

Business Continuity Toolkit

Crisis Management Plan Template

*The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.*

Document review and approval

Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Date | Revision |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

This document has been approved by

|  |  |  |
| --- | --- | --- |
|  | Approver name | Date approved |
|  |  |  |
|  |  |  |

Contents

[1 Purpose 4](#_Toc64979398)

[2 Scope 4](#_Toc64979399)

[3 Plan possession 4](#_Toc64979400)

[4 Crisis management roles & responsibilities 5](#_Toc64979401)

[5 Crisis management procedures 7](#_Toc64979402)

[Detection, response & initial assessment 8](#_Toc64979403)

[Activation (crisis situation declaration) 8](#_Toc64979404)

[Supporting incident/emergency response 8](#_Toc64979405)

[Recovery for critical business activities 8](#_Toc64979406)

[Review and learning (post-crisis) 8](#_Toc64979407)

[6 Command center setup & operation 9](#_Toc64979408)

[7 Continuous monitoring 9](#_Toc64979409)

[8 Communications 10](#_Toc64979410)

[9 Appendix 1 – contact information list 11](#_Toc64979411)

[10 Appendix 2 – pre-prepared media statements 12](#_Toc64979412)

# Purpose

The purpose of this crisis management plan (CMP) is to provide guidance and documented procedures to assist the crisis management team (CMT), who is responsible for coordinating the organization-wide response to crises and business recovery activities.

The CMP procedures and measures are intended to protect the people, assets and reputation of the organization, in addition to minimizing other negative impacts that may arise from various crises.

The CMP applies to events that prompt the activation of the CMT to lead, support and guide the organization through a crisis situation that impacts the organization. The CMP is to be activated when a crisis or situation has the potential to escalate beyond control and cause significant negative impact to the organization and its stakeholders, or cause economic / financial loss above acceptable financial thresholds.

# Scope

The CMP is intended to guide the response and recovery from significant disruptions that impact the continuity of the organization’s critical services and activities, including the following situations:

* Intentional acts, e.g., cyber-attack, labor strike/protest, physical vandalism/attack, theft of critical assets
* Accidental events, e.g., fire / explosion, equipment/hardware malfunction, power failure, chemical/hazmat spill, software malfunction, supplier failure/bankruptcy, industrial accidents
* Natural hazards, e.g., epidemic/pandemic, snowstorm, earthquake, hurricane, flooding / tidal wave, extreme cold temperatures.

In addition to this CMP, the following plans exist to support response and recovery activities:

* Emergency response plans to mitigate damage and respond to emergency situations, e.g., fire evacuation or response to cyber-attacks
* Business continuity plans to recover business processes
* IT disaster recovery plan to recover IT systems and communications.

# Plan possession

All personnel identified in section 4 as having crisis management responsibilities will have a copy of the latest version of this CMP through SharePoint access and either printed copies or digital copies on encrypted USB storage devices.

# Crisis management roles & responsibilities

The CMT provides the necessary expertise to deal with a wide range of negative events impacting the organization, and includes representation across all business lines and domains. Therefore, the composition of the CMT is flexible to adapt to the different types of crises requiring the participation of different support and business areas.

The CMT Lead will determine the most adequate team to deal with each disruption and can expand or reduce the team as appropriate.

The following table presents the roles and responsibilities of the CMT members:

