Template

Purpose

Define the purpose of this document. Highlight when this should be referenced and what kind of information and references will be outlined.

Escalation Framework

Use this framework below to determine the severity of a crisis.

In the "description" column, describe what constitutes that definition of a crisis and what actions must be taken in response. Also, include a few examples of what that crisis would look like.

In the "action" column, mention teams or individuals who may take action, such as legal, the PR & communications team, customer marketing, the social media team, executive assistants, the C-suite, account managers or executives, and more.

Level	Description	Action
Level 1	<p><i>This is the highest level of crisis escalation and should involve an all-hands-on-deck approach. Describe this situation as immediate to your customers, partners, employees, and/or all stakeholders.</i></p> <p><i>Examples: list the examples of this level. Typically, they involve violence, executive misconduct, or a long-term threat of damage to your customers, the company and/or stakeholders.</i></p>	<p><i>Person/Team #1: Task or action</i></p> <p><i>Person/Team #2: Task or action</i></p> <p><i>Person/Team #3: Task or action</i></p>

<p>Level 2</p>	<p><i>Level 2 presents a moderate potential risk or impact on business operations, customer success, and/or company reputation.</i></p> <p><i>Examples: list the examples of this level. These may include the risk of immediate major customer churn.</i></p>	<p>Person/Team #1: <i>Task or action</i></p> <p>Person/Team #2: <i>Task or action</i></p> <p>Person/Team #3: <i>Task or action</i></p>
<p>Level 3</p>	<p><i>This is unlikely to pose a long-term risk to or impact business operations, customer success, and/or company reputation, but the team should still be on the same page for responding.</i></p> <p><i>Examples: instances can include an executive leave of absence, a moderate customer impact that can easily be (or already has been) remedied, or rumors (such as a merger/acquisition).</i></p>	<p>Person/Team #1: <i>Task or action</i></p> <p>Person/Team #2: <i>Task or action</i></p> <p>Person/Team #3: <i>Task or action</i></p>
<p>Level 4</p>	<p><i>This is where most "crises" will fall into. They tend to be slightly bigger versions of day-to-day issues that may need a bit of extra effort to be fully resolved or addressed.</i></p> <p><i>Examples: Some examples include a short outage with no impact on support or an angry customer on Twitter.</i></p>	<p>Person/Team #1: <i>Task or action</i></p> <p>Person/Team #2: <i>Task or action</i></p> <p>Person/Team #3: <i>Task or action</i></p>

Incident Response Team

Describe the purpose of this team, why it was assembled, and what it is responsible for doing.

First Line of Defense

Identify the key players to be informed once the company is aware of the crisis. The list should include the names of the individuals, the team/department those people are members of, and how to best communicate to each member individually. If there is an internal chat system or group email for the whole team, list that here as well.

- Person/Team #1: Email and/or Phone Number
- Person/Team #2: Email and/or Phone Number
- Person/Team #3: Email and/or Phone Number
- Person/Team #4: Email and/or Phone Number
- Group Email/Communication Method: List Here

Greater Response Team

Indicate which escalation level will involve the Greater Response Team. Additionally, list out the core departments that comprise the Greater Response Team, and if appropriate, note that other departments or individuals not listed below may be brought in as needed. Teams that make up a greater incident response team may include the following:

- Communications
- Customer Support
- Legal
- Partner Communications
- Social Media
- Customer Marketing
- People Ops and HR
- Product/Engineering
- Executives
- Security

Roles and Responsibilities

In a general crisis – regardless of escalation – what should each of these departments be responsible for once informed of the crisis? Feel free to add a row to include any other department that is right for your business.

Team	Contact Name	Roles and Responsibilities
Communications	Name	● Example Responsibility
Customer Support	Name	● Example Responsibility

Legal	Name	● <i>Example Responsibility</i>
Social Media/Marketing	Name	● <i>Example Responsibility</i>
HR	Name	● <i>Example Responsibility</i>
Product/Engineering	Name	● <i>Example Responsibility</i>
[Other Department]	Name	● <i>Example Responsibility</i>

Crisis Management Process

Phase 1: ALERT

Outline the actions necessary to ensure the response team is notified as soon as possible. Emphasize that if someone is unsure if he or she should alert the team to alert the team that he or she should, just in case.

