



Central Plaza Hotel Public Company Limited

Procedure

Business Continuity Plan: BCP

(2026 Edition)

Approved by Board of Directors Meeting No. 7/2025
on 14 November 2025

By Risk Management Department

INTERNAL USE ONLY

	Procedure: Business Continuity Plan: BCP	Doc. NO.: SOP-CHR-RM-001
		Doc. Sensitivity: Internal Use Only
		Effective Date: 01/01/2026
		Responsible by: Risk Management

1. Document Control

Preparer	Risk Management Department
Confidential Classification	Internal use only
Document Code	SOP-CHR-RM-001
Document Title	Procedure Subject: Business Continuity Plan: BCP
Version	1.0
Document Status	Approved
Effective Date	1 January 2026

2. Document Preparation / Review by

Name	Position	Date
Miss Ploylalin Kicwattanataworn	Corporate Risk & Data Protection Manager	1 Nov 2025

3. Document Review By

Name	Position	Date
Mr. Thaschai Phattanagosai	Assistant Vice President - Corporate Risk, Legal & Sustainability	1 Nov 2025
Mr. Thirayuth Chirathivat	Chief Executive Officer	1 Nov 2025
Risk Management, Corporate Governance, and Sustainability Committee Meeting No. 4/2568		5 Nov 2025

4. Document Approval By

Name	Meeting No.	Date
Board of Directors Meeting	7/2025	14 Nov 2025

5. History of Document Revisions

Version	Effective Date	Description of Revision	Prepared/ Revised by
0.0	1 Jan 2023	Promulgation commencement	Miss Ploylalin Kicwattanataworn
1.0	1 Jan 2025	Revision 1. Clause 3.2: Clause 3.2: Overview of the Business Continuity Management Framework – Two additional strategies for	Miss Ploylalin Kicwattanataworn

Version	Effective Date	Description of Revision	Prepared/ Revised by
		<p>resource management have been added: information management and budget management.</p> <p>2. Add Clause 4.1.5: Considerations for Terminating the Use of the Business Continuity Plan (BCP).</p> <p>3. Clause 4.1.6: Business Impact Analysis (BIA) and Risk Assessment of crises or threats involve reassessing risks and enhancing current control measures.</p>	
1.0	1 Jan 2026	Reviewed and no revisions required.	Miss Ploylalin Kicwattanataworn

 Procedure: Business Continuity Plan: BCP	Doc. NO.: SOP-CHR-RM-001
	Doc. Sensitivity: Internal Use Only
	Effective Date: 01/01/2026
	Responsible by: Risk Management

Table of Contents

1. Introduction.....	5
2. Glossary Definition	6
3. Business Continuity Management: BCM.....	8
3.1 Business Continuity Management-Related General Knowledge	8
3.2 Overview of the Practical Guidelines for Business Continuity Management consists of six main elements	9
3.3 Business Continuity Management Policy (BCM Policy)	10
4. Business Continuity Plan (BCP)	13
4.1 General Information	13
4.1.1 Scope of the Business Continuity Plan BCP	13
4.1.2 Objectives of the Business Continuity Plan Preparation.....	13
4.1.3 Structure of the Business Continuity Plan	14
4.1.4 The Implementation of the Business Continuity Plan (BCP).....	14
4.1.5 Considerations for Terminating the Use of the Business Continuity Plan (BCP).....	15
4.1.6 Business Impact Analysis (BIA) and Risk Assessment	15
4.2 Structure of the Duties and Responsibilities in BCP Governance	23
4.2.1 BCP Governance Structure	23
4.2.2 Roles and Duties and Responsibilities of BCP Governance.....	24
4.3 Contingency Plan at the Time of Crisis Event or Emergency Incident	28
4.3.1 Overview of the Business Continuity Management Plan	28
4.3.2 Annoucement and Notification of the BCP Activation in Working Hours	29
4.3.3 Communication and Public Relations upon the Crisis Declaration	30
4.3.4 Evacuation upon receiving notification of the activation of the BCP plan.....	33
4.3.5 Operating Procedure in the Case of the Event Incidence in Late Working Hours	36
4.3.6 Assemby Point	37
4.3.7 Alternate Site	38
4.4 Contingency Plan in the Case of the Emerging Infectious Disease Outbreak	39

 Procedure: Business Continuity Plan: BCP	Doc. NO.: SOP-CHR-RM-001
	Doc. Sensitivity: Internal Use Only
	Effective Date: 01/01/2026
	Responsible by: Risk Management

4.4.1 Outbreak Period	39
4.4.2 Workplace Contingency Plan	39
4.4.3 Personnel Contingency Plan.....	42
4.4.4 Communication Contingency Plan	44
4.4.5 Operation Continuity Plan for the Department	45
4.5 Recovery Plan	46
4.6 BCP Testing and Review	47
4.6.1 BCP Testing.....	47
4.6.2 BCP Review.....	47
Annex 1: Checklist of the Staff in Work Unit in Evacuation Procedure	48
Annex 2: Notification of Incident.....	49
Annex 3: List of Incident Impact Assessment	50
Annex 4: Emergency Call Numbers.....	51

1. Introduction

With the rapidly changing environment, the unexpected current incidents have been natural disasters, all forms of threats, events of terrorism, sabotage, and disease outbreak incidents. They have been wholly uncontrollable incidents and may affect the business operation capability, causing operational disruption and damage both to the personnel's property and life. The stakeholders will be broadly affected if unrecoverable.

Therefore, Central Plaza Hotel Public Company Limited gives precedence to the determination of consistent management strategies at the corporate level, formulation of preventive measures, preparedness, encouragement of awareness and responsibility according to the Guidelines for Business Continuity Management (BCM) and Business Continuity Plan (BCP) to control the contingent financial, legal, and reputation impacts, and other impacts.

This practice aims to provide useful information in the aspects of the Company's preparedness for personal development, determination of response or contingency plan to contribute to the mitigation of severity and impact that will occur with the Company, and also contribute to the Company's ability to make a rapid and proper decision when it is in crisis, without disruption of business operations and minimum impact on the Company's stakeholders.

Samples of the Disrupting Incidents

Natural Disasters	Flood, fire, storm, earthquake, tsunami, severe disease outbreak, building failure
Human-Caused Disasters	Terrorism, such as stealthily bombing, stealthily fire setting, protestation, riot
System Disasters	IT System damage, data inaccessibility or cyber threat, building and workplace inaccessibility, electrical system disconnection
Human Resources	Loss of important executives and key personnel, nonattendance of the important executives and personnel or work absenteeism of many staff

2. Definition

Business Continuity Management (BCM)	It refers to the approach for defining the policies, standards, and processes of an organization to ensure that in the event of an incident or disaster that causes operational disruptions, critical activities can continue without interruption.
Business Continuity Plan (BCP)	It refers to the steps of any plan developed under the business continuity management policy to ensure that the Company's operations can continue under crisis situations.
Business Impact Analysis (BIA)	It refers to the process of analyzing and measuring the impact or business loss caused by the disruption of the Company's operations, both quantitatively and qualitatively.
Critical Business Function (CBF)	It refers to the business function that is disrupted and may significantly affect the Company's operations, business, reputation, status, and performance.
Maximum Tolerable Period of Disruption (MTPD)	It refers to the maximum tolerable period of the system's disruption.
Recovery Time Objectives (RTO)	It refers to the target timeframe used to restore the delivery of products, services, and activities or processes to normal after a disruption.
Recovery Point Objective (RPO)	It refers to the maximum allowable data loss period that an organization can accept. For example, if the most recent data is 18 hours old and the organization requires an RPO of 20 hours, it indicates compliance with the organization's criteria.
Minimum Business Continuity Objective (MBCO)	It refers to the minimum acceptable level of service for the resumption of processes or activities.
Recovery Strategy	It refers to the guidelines for responding to the disruption of the critical system's operation.
Business Recovery Plan: BRP or Disaster Recovery Plan: DRP)	It refers to the written plan prepared in the system recovery in the case of the system's failure, contributing to the capability to recover the system and function.
Alternate Site	It refers to the replacement workplace for business operations when the main workplace cannot operate as usual. The said workplace should be adequately far from the head office not to have the same impact and should not use the public utility from the same source. The Alternate Site should support the situations in the long term and be available
Command Center	It refers to a location designated as the command center for the crisis management team during a crisis. This center may be established at

the computer center, backup operations center, or any other suitable location.	
Call Tree	It refers to the call tree of the staff inside the Company to communicate the staff for acknowledgment upon the incidence of crisis or upon the promulgation of the Business Continuity Plan
Testing	It refers to an activity organized to simulate a real crisis situation for various departments with the aim of training and creating operational familiarity. The testing reveals the effectiveness of the plan when implemented, and the results are used to further develop and refine the plan for greater completeness.
Emerging Infectious Diseases	It refers to an infectious disease caused by a new pathogen, an infectious disease found in a new area, a recurrent infectious disease, a drug-resistant pathogen, and a biological weapon (according to the definition by the World Health Organization).
Work from home	means the operation outside the Company's workplace, or outside the regular workplace or the staff's residence, or the place supported by the Company, where the goal setting, working planning, and work success, as well as explicit determination of operation hours and mode of communication used during operation from the outside of the regular establishment of the Company.

3. Business Continuity Management: BCM

3.1 Business Continuity Management-Related General Knowledge

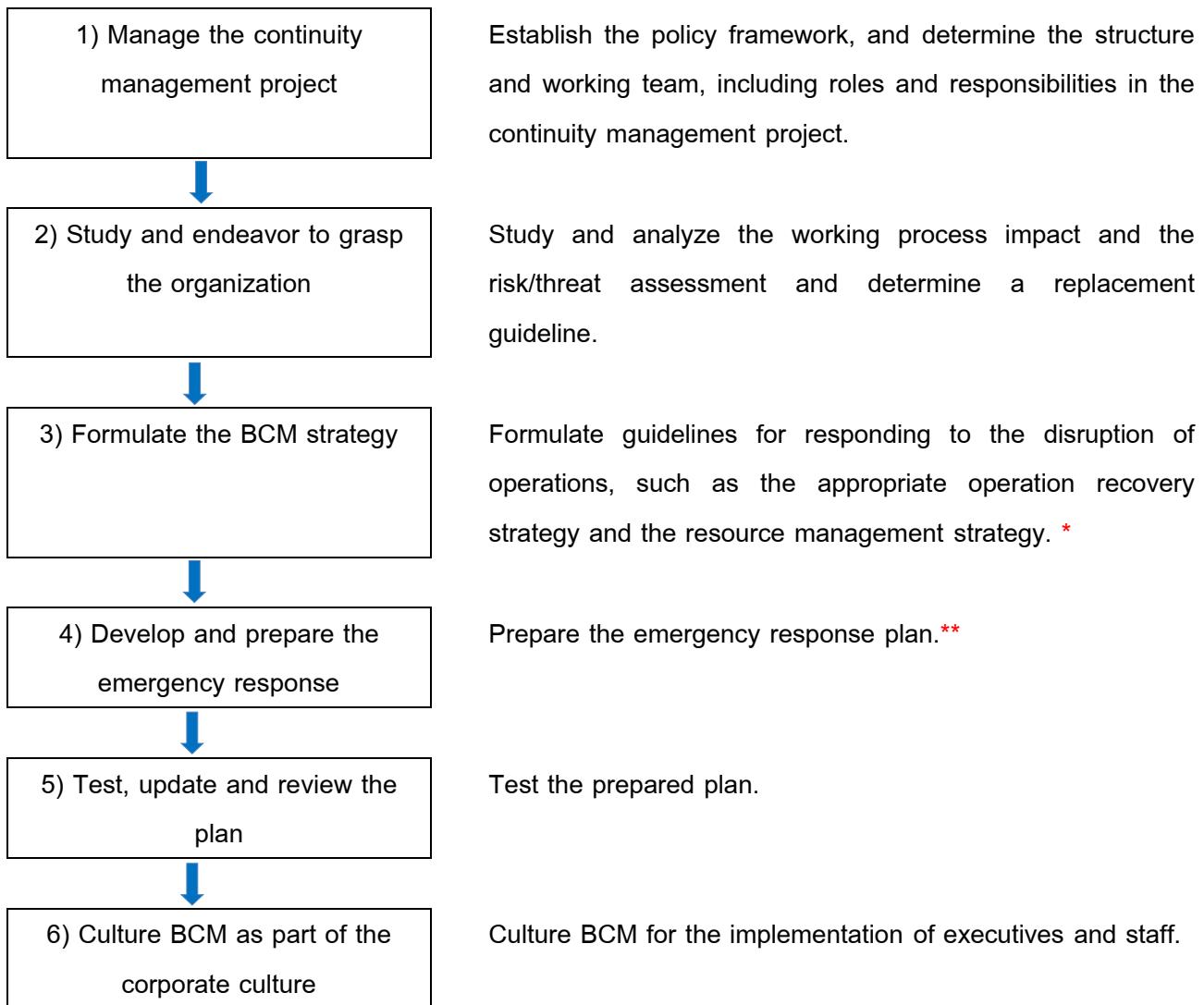
Business Continuity Management (BCM) means the guidelines for formulating the Company's policies, standards, and work processes to ensure that in the case of incidents disrupting regular operation, the critical systems will be continuously operable or return to be operable at a suitable time.