| Role | Responsibilities | Primary | Alternate(s) |
| --- | --- | --- | --- |
| CMT Lead | * Review CMT membership requirements for an appropriate response, and if necessary, appoint additional members/advisors
* Declare a crisis situation in coordination with the business continuity coordinator
* Direct CMT members to the crisis command center or establish contact with them if meeting in the center is not possible
* Chair the CMT meetings and direct the overall response to the crisis.
 | *<Add>* | *<Add>* |
| Crisis Coordinator(same as business continuity coordinator) | * Support the classification of event severity and notify the CMT Lead
* Communicate with CMT members the details of the command center, as directed by the DMT Lead
* Advise the CMT of the affected critical business processes, the resources required for recovery and on the available recovery options, in order to support the prioritization and mobilization of available resources
* Coordinate with business recovery leads and activation of their business continuity plans.
 | *<Add>* | *<Add>* |
| Communications Lead | * Participate in CMT meetings when requested by the CMT Lead
* Direct all external communications with media outlets, social media responses and other third parties (customers, vendors, etc.)
* Direct all mass internal communications
* Oversee the refinement of the communication strategy during the crisis and list of stakeholders to communicate with
* Oversee the monitoring of media coverage
* Suggest and approve informational content.
 | *<Add>* | *<Add>* |
| Information Technology Lead | * Participate in CMT meetings when requested by the CMT Lead
* Coordinate technology and communications recovery activities (IT disaster recovery) and provide regular updates on progress
* Provide details on incident response progress for IT operational disruptions or cyber-attacks
* Coordinate with technology service providers.
 | *<Add>* | *<Add>* |
| Human Resources Lead | * Participate in CMT meetings when requested by the CMT Lead
* Ensure that employees and their families are updated on relevant information regarding the incident/emergency, whenever it affects their well-being and safety
* Ensure that employees affected by the incident/emergency receive the care and follow-up required.
 | *<Add>* | *<Add>* |
| Legal Lead | * Participate in CMT meetings when requested by the CMT Lead
* Provide legal counsel to the CMT and arrangements for external legal support as necessary
* Evaluate decisions with regard to legal consequences.
 | *<Add>* | *<Add>* |

# Crisis management procedures

Although each incident/emergency is unique and requires a specific response, the following criteria guides the teams on how to classify these events into ‘Low’, ‘Moderate’ and ‘High’ severity crises, and escalate them accordingly to the CMT. Scenario-specific response procedures are covered in the respective incident/emergency response plans.

**Incident classification**

|  |  |
| --- | --- |
| **Severity** | **Definition** |
| Low | * Potential or actual incident which does not materially affect business operations
* Limited media coverage
* Response is managed by operations teams.
 |
| Moderate | * Incident is localized to one site with limited impact on business operations
* The situation is attracting minor media response and minimal social media attention
* Response is managed by incident/emergency response teams.
 |
| High | * Major incident/emergency requiring intervention from local authorities
* Broad coverage in traditional and social media
* Response is managed by incident/emergency response teams and local civil defense authorities
* Senior management intervention and external communications required.
 |

**Business resilience flow**

The following diagram illustrates the flow from detection to recovery:

****

Detection, response & initial assessment

Incident and emergency response teams are the first to detect or be notified of a disruptive event and are responsible for the initial assessment and response, following their pre-defined incident and emergency response plans

Following the initial assessment and damage control procedures, the team will assess the disruption effect on employee’s health and safety, assess damages on facilities and information systems and estimate the time for resolution and return to normal operations, and report to the business continuity officer/coordinator.

Activation (crisis situation declaration)

The business continuity officer/coordinator will reassess the event severity based on the available information and decide if the event can me contained by coordinating and monitoring the resolution until operations return to normal (low/moderate events), or escalates it to a high severity event which requires activation of the CMP.

Upon activation, the business continuity officer/coordinator will notify the CMT Lead and issue communication to all required CMT members, who are required to attend depending on the relevance of the crisis to their domain.

See section 6 below for the command center setup procedure.

Supporting incident/emergency response

During the response phase, the CMT will focus on containing the immediate impacts of the disruption in order to ensure the well-being and safety of organization’s employees and protect the organization´s assets.

The CMT will manage all communication with internal and external stakeholders, other than urgent alerts and warnings that are issued by emergency response teams.

Recovery for critical business activities

The CMT will notify personnel responsible for business recovery to activate their business continuity plans, oversee the recovery efforts and obtain periodic updates.

The CMT will also approve major deviations from documented plans and approve incremental funding requests that are needed to support recovery efforts.

Review and learning (post-crisis)

Following the crisis, the CMT Lead will appoint a team to perform a post-crisis review in order to evaluate the effectiveness of the response, including plans, procedures, tools and facilities to identify areas for improvement.