Your alert system can be as simple as an internal chat system channel or email alias.

Phase 2: ASSESS

Once the Response Team has been notified, what happens next? Explain how the team will assess the (potential) crisis, gather any available information, classify the incident via the escalation framework above, and prepare to take subsequent action.

Here are some questions to answer to get you started:

- What happened
- Where and when?
- Who was affected?
- Who is involved?
- When did we learn about the incident?
- What is the impact/likely impact?
- Is there any immediate danger?
- Do we understand the entire issue?

Phase 3: ACTIVATE

Turn your plan into action. Explain how the response team will communicate with the appropriate team members for their tasks and/or with external stakeholders for specific messaging.

In the box below, write out a few common tasks expected in a crisis situation, and delegate that task to a responsible party in the form of a department or an individual. These tasks could include incident response team communication, initial external messaging, gathering/monitoring information, finding a meeting space, team check-in cadence, etc.

Action Items	Responsible Party
<i>Example Action</i>	<i>Responsible Party</i>
<i>Example Action</i>	<i>Responsible Party</i>
<i>Example Action</i>	<i>Responsible Party</i>
<i>Example Action</i>	<i>Responsible Party</i>
<i>Example Action</i>	<i>Responsible Party</i>

Phase 4: ADMINISTER

Determine how the Incident Response Team will continue to assess, address, and resolve the incident. Once again, the type, scale, scope, and severity of the incident or crisis will determine the response. Tasks include communication to stakeholders, employees, and customers if appropriate, as well as developing a timeline, seeking external legal or technical assistance, moderating and responding to media, and updating your crisis communication plan. This section should address the steps for any crisis, whether long-term or short-term.

Action Items	Responsible Party
<i>Example Action</i>	<i>Responsible Party</i>
<i>Example Action</i>	<i>Responsible Party</i>
<i>Example Action</i>	<i>Responsible Party</i>
<i>Example Action</i>	<i>Responsible Party</i>

<i>Example Action</i>	<i>Responsible Party</i>
-----------------------	--------------------------

Part 5: ADJOURN

Once the immediacy of the crisis has dissipated, regroup as a team to go over your process for crisis management, response, and communication. Consider what changes should be made and update this plan with those changes.

Additionally, someone should take point on documenting exactly what the process was for this crisis, alongside any successes, learnings, or shortcomings. The team should work together to grade themselves on how this situation was handled using a self-review template included in your download.

Finally, if any outstanding issues need to be addressed, or if further monitoring of communication/media is necessary, delegate individuals or departments to manage those tasks.

Action Items	Responsible Party
<i>Example Action</i>	<i>Responsible Party</i>
<i>Example Action</i>	<i>Responsible Party</i>
<i>Example Action</i>	<i>Responsible Party</i>
<i>Example Action</i>	<i>Responsible Party</i>
<i>Example Action</i>	<i>Responsible Party</i>

Do's and Don'ts

What are the best practices for your crisis communication? During these times, it can be stressful and easy to jump to a decision that could cause more harm than good. Outline the do's and don'ts for crisis management below.

DO'S	DON'TS
------	--------

<input checked="" type="checkbox"/> Example Do	<input type="checkbox"/> Example Don't
Example Do	Example Don't
Example Do	Example Don't
Example Do	Example Don't
<input checked="" type="checkbox"/> Example Do	<input type="checkbox"/> Example Don't

Maintaining an Effective Response Plan

To help ensure your company's crisis communication plan will be effective and current, take steps to keep the plan fresh and test your team's ability to manage a crisis. This means editing this plan as needed, running mock-crisis war rooms on a set cadence, and developing a training program for all members of the crisis communication team. Outline those processes in this section.