The whole administration process that indicates the organizational threats and business operation impact from such threats is formulated, and the guidelines for creating the capacity to ensure the organizational elasticity are established to respond and protect the stakeholder benefits, reputation, image, and activities that create the effective value.

Organizational management in crisis generally classifies the management life cycle into four steps, which are the necessary matters for the in-house personnel to be aware, cautious, and not nervous about the situation. Therefore, the crisis management life cycle is the following.



3.2 Overview of the Practical Guidelines for Business Continuity Management consists of six main elements.



Remark:

* Appropriate resource management strategy

1. **People.** By the principle of BCM, the organizational structure and the personnel roles and duties, including the chain of command, shall be clearly formulated to ensure the efficiency of the exercise of deciding power and crisis communication. In addition, the personnel shall physically and mentally practice the plans to ensure teamwork in a crisis. Moreover, the organization should also determine the alternate personnel to work in a crisis, such as the crisis management supporting team, business recovery team, IT recovery team, etc.

 Procedure: Business Continuity Plan: BCP	Doc. NO.: SOP-CHR-RM-001
	Doc. Sensitivity: Internal Use Only
	Effective Date: 01/01/2026
	Responsible by: Risk Management

2. Site and Infrastructure: The backup location in a crisis should not be too close to the primary site, such as the command center. It must have reliable communication and IT equipment to ensure easy and fast access to data during a crisis. Additionally, a robust data backup system should be in place, with backups stored offsite.

3. Plans: The plans shall be prepared by considering the plans focusing on the process requiring the performance, easy and concise understanding, determination of clear roles and duties, and coordination with the locality, government sector, and regulatory agency, including people movement plan as part of the BCM. These plans shall be regularly tested and updated

4. Data: Critical data related to key activities, or the business must be backed up. In the event of an abnormal incident affecting this data, the backup data should be immediately utilized as a substitute.

5. Budget: An emergency reserve budget must be allocated, along with specific processes for its utilization that differ from standard procedures. This ensures the budget can be promptly accessed to mitigate impacts effectively.

** The emergency incident response plan shall be prepared and consist of the following.

1. Business Continuity Plans (BCP) are designed to ensure continuous management of business operations. The focus is on carrying out critical emergency tasks for the business while utilizing key resources efficiently and at a minimum level. Additionally, the plan includes preparations for mitigating impacts in worst-case scenarios.

2. Incident Management Plans (IMP) are designated to address the emergency crises that arise --> [referencing the document from the Corporate Administration and Operations Division titled “Emergency Safety Procedures Manual.”](#)

3. Outage Impact and Allowable Outage Times --> [referencing the document from Corporate Administration and Operations Operation titled “Business Continuity & Disaster Recovery Plan – version 2018”](#)

4. Disaster Recovery Plans (DRP) --> [referencing Document No. PLN-CHR-ITC-001 from Information Technology & Transformation](#)

3.3 Business Continuity Management Policy (BCM Policy)

As mentioned above, the Company places great importance on managing uncontrollable events that may impact its ability to operate. A Business Continuity Management Policy has been established to ensure uninterrupted operations and a swift return to normal business conditions. This includes enabling customers to conduct transactions and access services seamlessly.

	Procedure: Business Continuity Plan: BCP	Doc. NO.: SOP-CHR-RM-001
		Doc. Sensitivity: Internal Use Only
		Effective Date: 01/01/2026
		Responsible by: Risk Management

Even in emergencies, the Company also prioritizes the safety of its employees and assets, evaluates financial impacts, and ensures continuity in operations. This includes critical systems to business operations that are able to be recovered and restored within the specified timeframe for each division. Additionally, the Company has provided data protection systems, including storage and retrieval of information in emergencies. These measures address the assumption that such emergencies are force majeure events causing disruptions to the Company's ability to maintain continuous operations.

The Board of Directors has approved the core policy, which is the Business Continuity Management Policy. In addition, the Risk Management, Corporate Governance, and Sustainability Committee has approved the Company's Business Continuity Plan (BCP) regulations. The authority to review the policy and update the Business Continuity Plan has been delegated to the Chief Executive Officer. Operational responsibilities have been assigned to the Business Continuity Management Committee (BCM Committee), supported by the Crisis Management Team (CMT) as the working group.

Contingency Plan Policy

1) Command on Activation of the Contingency Plan (BCP Activator)

Due to the sudden business disruptions in various forms and the uncertain period, the Company assigns the Company's Chief Executive Officer (CEO) to exercise discretion and to be the person who has the absolute power to command to use of the business operation plan or the Contingency Plan according to the situation suitability (Severity) and can authorize the appropriate command power to the crucial sections by determining the action according to the determined Call Tree. If the CEO is engaged, the following authorized person, according to the Company's organizational structure, is assigned to perform instead.

2) Setup of the Alternate Sites (Plan A – Alternate Sites)

In the case where an emergency occurs at the Company's office or the nearby area where the staff cannot enter for normal operation, the Company assigns the Crisis Management Team to be responsible for arranging the site for the staff's operation or may consider allowing each staff backing up his/her data to work from home as the case may be.

3) Replacement Personnel Plan for all Crucial Sections

In the case where a disease outbreak occurs, many staff may take leave or suddenly lose the staff in the crucial section. Therefore, all line superiors are assigned to be responsible for organizing training through the control of the Human Resource (HR) Department to train the staff

	Procedure: Business Continuity Plan: BCP	Doc. NO.: SOP-CHR-RM-001
		Doc. Sensitivity: Internal Use Only
		Effective Date: 01/01/2026
		Responsible by: Risk Management

to be able to work various duties and prepare the operation manual to ensure that the staff can work in replacement, particularly for the section which is the Critical Business Function.

4) Availability of Fire Prevention and Suppression System

The Corporate Administration and Operations Section is determined to take responsibility for the availability of the fire prevention plan, including the training plan, inspection and testing plan for the functional efficiency of the Company's fire prevention and suppression system at least once a year, and report the inspection result to the line superior for acknowledgment.

5) Fire Fighting and Evacuation Fire Drill

The Corporate Administration and Operations Section is assigned to rehearse fire escape for the Company's staff at least once a year for the staff's acknowledgment of the proper conduct procedure upon the occurrence of the event of a fire and determine the assembly point in the event of fire occurs, as well as organizes the fire fighting drill of the working team that is jointly responsible together with the officer of Office Building Department.

6) Staff Training, Yearly Rehearsal and Evaluation (BCP Awareness /Testing / Reviewing)

The Risk Management Division is designated as the coordinator for conducting BCP Awareness Training to educate employees about the Business Continuity Plan (BCP). It is also responsible for presenting proposals to the Chief Executive Officer regarding the scheduling of drills and reporting the annual emergency drill results. Additionally, the division ensures the contact list (Call Tree) is continuously updated.

	Procedure: Business Continuity Plan: BCP	Doc. NO.: SOP-CHR-RM-001
		Doc. Sensitivity: Internal Use Only
		Effective Date: 01/01/2026
		Responsible by: Risk Management

4. Business Continuity Plan (BCP)

4.1 General Information

4.1.1 Scope of the Business Continuity Plan BCP

1) Support the crisis or serious incident causing failure to access the building or impact on the resources consumed in the operations causing incapability of the normal operation, such as accident, natural disaster, fire, flood, sabotage or incidence of disease outbreak, etc.

2) Cover the Company's critical products or functions to ensure that when a serious incident occurs, the Company's Critical Business Function will return to execute in the suitable period.

3) It is unavailable to support the event of obstructions occurring in the Company's normal business operations since the said obstructions should be managed or improved and corrected to be appropriate by the executive of each Department and arrange the regular review and improvement of the operation process.

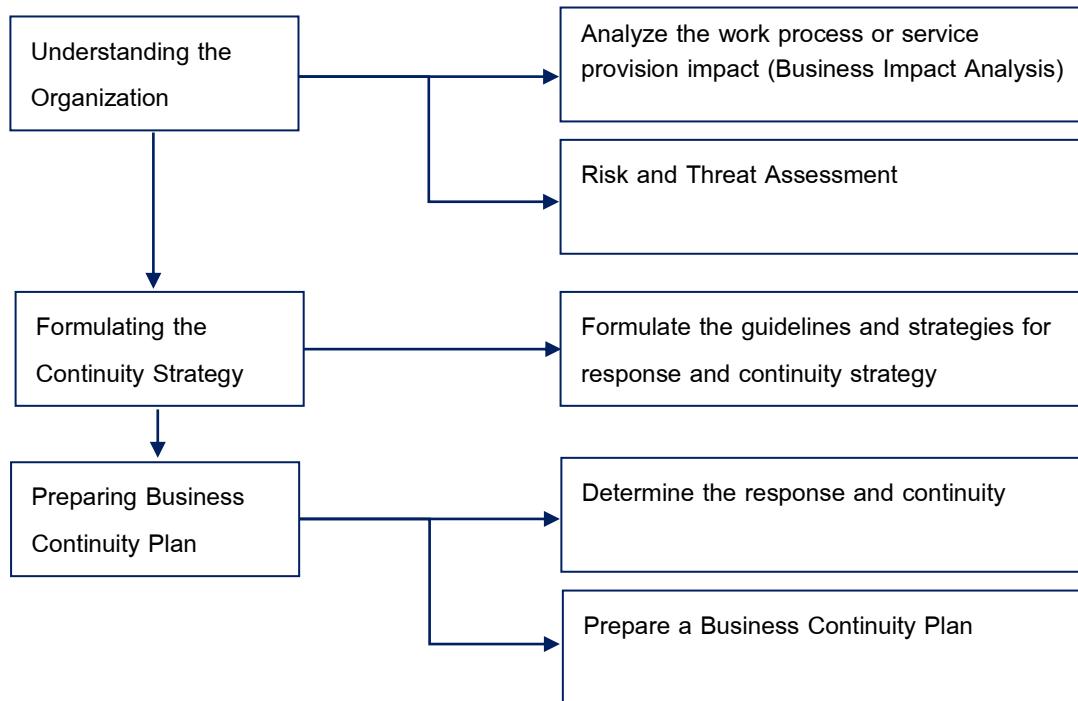
4) The Alternate Site of the Company must not be affected by the event of a severe crisis incident, and the services of the public utility system and communication system inside Bangkok can still be provided.

5) In the case of the business function supporting the system's failure, BCP shall be used accompanied by an IT Contingency Plan and Disaster Recovery Plan (DRP) responsible and supervised by the Company's IT Department for preparation.

4.1.2 Objectives of the Business Continuity Plan Preparation

- 1) For the use as the guidelines for the management continuity of operation in a crisis
- 2) For the work unit's advanced preparedness to cope with the contingent crisis or emergency incidents
- 3) For the impact mitigation in different aspects due to the disruption of execution
- 4) For the damage mitigation to be at a tolerable level

4.1.3 Structure of the Business Continuity Plan



4.1.4 The Implementation of the Business Continuity Plan (BCP)

The implementation of the Business Continuity Plan (BCP) will be applied to crisis incidents according to the nature of the impacts, specifically on the Company's critical resources. These impacts are categorized into four aspects as follows:

- 1) **Building/ Workplace Impact:** To address situations where operations at the primary workplace are not possible, it is divided into:
 - Alternate Workplace: The Company has designated a backup operational site to address crisis situations affecting the headquarters, making it inaccessible for employees to perform their duties as usual. This designated site is the Centara Grand at Central Plaza Ladprao Bangkok (CGLB), the office operations center. For all other tasks, employees are advised to work from home.
 - Data: The Information Technology Department shall be assigned to be responsible for the data backup preparedness at the Alternate Site, the office of Centara Grand at Central Plaza Ladprao Bangkok (CGLB).
- 2) **Crucial Materials and Equipment Impact:** To address situations where critical equipment cannot be used or where the procurement and delivery of essential materials for operations are not feasible, the details are as follows:
 - The backup tools and equipment are prepared for use in a crisis.