As a result of the evaluation and the lessons learned, the appointed team will issue recommendations for corrective and improvement actions and will develop an action plan with appropriate teams defining the responsibilities and timelines to ensure they are carried out.

# Command center setup & operation

Once a crisis situation is declared, the CMT Lead will activate the crisis command center to ensure that the required meeting space and logistics are available for the CMT to convene. The command center may be virtual or physical.

Physical command center details

|  |  |  |  |
| --- | --- | --- | --- |
| **Location** | *<ADD – onsite>* | *<ADD – nearby site>* | *<ADD – offsite>* |
| **Access instructions** | *<ADD>* | *<ADD>* | *<ADD>* |

Virtual command center details (internal communication tools)

|  |  |
| --- | --- |
| **Communication medium** | *<ADD>* |
| **Conference bridge details** | *<ADD>* |

Backup virtual command center details (external solution)

|  |  |
| --- | --- |
| **Communication medium** | *<ADD>* |
| **Conference bridge details** | *<ADD>* |

Minutes of meeting should be documented during CMT meetings and may include a situation report, action plan/action items and specify the next meeting time.

# Continuous monitoring

The CMT should meet on regular basis to oversee the crisis response. The meeting interval will be driven by the nature of the crisis, which may require a continuous bridge to be open (short term crises) or periodic check-ins by the CMT (longer-term crises).

The CMT will also assign support personnel to help monitor the situation and what is being said in media channels to contain the crisis impact on the organization. These support personnel will report back to the CMT immediately or at pre-defined intervals, depending on the nature of the crisis.

# Communications

1. Upon plan activation
	* The CMT Lead authorizing CMP activation must notify the business continuity coordinator of the activation and scope
	* The business continuity coordinator begins notifying personnel with crisis management responsibilities that the CMP has been activated and their involvement is required
	* The Communications Lead issues a mass internal notification to all organization staff or subset of impacted staff notifying them of the CMP activation and any relevant instructions based on the procedures being executed
	* The Communications Lead issues external notifications to relevant parties informing them of the disruption and that recovery procedures are underway.
2. On-going communications during a crisis
	* The business continuity coordinator or the Communications Lead will issue periodic status updates to impacted internal stakeholders informing them of the progress. The communications interval will be driven by the nature of the crisis
	* The business continuity coordinator will issue separate status updates to organization’s management at the same frequency, including a copy of the decisions-made form and any additional relevant details on recovery progress
	* Additional communications may be issued by the business continuity coordinator (internally) and the Communications Lead (internally/externally) throughout the crisis, as required
	* In addition to the communications above, pre-defined messages have been developed in Appendix 2 below which are specific to different crisis situations.
3. At the conclusion of a disruption:
	* The business continuity coordinator or the Communications Lead will inform internal stakeholders that the crisis situation is over, and the Communications Lead will do the same for external parties
	* The business continuity coordinator will also gather feedback from relevant stakeholders on the effectiveness of CMP procedures and the overall process.

# Appendix 1 – contact information list

**Crisis management team**

| Name | Role | Phone number(s) | Email address |
| --- | --- | --- | --- |
|
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Emergency response team leads and alternates**

| Name | Role | Phone number(s) | Email address |
| --- | --- | --- | --- |
|
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

#  Appendix 2 – pre-prepared media statements

| Scenario | Authorized speaker | Primary messaging |
| --- | --- | --- |
|
| Cyber-attack |  |  |
| Labor strike / protest |  |  |
| Physical vandalism / attack |  |  |
| Theft of critical assets |  |  |
| Fire / explosion |  |  |
| Equipment / hardware malfunction |  |  |
| Power failure |  |  |
| Chemical / hazmat spill |  |  |
| Software malfunction |  |  |
| Supplier failure / bankruptcy |  |  |
| Industrial accidents |  |  |
| Epidemic / pandemic |  |  |
| Snow storm |  |  |
| Earthquake |  |  |
| Hurricane |  |  |
| Flooding / tidal wave |  |  |
| Extreme cold temperatures |  |  |