 CENTARA HOTELS & RESORTS	Procedure:	Doc. NO.: SOP-CHR-RM-001
	Business Continuity Plan: BCP	Doc. Sensitivity: Internal Use Only
		Effective Date: 01/01/2026
		Responsible by: Risk Management

3) **System Impact:** To address situations where computer systems or networks cannot function normally on a continuous basis, the following measures are in place:

- The Company has established an IT Contingency Plan and a Disaster Recovery Plan (DRP) as part of its Business Continuity Plan. These serve as guidelines for restoring computer systems at the Company's data center.

4) **Personel Impact:** To address situations where the company's personnel are insufficient for operations or employees are unable to work during emergencies, the following measures are implemented:

- All departments must maintain operation procedures with clear details and procedures to serve as a guideline for substitute operations.
- Employees within departments are rotated to ensure they can perform each other's tasks when needed.
- A hierarchy of replacement personnel is established within the scope of the emergency plan to ensure work continuity if the primary responsible individual is unavailable.

4.1.5 Considerations for Terminating the Use of the Business Continuity Plan (BCP)

The termination of the Business Continuity Plan (BCP) can proceed when the emergency or disaster situation has returned to normal, and operations are ready to follow the procedures for transitioning systems back to their normal state. The BCM Committee is responsible for determining the termination of the BCP.

4.1.6 Business Impact Analysis (BIA) and Risk Assessment

The Company has established the process for considering the Critical Business Function that must be performed in the crisis occurrence period with the following process.

- Defining criteria for the severity level of potential business impacts and the likelihood of such events occurring.
- Risk Assessment is performed to specify the incident, situation, or factor that may disrupt business operations by analyzing the likelihood or impact affecting the business operation.
- A scenario is determined by considering the incident with the crucial likelihood and impact acquired by the Company from the risk assessment.
- The business impact or loss from the disruption of the crucial execution is assessed and taken for analyzing and determining the Critical Business Function. If there is disruption, it will significantly affect the Company's execution, reputation, and performance.

Risk Assessment of the Crisis or Threat

Crisis / Damage Event	Risk Assessment		Arisen Impact				
	Like lihood	Impact	Inaccessibility to the Operating Area	Damaged Building and Site	Failure of IT System to Support Working	Loss of Key Executives and Personnel	Discredit / Customer's Lack of Confidence and Disuse of Services
1 Economy/Physics							
Staff Protestation	L	H	X	X		X	X
Political Assembly	L	H	X	X		X	X
Electric Current Failure	L	L			X		
2 Natural Disaster							
Flood	L	H	X	X	X		
Fire	L	H	X	X	X	X	
Flood	L	H	X	X	X		
Tsunami	L	H	X	X	X	X	
Emerging Infectious Disease	L	H	X			X	X
3 Human Disaster							
Terrorism/Sabotage	L	H	X	X		X	X
4 Computer System							
Computer Center Disaster	L	H			X		X
Information Theft	L	H			X		X
Network System Failure	L	H			X		X
5 Reputation							
Being sued and taken for legal proceedings with the serious lawsuits	L	H				X	X
Corporate Derogatory Rumor	L	H				X	X

Remark :

Likelihood Level of Incident H = High, frequent or probable likelihood of an incident

L = Low and seldom likelihood of an incident

Impact Level H = High damage until the entity must be temporarily closed (the operation suspension period of more than 1 day)

L = Damage, but the situation is controllable (the operation suspension period of not exceeding 1 day)

	Procedure: Business Continuity Plan: BCP	Doc. NO.: SOP-CHR-RM-001
		Doc. Sensitivity: Internal Use Only
		Effective Date: 01/01/2026
		Responsible by: Risk Management

Step 1: Identify criteria for the severity of potential business impacts (Business Impact Analysis: BIA) and the likelihood of occurring event

Criteria	1	2	3	4	5
Impact	Negligible	Minor	Moderate	Significant	Disastrous
Financial Impact	Damage cost \leq 50,000 Baht	Damage cost >50,000 - 100,000	Damage cost >100,000 - 200,000	Damage cost >200,000 - 300,000	Damage cost >300,000
Customer Impact	Negligible impact on customer service, and services remain fully operational as usual.	Minor impact on customer service, with some dissatisfaction, though customers continue doing business with the Company.	Moderate impact on customer service, leading to some dissatisfaction and partial cancellation of services with the Company.	Significant impact on customer service, resulting in customers canceling the Company's services.	Severe impact on customer service, drastically affecting business operations.
Reputation and Credibility Impact	No impact on the Company's reputation.	Minor impact on the Company's reputation and credibility, or it occurs within a specific industry.	Impact on the Company's reputation and credibility, with negative headlines in newspapers, radio, television, or online media for 1 day.	Significant impact on the Company's reputation and credibility, with negative headlines in newspapers, radio, television, or online media for more than 1 day.	Severe impact on the Company's reputation and credibility, with continuous negative headlines in newspapers, radio, television, or online media.
Legal Impact	No impact if there is a breach of law or failure to comply with the service agreement.	If actions do not comply with legal requirements or the service agreement, it may have a minor impact on the Company.	If actions do not comply with legal requirements or the service agreement, the Company may be fined as stipulated in the law or contract.	If actions do not comply with legal requirements or the service agreement, the Company may face civil litigation.	If actions do not comply with legal requirements or the service agreement, the Company may face both civil and criminal litigation.

Criteria	1	2	3	4	5
Likelihood	Very unlikely	Unlikely	Possible	Highly Possible	Probable
Incident history in the Company or within the hotel industry group (over the past 10 years).	Never occurred before in the hotel industry	Has occurred before in the hotel industry group but never in the Company	Has occurred 1-3 times in the Company	Has occurred frequently in the Company 4-5 times	Has occurred frequently in the Company more than 5 times
Volume of items (for each activity)	< 10% or 1 time per year	10% - 20% or 2 times per year	>20% - 30% or 3-4 times per year	>30% - 40% or 5-12 times per year	> 40% or 13 times per year or more

Step 2: Assess the impact based on business transaction activities.

Functions	Critical Business Function: CBF	Business Impact				
		Monetary	Customer	Reputation	Law	Total
1	Business transactions must be carried out in accordance with regulations and legal requirements.					
1.1 Calculation and submission of the monthly tax return, social security, and provident fund	X	3	1	2	4	10
1.2 Follow-up of the existing lawsuit progress	X	3	1	3	4	11
2	The main processes for receiving customers to use services include room accommodation, dining, fitness, and spa services.	✓	5	5	5	5
3	Transactions in which the company has obligations to external parties and items that are in progress to be completed.					
3.1 Payment of expenses						
- Employee salary payments	X	3	1	2	4	10
- Loan repayments						
- Payment of various taxes, social security, and SSF						
- Payments to suppliers/vendors for goods/services						
- Payment of other expenses as per invoices, such as utilities, etc.						
3.2 Payment Receipt	X	4	2	2	1	9
3.3 Renewal of hotel business licenses	X	3	1	2	4	10
4	Business transactions that support various operations.					
4.1 Procurement of goods (items with a Purchase Order issued).	X	4	4	4	3	15
4.2 Insurance Notification/Payment	X	4	2	4	4	14
4.3 Collection of Outstanding Account	X	4	1	2	4	11
4.4 Follow-Up of the Contracts under Operation	X	4	1	2	4	11
5	Source of Investment Funds Management	X	3	1	3	3
						10

Transactions with a total business impact assessment score of 15 or higher are designated by the company as critical business activities to be carried out during a crisis.

From the aforementioned critical business transactions, the required resources can be detailed as follows:

- Personel: Front desk staff, restaurant staff, fitness center staff, and spa staff.
- Technology: Property Management System (PMS), Point of Sales System (POS), Door Locking System, Un-interruption Power Supply System, Main and Distribution Switches, Intranet, Internet

Step 3: Business Impact Analysis (BIA)

1) Maximum Tolerable Period of Disruption (MTPD)

Prioritized Activities	Allowable Outage Time *** (MTPD)	Resources	dependencies, including partners and suppliers interdependencies
The primary processes for accommodating customers include providing services for accommodations, dining, fitness, and spa facilities.	6 hours	Property Management System (PMS)	Unable to execute reservation, guest info, billing and accounting process
	6 hours	Point of Sales System (POS)	Venues couldn't issue guest bill and post to guest account
	6 hours	Door Locking System	User couldn't issue new key for guest
	24 hours	Un-interruption Power Supply System	Unable to supply power when main electric power outage
	6 hours	Main and Distribution Switches	Users couldn't access to network

Remark: ** Reference is made to the document from the Corporate Administration and Operations department titled *Business Continuity & Disaster Recovery Plan – Version 2018*, which has already defined the MTPD values.

2) Assess the business impact in relation to time.

Operation Process	Disrupt Event	Impact	Impact Over Time									
			30 Min	1 Hrs	2 Hrs	4 Hrs	6 Hrs	8 Hrs	10 Hrs	12 Hrs	24 Hrs	> 24 Hrs
1. Service: Accommodation												
Welcoming customers process	The shutdown of the PMS system causes service disruptions, leading to the unavailability of information on room reservations, customer check-out times, and various charges applied to the rooms.	Financial impact	1	2	4	5	5	5	5	5	5	5
		Customer impact	1	2	3	4	5	5	5	5	5	5
		Reputation and credibility impact	1	1	2	3	4	4	4	4	4	4
		Legal impact	1	1	1	2	2	2	2	2	2	2
	A data breach incident occurs, leading to customer lawsuits or the Personal Data Protection Committee (PDPC) ordering the suspension of services.	Financial impact	5	5	5	5	5	5	5	5	5	5
		Customer impact	4	4	4	4	4	4	4	4	4	4
		Reputation and credibility impact	4	4	4	4	4	4	4	4	4	4
		Legal impact	5	5	5	5	5	5	5	5	5	5
	Employees gather to protest due to dissatisfaction with the Company.	Financial impact	2	3	4	5	5	5	5	5	5	5
		Customer impact	3	3	3	4	4	4	4	4	4	4
		Reputation and credibility impact	3	3	3	4	5	5	5	5	5	5
		Legal impact	3	3	3	3	3	3	3	3	3	3

Operation Process	Disrupt Event	Impact	Impact Over Time									
			30 Min	1 Hrs	2 Hrs	4 Hrs	6 Hrs	8 Hrs	10 Hrs	12 Hrs	24 Hrs	> 24 Hrs
2. Restaurant and Spa												
The process of posting the bill to the customer.	Closing the POS system prevents the ability to verify whether a guest has made a reservation, or which room they are staying in, which could result in posting the bill to the wrong room.	Financial impact	1	1	2	2	4	4	4	4	4	4
		Customer impact	1	1	1	2	3	3	3	3	3	3
		Reputation and credibility impact	1	1	2	2	2	2	2	2	2	2
		Legal impact	1	1	1	2	2	2	2	2	2	2
The process of providing customer service using labor.	The emergence of new infections leads to widespread transmission, resulting in an insufficient number of employees to provide customer service.	Financial impact	1	2	3	4	5	5	5	5	5	5
		Customer impact	3	3	3	4	4	4	4	4	4	4
		Reputation and credibility impact	1	1	2	2	3	3	3	3	3	3
		Legal impact	1	1	1	2	2	2	2	2	2	2
3. Security Service												
The process of ensuring the safety of all customers and employees.	A fire occurred in the sauna room / restaurant / guest room.	Financial impact	3	3	4	5	5	5	5	5	5	5
		Customer impact	3	4	5	5	5	5	5	5	5	5
		Reputation and credibility impact	2	2	4	4	4	4	4	4	4	4
		Legal impact	1	1	1	2	2	2	2	2	2	2
The process of ensuring the safety of all customers and employees.	A flooding event occurred in the basement area, affecting the first floor of the hotel.	Financial impact	3	3	4	5	5	5	5	5	5	5
		Customer impact	2	2	2	3	3	3	3	3	3	3
		Reputation and credibility impact	1	1	2	2	3	3	3	3	3	3
		Legal impact	1	1	1	2	2	2	2	2	2	2
The process of ensuring the safety of all customers and employees.	A political protest occurred near the hotel, causing the hotel to be surrounded. However, operations continued as usual inside, with heightened security monitoring within the building.	Financial impact	2	3	4	5	5	5	5	5	5	5
		Customer impact	3	3	3	4	4	4	4	4	4	4
		Reputation and credibility impact	3	3	3	4	5	5	5	5	5	5
		Legal impact	3	3	3	3	3	3	3	3	3	3
4. IT System												
IT system shutdown	IT system shutdown and failure	Financial impact	1	2	4	5	5	5	5	5	5	5
		Customer impact	1	2	3	4	5	5	5	5	5	5
		Reputation and credibility impact	1	1	2	3	4	4	4	4	4	4

Operation Process	Disrupt Event	Impact	Impact Over Time									
			30 Min	1 Hrs	2 Hrs	4 Hrs	6 Hrs	8 Hrs	10 Hrs	12 Hrs	24 Hrs	> 24 Hrs
		Legal impact	1	1	1	2	2	2	2	2	2	2
			49%	53%	66%	80%	88%	88%	88%	88%	88%	88%

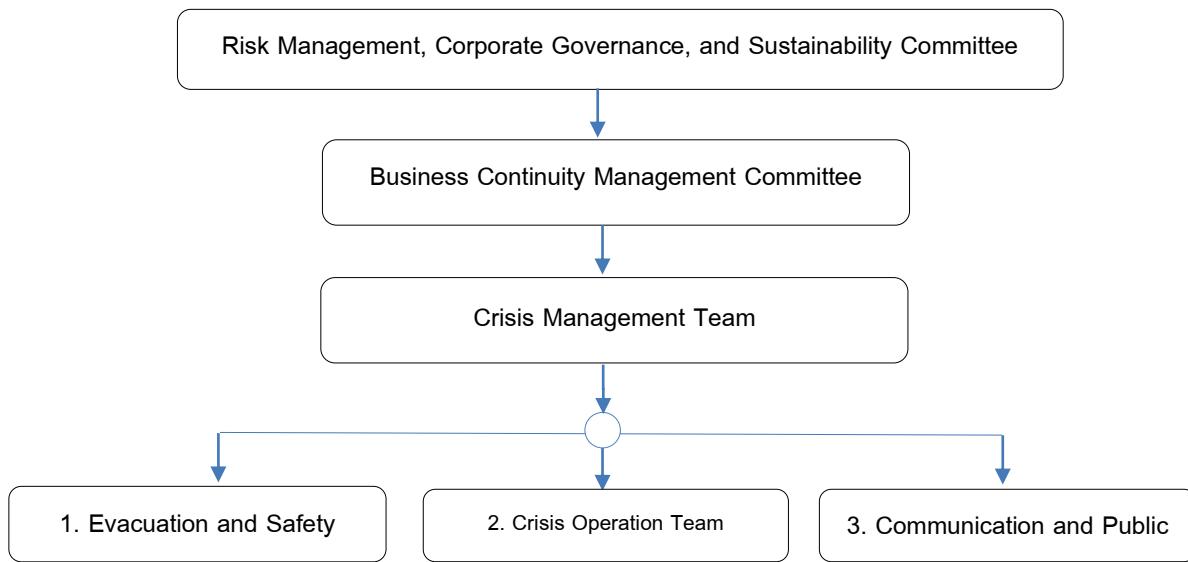
Step 4: Risk Assessment of crises or threats.

Crisis / Damage event.	Risk Assessment		Risk Level	Existing Plan						
	Maximum Impact	Likelihood								
1. Welcoming customer process										
The shutdown of the PMS system causes service disruptions, leading to the unavailability of information on room reservations, customer check-out times, and various charges applied to the rooms.	2 hrs.	4	3	High	If it's only 2-4 hours, the front desk has a manual procedure to handle customers. However, if it's 6 hours, it becomes difficult to manage. IT will pull customer stay data every 6 hours as a backup in case the system crashes, which is called a Downtime Report. This report includes information on guest stays, restaurant reservations, and spa bookings. Therefore, if it exceeds 6 hours, the BCP plan must be activated because the backup is only available for 6 hours.					
	4 hrs.	5	3	High						
	6 hrs.	5	3	High						
A data breach incident occurs, leading to customer lawsuits or the Personal Data Protection Committee (PDPC) ordering the suspension of services.	2 hrs.	5	2	High	When an incident occurs, the person who discovers it must report it to the Risk Management and Legal Department within 24 hours and follow the SOP PDPA. In the case of widespread damage or media exposure, the BCP plan must be activated.					
	4 hrs.	5	2	High						
	6 hrs.	5	2	High						
Employees gather to protest due to dissatisfaction with the Company	2 hrs.	4	1	Low						
	4 hrs.	5	1	Low						
	6 hrs.	5	1	Low						
2. The process of posting the bill to the customer										
Closing the POS system prevents the ability to verify whether a guest has made a reservation, or which room they are staying in, which could result in posting the bill to the wrong room.	2 hrs.	2	3	Medium	IT will export customer stay data every 6 hours as a backup in case the system crashes, known as the Downtime Report. This report will include information on guest stays, restaurant reservations, and spa bookings. Therefore, if the downtime exceeds 6 hours, the BCP plan must be activated, as the backup is only available for 6 hours.					
	4 hrs.	2	3	Medium						
	6 hrs.	4	3	High						

Crisis / Damage event.	Risk Assessment			Risk Level	Existing Plan
	Maximum Impact	Likelihood			
3. The process of providing customer service using labor					
The emergence of new infections leads to widespread transmission, resulting in an insufficient number of employees to provide customer service.	2 hrs.	3	3	Medium	There is a plan in place to support personnel, including raising awareness, issuing warnings, and training on self-protection methods. Additionally, there are measures to control diseases in the workplace, such as reducing overcrowding, etc.
	4 hrs.	4	3	High	
	6 hrs.	5	3	High	
4. The process of ensuring the safety of all customers and employees.					
A fire occurred in the sauna room / restaurant / guest room.	2 hrs.	5	3	High	The Central Group has established a working group called CMOC/RMOC to assist properties facing natural disasters or protests. When an incident occurs at any property, nearby Central Group properties, or those in neighboring areas will provide immediate assistance, whether in the form of equipment from Taiwatsadu or labor, among others.
	4 hrs.	5	3	High	
	6 hrs.	5	3	High	
A flooding event occurred in the basement area, affecting the first floor of the hotel.	2 hrs.	4	3	High	
	4 hrs.	5	3	High	
	6 hrs.	5	3	High	
A political protest occurred near the hotel, causing the hotel to be surrounded. However, operations continued as usual inside, with heightened security monitoring within the building.	2 hrs.	4	3	High	
	4 hrs.	5	3	High	
	6 hrs.	5	3	High	
5. IT system shutdown					
IT system shutdown and failure	2 hrs.	4	2	Medium	There is a clear IT operational plan in place, along with system backups. In the event of a system failure, recovery can be achieved within 6 hours according to the established SOP. If it is merely a system outage without other impacts such as data leakage or lawsuits, the BCP plan will not be activated. Instead, it will be reported according to the defined Crisis Escalation Flow.
	4 hrs.	5	2	High	
	6 hrs.	5	2	High	

4.2 Structure of the Duties and Responsibilities in BCP Governance

4.2.1 BCP Governance Structure



The Business Continuity Management Committee (BCM Committee) consists of the following:

1) Chief Executive Officer	Chairman of the Committee
2) Operations Executive	Committee Member
3) Accounting and Finance Executive	Committee Member
4) IT Executive	Committee Member
5) Human Resources Executive	Committee Member
6) Sales & Marketing Executive	Committee Member
7) Risk Management and Legal Executive	Committee Member and Committee Secretary

The Crisis Management Team (CMT) consists of the following:

1) Operations Executive	Team Leader
2) Head of Accounting and Finance	Team Member
3) Head of IT	Team Member
4) Head of Human Resources	Team Member
5) Head of Sales & Marketing	Team Member
6) Head of Risk Management and Legal	Team Member
7) GM of every hotel	Team Member
8) Head of Operations	Team Member and Team Secretary

Remark:

Upon the emergency incidence, the CMT will be divided into three sub-teams in operation as follows:

- Evacuation and Safety Team, where the Head of the Human Resources and the Head of the Operations are the Team Leaders.
- Crisis Operation Team, where the Head of the IT is the Team Leader.
- Communication and Public Relations Team, where the Head of the PR is the Team Leader.

4.2.2 Roles and Duties and Responsibilities of BCP Governance

1. Risk Management, Corporate Governance, and Sustainability Committee

- 1) Determine the scope of the Business Continuity Plan (BCP) to ensure that the Company can continuously operate the Critical Business Function without disruption or can recover within the specified period.
- 2) Give consent to the Business Continuity Plan (BCP).
- 3) Give consent to the BCM Committee's appointment to manage emergency situations.

2. BCM Committee

Pre-crisis occurrence

- 1) Monitor and oversee the working group to comply with the duties and responsibilities specified in the BCP.
- 2) Establish the BCP and schedule the BCP review and testing at least once a year or upon significant change.

Upon crisis occurrence

- 1) Summarize the situation assessment result report, and resolve the promulgation of the Business Continuity Plan
- 2) Promulgate the BCP via the Call Tree Structure.
- 3) Being the center to decide the matters until the crisis passes by and control the overall crisis incident management.
- 4) Approve the resources and budget used in executing the crisis occurrence period. However, the Chief Executive Officer or the entrusted person shall have the power and absolute right to decide.
- 5) Decide to announce the cancellation of the BCP activation upon resumption.

3. Crisis Management Team (CMT)

The Crisis Management Teams, such as the Evacuation and Safety Team, Crisis Operation Team, and Communication and Public Relations Team, are appointed.

➤ Evacuation and Safety Team

Pre-crisis occurrence

- 1) Establish the Staff Evacuation Plan if a crisis event occurs and review it to be updated.
- 2) Prepare the information of the name list of staff, building layout, name list, and contact telephone numbers of agencies, such as police stations, fire stations, hospitals, rescue units, and service providers or contractors, and review to be updated.
- 3) Oversee the readiness of the security equipment, such as fire extinguishers, fire hoses, etc.
- 4) Prepare the essential equipment for staff evacuation, such as a guiding signboard, flashlight, first-aid kit, etc.

Upon crisis occurrence

- 1) Coordinate with the evacuation leader of the Department to prepare the staff evacuation, control and oversee the staff evacuation upon the incidence of crisis event to the assembly point.
- 2) Coordinate and contact the rescue units to ask for assistance and suppression of the event.
- 3) Assist and transfer the victims upon detection.
- 4) Count the number of evacuees from the staff's name list, survey the staff damage, and assist the injured and dead staff according to the welfare and rights that should be obtained during the incident.
- 5) Allocate the personnel who must go to operate at the Alternate Site.
- 6) Coordinate with other sub-teams to support the procurement of manpower and equipment as requested.
- 7) Report the situations and progresses to the BCM Committee.

➤ Crisis Operation Team

Pre-crisis occurrence

- 1) Prepare the Alternate Site Command Center and the essential office equipment to be available.
- 2) Prepare the Computer Center's information system and computer hardware to be constantly available and modern.
- 3) Wholly and regularly backup the data used in operation, and the system, operations, and programs of the computer system used in working.
- 4) Prepare and store the information document forms that must be used in operation in electronic format to ensure the operation support at the Alternate Site during the crisis occurrence period.
- 5) Update the name list and telephone numbers of the computer-related service providers, the outsourced companies, and system consultants, and review to be updated.
- 6) Store the latest version of BCP documents at the main operation site in the electronic file at the File Server.

Upon crisis occurrence

- 1) Assess the primary damage to the system and computer hardware.
- 2) Control and supervise the Company's computer system preparation at the Alternate Site to be operable within the specified period.
- 3) Coordinate with the BCP Coordinator of the Department (oversee the documents and the operational readiness for preparedness of the office equipment and documents that must be used in operation).
- 4) Control and supervise the operation in the crisis occurrence period according to the BCP.
- 5) Report the situation and progress to the BCM Committee.

➤ Communication and Public Relations Tem

Pre-crisis occurrence

- 1) Establish the public relations and notification plan for news information to both internal and external related parties, and review to be updated.
- 2) Clearly assign the responsible person to be the spokesman to report and inform the incident news to both internal and external related parties.

	Procedure: Business Continuity Plan: BCP	Doc. NO.: SOP-CHR-RM-001
		Doc. Sensitivity: Internal Use Only
		Effective Date: 01/01/2026
		Responsible by: Risk Management

Upon crisis occurrence

- 1) Monitor the situation, take photographs, and collect the incident information for use as evidence.
- 2) When the BCM Committee declares the crisis and activates the BCP, the BCM Committee and the sub-teams shall be coordinated to monitor the situational progress.
- 3) Inform the news information within the organization via communication channels as specified in the BCP, such as Call Tree, Website, E-mail, telephone number, etc.
- 4) Properly, quickly, and timely publicize news to the related third parties, such as customers, business partners, and mass media, after the resolution of the BCM Committee.
- 5) Report the situation and progress to the BCM Committee.

4. The Work Unit Executive and the Head

The Contingency Plan for the Critical Business Function under the responsibility shall be established to ensure operation continuity during a crisis or when an incident disrupts execution.

5. Internal Audit Department

Review the BCP plan regularly, at least once a year, to ensure it is practical and up-to-date.

6. Risk Management Department

- 1) Monitor, coordinate, and ensure the testing and review of the BCP plan as outlined, and report the results to the Risk Management, Good Governance, and Sustainability Committee.
- 2) Oversee the development, implementation, training, and regular updates of the BCP plan to keep it current.

7. BCP Coordinator of the Department

Pre-crisis occurrence

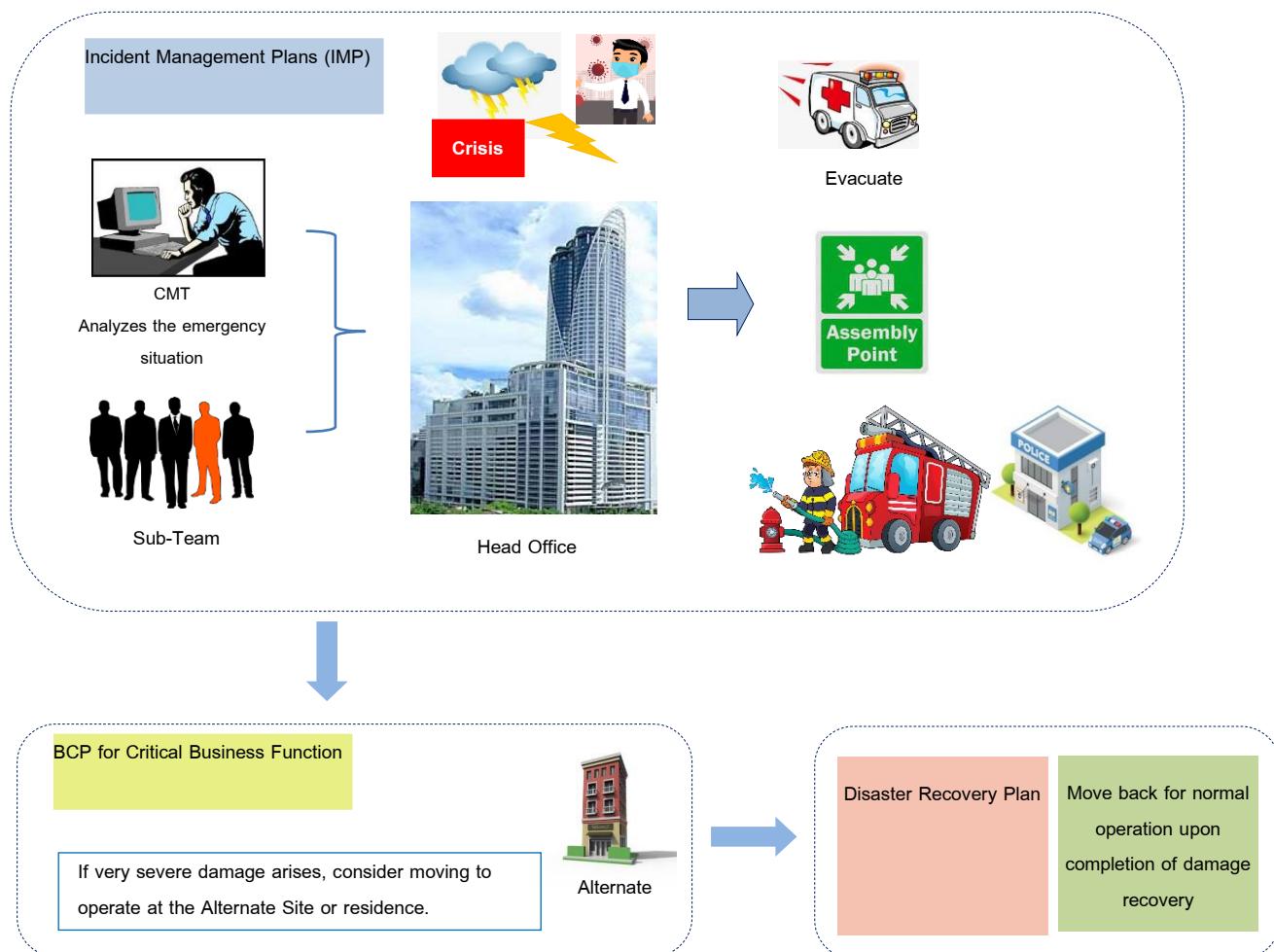
- 1) Prepare the information of the list of the important documents used in the work unit's operation and review to be updated.
- 2) Orderly control and oversee the work units to collect the important documents for on-hand convenience upon the incidence of the crisis event.
- 3) Supervise the work units to back up the information used in operation regularly.

Upon crisis occurrence

Other sub-teams are coordinated to be prepared for operation and supervise the operation in the crisis period, according to the BCP.

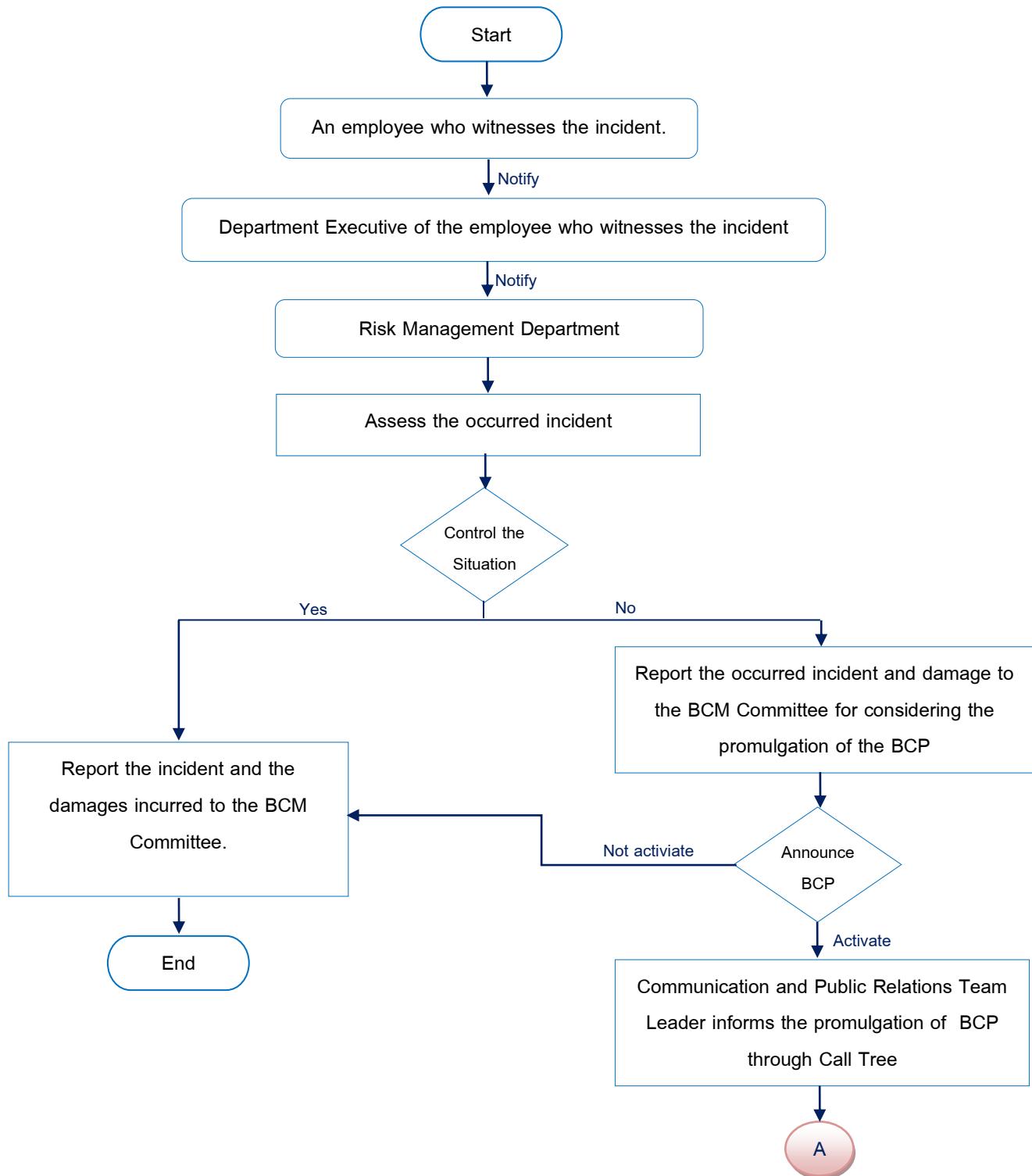
4.3 Contingency Plan at the Time of Crisis Event or Emergency Incident

4.3.1 Overview of the Business Continuity Management Plan



4.3.2 Announcement and Notification of the BCP Activation in Working Hours

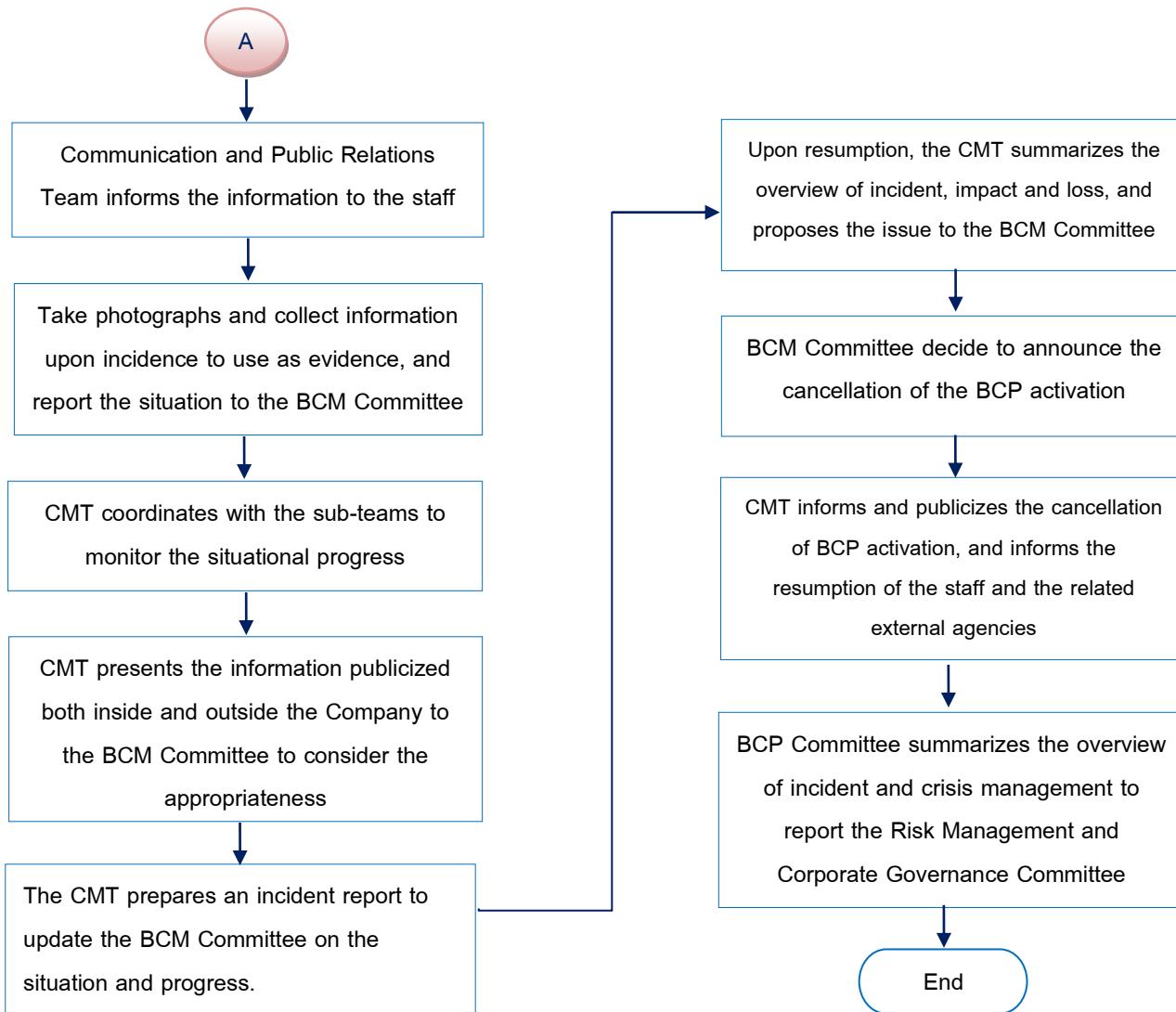
When a crisis or emergency incident occurs, the CMT shall primarily assess the severity of the incident. If the CMT deems that the incident damage is severe beyond its control, it will propose the issue to the BCM Committee to decide to immediately declare the crisis and start activating the BCP with the following procedure.



4.3.3 Communication and Public Relations upon the Crisis Declaration

➤ Communication and Public Relations Procedures

The Company determines the communication upon the promulgation of BCP by the BCM with the following procedure.

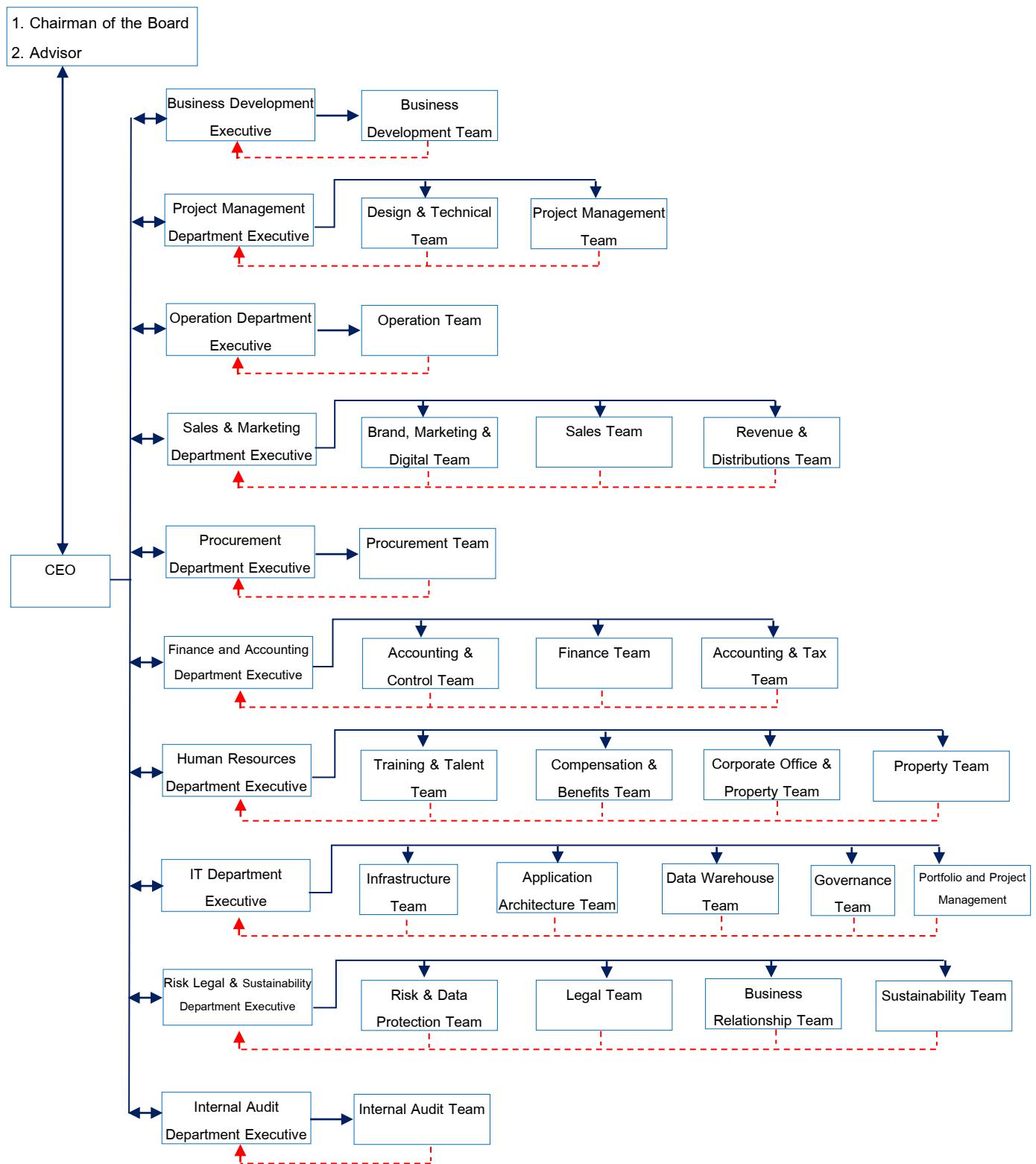


Remark :

In the case of the promulgation of BCP for a long time, the BCP Committee should continuously report the situation and management progress to the Risk Management, Corporate Governance, and Sustainability Committee

➤ Communication and Public Relations Procedure

The Company determines the communication upon the promulgation of BCP by the BCM Committee, with the following procedure.



	Procedure: Business Continuity Plan: BCP	Doc. NO.: SOP-CHR-RM-001
		Doc. Sensitivity: Internal Use Only
		Effective Date: 01/01/2026
		Responsible by: Risk Management

Practical Guidelines for Communication and Public Relations

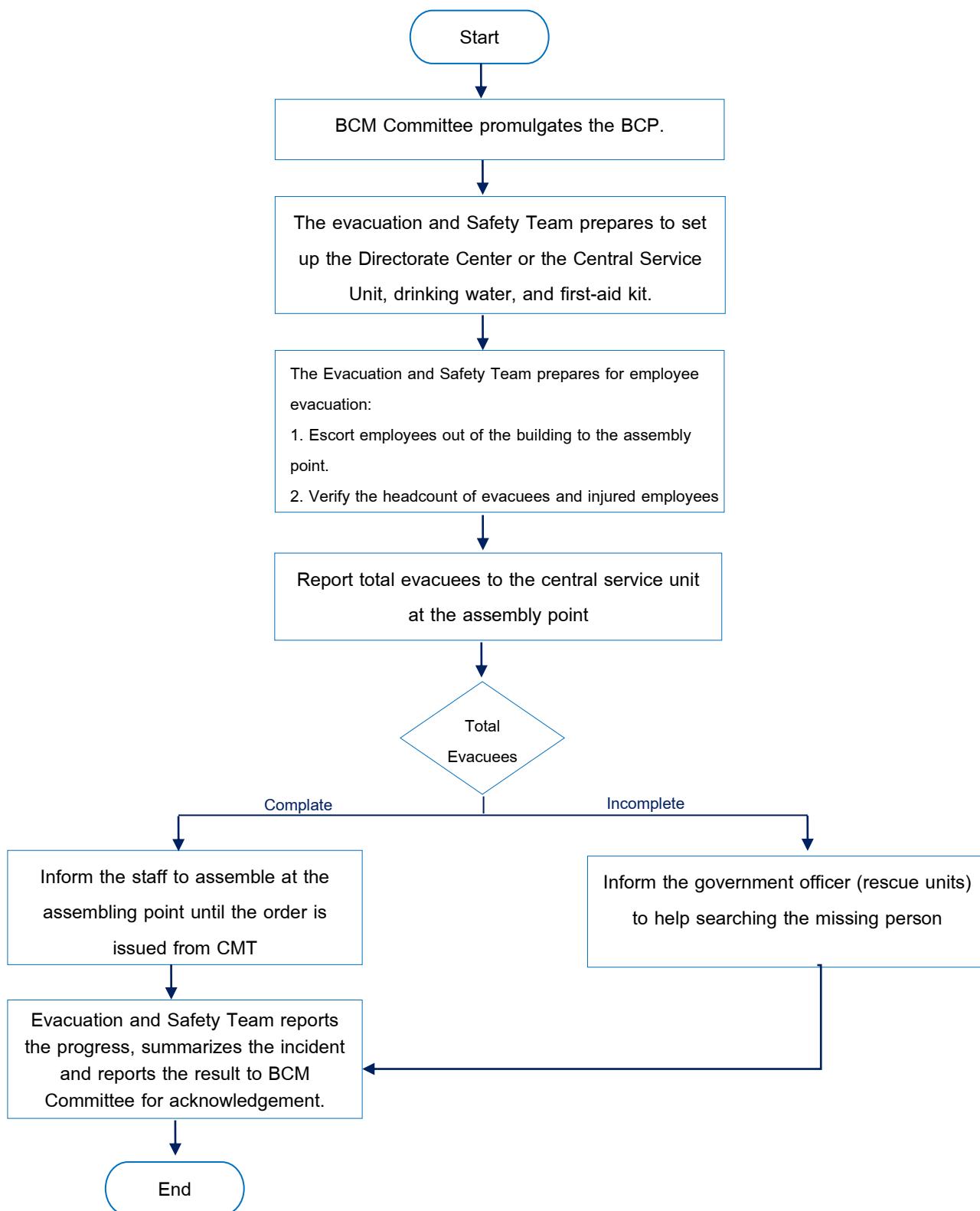
The Company determines the operation guidelines to communicate and publicize the incidents to third parties, where the Communication and Public Relations Team is mainly responsible for the following.

- 1) Inform the news via the communication channels (as deemed appropriate by CMT), and send to the business partners, customers, or related parties for acknowledgement about the location and contact telephone number of the Company, such as
 - SMS via mobile phones of all networks
 - Internet via Web site, Social Media of the Company
- 2) In the event that the news publishing must be organized for the mass media, the Communication and Public Relations Team shall arrange the venue and determine the person who acts as the spokesperson to publish news to the mass media to inform the location, and telephone number of the Company's Alternate Operating Site, including the occurred situation and the readiness of the Company to enable to resume the operation in the normal condition
- 3) Assign the Company's secretary to inform the related external regulatory agencies of the news.
- 4) Assign the Operations Department executive to inform business partners, customers, and third parties of the news.
- 5) Assign the Human Resources Department executive to inform the news to executives and staff for acknowledgement, respectively, and notify the news via the Company's Call Tree Structure.

4.3.4 Evacuation upon receiving notification of the activation of the BCP plan

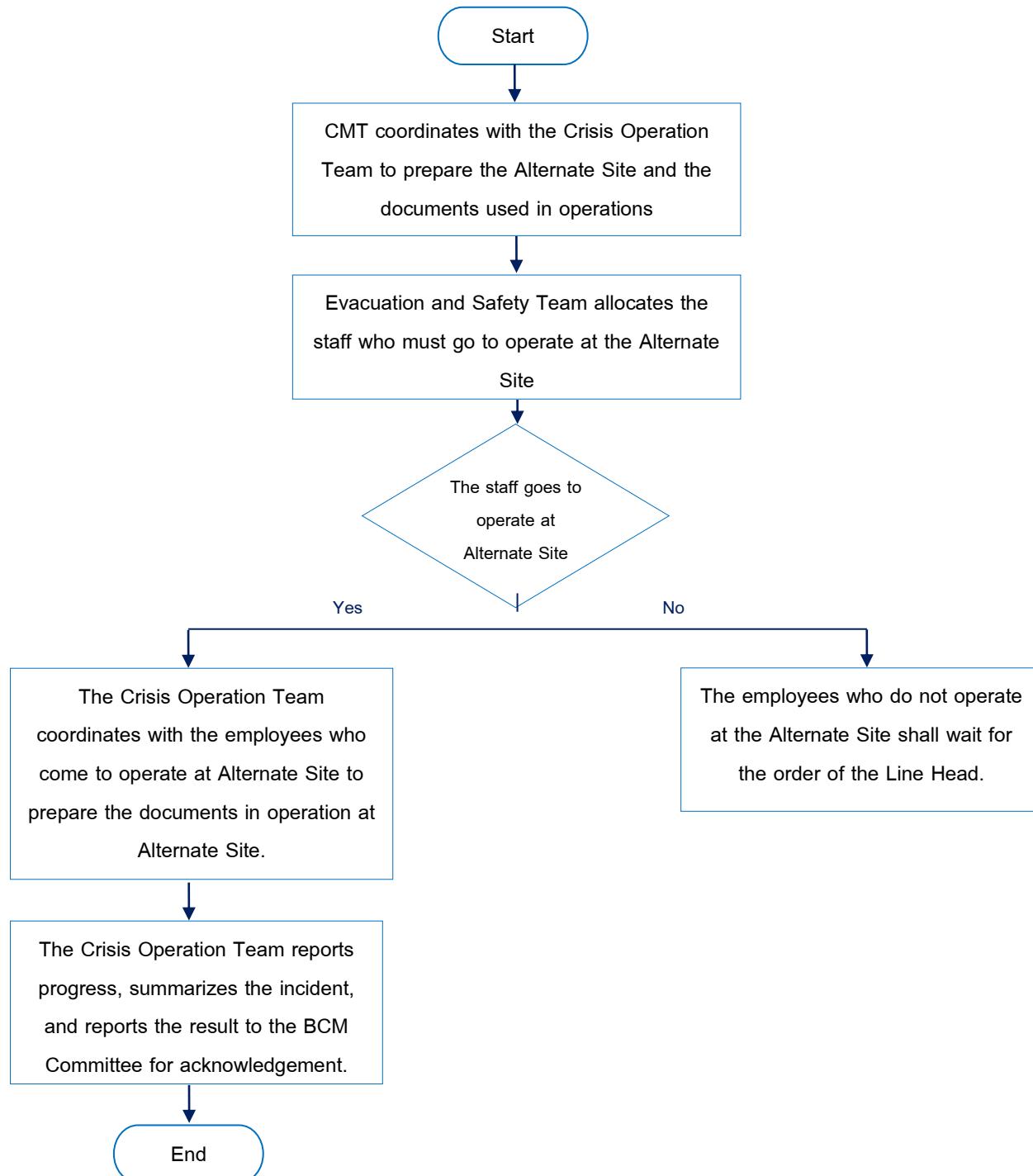
Evacuation procedure upon receiving notification of the activation of the BCP plan

The Company determines the evacuation procedure upon receipt of the notification on promulgation of BCP with the following procedure.



➤ Post-Evacuation Operation

The Company determines the post-evacuation procedure with the following procedure.



	Procedure: Business Continuity Plan: BCP	Doc. NO.: SOP-CHR-RM-001
		Doc. Sensitivity: Internal Use Only
		Effective Date: 01/01/2026
		Responsible by: Risk Management

➤ Practical Guideline for Evacuation

The Company formulates the guidelines for the staff evacuation from the building upon the incidence of emergency or casualty for safety and prevention to avoid turbulence until causing death and damage to the staff and the Company's properties, where the Evacuation and Safety Team is responsible for the following.

- 1) Coordinate with the BCP Coordinator of the Department to prepare the staff evacuation and documents used in operation in order based on the Critical Business Function in the crisis occurrence period.
- 2) Coordinate the Security Department of the building to prepare the staff evacuation out of the building.
- 3) The Evacuation and Safety Team prepares the guiding equipment used for the staff evacuation out of the building, such as guiding signboard on each floor, building layout, flashlight, whistle, etc.
- 4) The BCP Coordinator of the Department prepares the data of the name list of the departmental staff for use in checking the staff completeness after evacuation.
- 5) Arrange the area to set up the Directorate Center / Central Service Unit as the first-aid center.
- 6) Prepare the name list and telephone numbers of the rescue units: hospital, police station, fire station, public disaster mitigation units, including first-aid kits and drinking water, etc.
- 7) The BCP Coordinator of the Department prepares the departmental staff's evacuation from the building at the fire exit to the assembly point.
- 8) The BCP Coordinator of the Department checks the completeness of the departmental staff and the number of victims and reports to the Evacuation and Safety Team Leader.
- 9) The Central Service Unit carries out first-aid for the victim and coordinates the delivery to the hospital in cases with serious victims.
- 10) Allocate the staff who must go for operation at the Alternate Site.

4.3.5 Operating Procedure in the Case of the Event Incidence in Late Working Hours

The Company determines the announcement and notification procedure for the BCP activation during later working hours, with the following procedure.



4.3.6 Assembly Point

The Company determines the assembly point in the area in front of the gateway of Bangkok Convention Centre.



Remark:

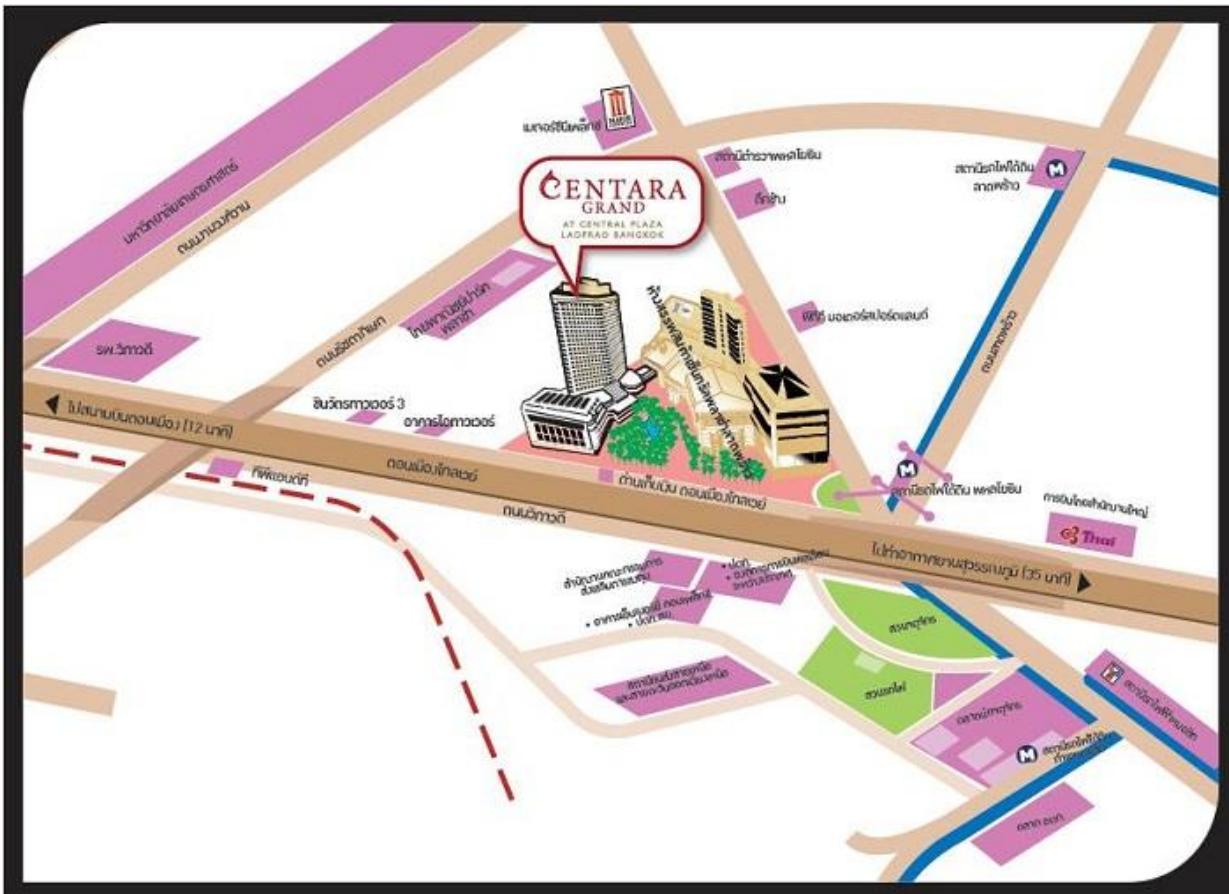
In the case of an incident that occurs in each hotel, the GM of each hotel is assigned to inform the staff or the related parties who are at that place about the assembling point.

4.3.7 Alternate Site

The Company determines an Alternate Site, which is the office at Centara Grand at Central Plaza Ladprao Bangkok (CGLB), that is the Alternate Site and Command Center in case a crisis occurs with the head office building, resulting in the staff's inability to enter for normal operation.

Business Function	Use in recovering the information technology system and as an Alternate Site in replacement of the emergency scene
Location of Alternate Site	1695 Phahon Yothin Road, Chatuchak Sub-district, Chatuchak District, Bangkok Metropolis
Telephone	0-2541-1234

Alternate Site Map Centara Grand at Central Plaza Ladprao Bangkok (CGLB) as follow:



4.4 Contingency Plan in the Case of the Emerging Infectious Disease Outbreak

4.4.1 Outbreak Period

The Company establishes the Business Continuity Plan to be consistent with the disease outbreak period determined by the Ministry of Public Health.

Phase No.	Outbreak Characteristics
1	<ul style="list-style-type: none"> Limited risk of the outbreak in a community A person in contact with a contagious disease comes from the origin of the first outbreak.
2	<ul style="list-style-type: none"> A continuous outbreak in the community in a narrow area A person's infection from anyone can be obviously explored in the person-to-person outbreak.
3	<ul style="list-style-type: none"> Widely and continuous outbreak in the community Any contagious person or source is unclearly known in the person's infection.

4.4.2 Workplace Contingency Plan

Outbreak	Plan-Based Implementation
Phase 1	<ol style="list-style-type: none"> 1. Security Preparedness Measures <ul style="list-style-type: none"> Determine the standards of building area access control. Determine the screening point and screening process. 2. Sanitation Measures <ol style="list-style-type: none"> 2.1 Preparation of the emerging infectious disease protective devices <ul style="list-style-type: none"> Prepare the Supplier List of the suppliers of the emerging infectious disease protective devices Prepare the list of type and quantity of the outbreak protective device usage, such as surgical masks, disposable gloves, thermometers, alcohol-based hand gels, floor cleaning disinfectants, and other equipment as necessary. Update the Supplier List and usage quantity of the infectious disease transmission protective devices at least once a year. Oversee and keep the area clean and sterilized. Formulation of the measures for area cleanliness care 2.2 Organizing the staff's training <ul style="list-style-type: none"> General information about the emerging infectious disease protection Knowledge about the use of the emerging infectious disease protective

Outbreak	Plan-Based Implementation
	<p>devices</p> <ul style="list-style-type: none"> Knowledge about cleanliness care in the state of the emerging infectious disease incidence. <p>3. General Measures</p> <ul style="list-style-type: none"> Determine the testing of the site and safety preparedness plan for supporting the emerging infectious disease outbreak once a year.
Phase 2	<p>1. Security Preparedness Measures</p> <ul style="list-style-type: none"> Review the established plan, such as the main operation site and alternate operation site preparation plan, including the criteria for considering the standards of building access control. Clarify and specify the staff's roles and duties that must be strictly carried out in the outbreak period. <p>2. Sanitation Measures</p> <ul style="list-style-type: none"> Supply the infectious protective devices. Inspect the quality and quantity of the reserved self-protective devices to be adequate for usability in the outbreak incidence period. Distribute the essential medical supplies, materials and protective devices for various groups of personnel on an importance basis. Clarify and reiterate the staff's duty that must be strictly carried out in the outbreak period.
Phase 3	<p>1. Security Measures</p> <p>1.1 Zoning Measures</p> <ul style="list-style-type: none"> Screening area at the building gateway area A waiting point for the visitors in the case of not being customers shall be arranged at the staff's entrance area. <p>1.2 Formulate the measures for building area access control where the pass of the screening process is required as follows.</p> <p>1.2.1 Define the screening point to have a regular officer at the point to perform the duty of screening the customers, the person who enters for operation or the third party who visits the Company, and record the medical examination result in the form of Building Access Permit.</p> <p>1.2.2 If the customer, staff, or third party are detected for the indicative symptom of the illness likelihood, they are strictly prohibited from accessing the area, and the customer, staff or third party are asked to</p>

Outbreak	Plan-Based Implementation
	<p>immediately see the physician together with the medical examination result.</p> <p>1.2.3 If the staff or the visitor passes the medical examination according to the determined standards, the said person shall perform as follows.</p> <ul style="list-style-type: none"> - Wear a basic protective device before entering the building area. - In the case of a third party, the visitor shall wait at the arranged area, and the Company's officer shall come out to meet at the waiting point. <p>1.2.4 The third party is not permitted to access the operation area unless accessing to execute for repairing and maintaining the office building, office equipment and supplies or computer program, affecting the Company's business operation. The third party shall pass the screening according to the Company's standards.</p> <p>1.3 Avoid or reduce interpersonal contact, avoid using the common area, such as a conference room, and use other communication systems instead of contact in the type of individual meeting or conference.</p> <p>2. Sanitation Measures</p> <ul style="list-style-type: none"> • Schedule more cleaning frequency. • Determine the equipment for individual use and prohibit other persons from sharing the equipment. • Daily spray disinfectant. <p>3. General Measures</p> <ul style="list-style-type: none"> • In the case of outbreak incidence in the workplace location area by the official announcement as the hazardous area, the staff shall move to operate at Alternate Site or other site specified by the Company, which is not in the epidemic disease zone according to the Public Health's announcement.
Resumption	<p>1. Security Measures</p> <ul style="list-style-type: none"> • Cancel the limitation of the working area. • Notify the third parties about the cancellation of the screening measures for the building access. • Arrange the operation area for the work units as before. • Gather the operation problems of the security officer to amend the training manual and measures to be suitable and consistent with the situations. <p>2. Sanitation Measures</p>

Outbreak	Plan-Based Implementation
	<ul style="list-style-type: none"> Survey the remaining outbreak protective devices to purchase at the suitable level. Review the name list of suppliers of the protective devices to be updated. Clean the area used in an operation, office equipment and air-conditioning system. Gather the operation problems of the cleaning officer to amend the training manuals and measures to be suitable and consistent with the situations.

4.4.3 Personnel Contingency Plan

Outbreak	Plan-Based Implementation
Phase 1	<ol style="list-style-type: none"> Creation of the staff knowledge understanding, and preparedness for the incidence of emerging disease <ul style="list-style-type: none"> Create the staff's awareness to help brainstorm in solving the problems and participate in finding the preventive method. Prepare the training plan for the understanding and recognition of all staff on the preparedness procedure upon the occurrence of an outbreak situation to understand the situation, resulting in the preparedness when encountering the actual situation, the staff can satisfactorily respond to the situation and reduce the staff's terror and anxiety. Educate the staff about self-protection, such as hand washing, cough and sneeze manners, and self- and family member care method in case of ailment at home. Prevention of transmission and supply of the physical protective devices and necessary devices for the staff <ul style="list-style-type: none"> Prepare and supply adequate personal protective devices, such as disposable surgical masks/gloves, to be usable, and prevent respiratory infection. Prepare the supply of medical instruments, such as body thermometers, in an adequate number for usability. Prepare the supply of adequate hand sanitizer / waterless hand cleansing cream Prepare the supply of adequate disinfectant for floor/toilet cleaning Specify the name list of the key organizations for the information and

Outbreak	Plan-Based Implementation
	suggestions of the emerging infectious disease outbreak.
Phase 2	<ol style="list-style-type: none"> 1. Announce to warn the staff for acknowledging the outbreak situation for the staff's avoidance of traveling in the outbreak area. 2. Monitor the outbreak news, and coordinate with the public service unit in the area where the office is located.
Phase 3	<ol style="list-style-type: none"> 1. The staff who travels in the risky area or travels back from the risky area must pass the physical examination as determined by the Company about the emerging infectious disease before resuming his/her work. 2. Control at the time of outbreak incidence <ul style="list-style-type: none"> • Assign each work unit to report to the Human Resource Management Department when the staff in the work unit is ill with an emerging infectious disease or is sicken. • Reduce the staff's congestion in the working hours period. • Measure everyone's temperature before entering the working area. • Arrange the working distance between the persons for at least 3 feet or according to the Public Health's announcement. • The staff who gets better shall declare the Medical Certificate when resuming for working. 3. Workplace Sanitation Management <ul style="list-style-type: none"> • Determine to take every staff's temperature when the outbreak situation is in Phase 3. • If the staff who is febrile over 37.5 °C or according to the Public Health's announcement, is detected, he/she shall comply with the advice of the screening guidelines. 4. Prepare the Registration showing the staff's status, illness, and death as the result of emerging infectious disease, and assist in welfare according to the staff's rights. 5. Promulgate the policies formulated in the crisis incident period. <p>Remark: The Company may adjust the appropriate working hours for the staff, such as:</p>

Outbreak	Plan-Based Implementation
	<ul style="list-style-type: none"> - Reduce operation hours. - Assign the staff to perform shift work. - Assign the staff who can work in replacement to alternate for entering to operate or working from home. <p>However, the selection of operation period for the staff depends on the discretion of the Company's executives and the severity of the disease outbreak.</p>
Resumption	<ol style="list-style-type: none"> 1. Monitor news of the emerging infectious disease outbreak situation from the government agencies and media. When the outbreak situation starts decelerating or settling, the BCM Committee shall be reported for acknowledgment. 2. Notify the outbreak situation in the country for the staff's acknowledgment and regularly provide the information to the staff to reduce anxiety. 3. Survey the remaining number of staff of all Departments in the Company to consider the adequacy and suitability of each Department. 4. Carry out according to the emerging infectious disease outbreak backup policy, such as remuneration payment and right of leave for the staff according to the obtained right. 5. Review the action policy and plan to be suitable and consistent with the outbreak situation.

4.4.4 Communication Contingency Plan

Outbreak	Plan-Based Implementation
Phase 1	<ol style="list-style-type: none"> 1. Prepare the name list and telephone numbers of the staff, business partners, suppliers, and others. 2. Prepare the means and contents used to inform customers and people of the news in case of the illness of the Company's staff with an emerging infectious disease. 3. Prepare the incident announcement and notification procedure for the staff's acknowledgment using various means, such as Email or LINE.
Phase 2	Publicize the staff via Email or LINE to be informed of the Phase 2 outbreak situation.
Phase 3	1. Publicize the staff's acknowledgment via Email or LINE to be informed of the Phase 3 outbreak situation, and conduct a method according to the Business Continuity Plan in the case of the emerging infectious disease outbreak.

Outbreak	Plan-Based Implementation
	2. Publicize the customer's acknowledgment via the Company's website.
Resumption	<ol style="list-style-type: none"> 1. Publicize the staff's acknowledgment via Email or LINE to be informed of the decelerating or settling outbreak situation for the staff's preparation to enter regular operation. 2. Publicize the Company's services that are prepared to be resumed for the customer's acknowledgment via various channels, such as the Company's website.

4.4.5 Operation Continuity Plan for the Department

Outbreak	Plan-Based Implementation
Phase 1	<ol style="list-style-type: none"> 1. The Department determines the Critical Business Function, the name list of the staff who are the main operators and alternate operators, and must operate at the head office and from home. 2. Formulate the risk mitigation measures to ensure that the services of the critical business functions can be continued in the outbreak incidence period. 3. The Department with the Critical Business Function participates in testing for preparedness in the related aspects, such as testing Work from Home.
Phase 2	<ol style="list-style-type: none"> 1. Monitor and listen to the outbreak announcement from the Company and prepare compliance with the Business Continuity Plan in the case of an emerging infectious disease outbreak. 2. The department executive considers and reviews the operation process needed to be used in operation to ensure the action in the infectious disease outbreak period.
Phase 3	<ol style="list-style-type: none"> 1. Closely monitor and listen to the disease outbreak announcement from the Company. 2. Oversee and control the staff to strictly comply with the Business Continuity Plan in the case of an emerging infectious disease outbreak. 3. Report the occurred situations and problems to CMT.
Resumption	<ol style="list-style-type: none"> 1. Closely monitor the emerging infectious disease outbreak situation from the Company's media. 2. Upon the deceleration or settlement of the outbreak situation, each work unit's executives / responsible persons shall notify the staff in their affiliations to be ready for entering to operate as usual. 3. The work unit shall gather the problems that occurred during the operation in the

Outbreak	Plan-Based Implementation
	<p>emerging infectious disease outbreak period to CMT to develop the working system to be more efficient in the following time.</p> <p>4. Amend the action plan of the work unit to be consistent with the outbreak situation.</p>

4.5 Recovery Plan

The Company has formulated practical guidelines for recovering the damage after a severe crisis incident and recovering when the incident has been peaceful, or the incident has been suppressed for the Company's resumption as follows.

No.	Action	Responsible Person	Duty
1	Security	GM and Operations Section	<p>1) Oversee and maintain the property's safety</p> <p>2) Coordinate the renovation of the building and premises to be restored for normal execution.</p> <p>3) Oversee the access and ask for the building access permission for resumption.</p>
2	Restoration of Buildings and Resources	GM, Operations Section, Risk Management and Law Section	<p>1) Inspect and assess the damage to the main operating site.</p> <p>2) Inspect and assess the damage to the properties and infrastructures.</p> <p>3) Improve and repair the properties and infrastructures.</p> <p>4) Claim the insurance</p>
3	Recovery of Information System	Information Technology Section	<p>1) Inspect and assess the system damage.</p> <p>2) Recover the Computer and Network Systems</p> <p>3) Improve and repair the computer hardware</p> <p>4) Claim the insurance</p>
4	Human Resource Recovery	Human Resource Section	<p>1) Examine the injured staff, and assist and support the restoration of the staff's morale and courage</p> <p>2) Oversee the matters of welfare and reward.</p>
5	Communication and Public Relations	Communication and Public Relations Team	Report the situation and notify the readiness to all staff and the related external agencies.

	Procedure: Business Continuity Plan: BCP	Doc. NO.: SOP-CHR-RM-001
		Doc. Sensitivity: Internal Use Only
		Effective Date: 01/01/2026
		Responsible by: Risk Management

4.6 BCP Testing and Review

4.6.1 BCP Testing

The Company schedules the testing of the Business Continuity Plan (BCP) at least once a year or upon the change in factors affecting the risk of the disruption of significant operations in the business operation.

During the plan testing process, the Risk Management Department will determine the appropriate testing format and ensure participation from stakeholders at all levels. The planned testing is categorized into three groups as follows:

- 1) Conducting a joint rehearsal with various departments in a Company meeting to review the steps to be taken during a business disruption.
- 2) Conduct operational tests at the alternate site to verify equipment functionality and ensure readiness at least once annually or whenever there are changes to the related system.
- 3) Conduct a full-scale test to assess the management of departments, work processes, equipment, and the backup workplace, ensuring that the BCP plan can be effectively executed.

4.6.2 BCP Review

The Company schedules the review of the Business Continuity Plan (BCP) at least once a year as follows.

- 1) The related work units, as specified in this BCP, are determined to review the name list and telephone numbers of the related work units and personnel every 6 (six) months.
- 2) The BCP review shall be performed once a year or every change in the work process or related operating systems.

Annex 1: Checklist of the Staff in Work Unit in Evacuation Procedure
Checklist of the Employees in Work Unit

Work Unit :

Contact Person: Hotel: Floor No:

No	Name List	Contact Number	Status (Present/Absent)
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Total Number of Staffs who attend work on that date persons

 Summary of Total Staff Evacuation Complete in the work attending number on incidence
 date

..... Incomplete in the absent number for persons

Number of Injured Staffs for persons

Number of Dead Staffs for persons

Recorder.....

Date.....

Remark: It is the Checklist for Contact Persons of the Work Unit used in checking the name list of the staffs in its work unit whether they completely evacuate from the building.

Annex 2: Notification of Incident

Notification of Incident	
Work Unit : BCP Coordinator: Hotel :	
<i>Upon the incidence, the department executive of the staff who detects the incident or BCP Coordinator shall record the below detail as follows.</i>	
1. Brief Detail of the Occurred Situation or Incident Site : Date : Time : Troublemaker : Detail of Incident : Timeline : Cause :	
2. Primary Impact Assessment Deceased : Victim : Damage : Damage Value :	
3. Other Related Information 	
Recorder..... Date.....	

Annex 3: List of Incident Impact Assessment

Incident Impact Assessment Report																																			
Acquired Impact																																			
Date/Time of Incidence.....	Scene																																		
Personnel Impact – Death Quantity	Injury Quantity																																		
Workplace Impact	<input type="radio"/> Unable to enter for working. <input type="radio"/> Able to enter, but the infrastructure is damaged. <input type="radio"/> Able to enter for regular working.																																		
Emergency Agencies at the Scene	<input type="radio"/> Police Station	<input type="radio"/> Fire Brigade	<input type="radio"/> Ambulance																																
Affected Critical Operation Process:																																			
Impact Assessment Opinion regarding the personnel's health and safety:																																			
Summary of the Impacts <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Summary of the Impacts</th> <th style="width: 40%;">Estimated Damage Value</th> <th style="width: 30%;">Remark</th> </tr> </thead> <tbody> <tr> <td>1. Building Access and Damage</td> <td></td> <td></td> </tr> <tr> <td>2. Damaged Area Impact</td> <td></td> <td></td> </tr> <tr> <td>3. Damaged Area Recovery</td> <td></td> <td></td> </tr> <tr> <td>4. Tools/Infrastructures</td> <td></td> <td></td> </tr> <tr> <td>5. Operation</td> <td></td> <td></td> </tr> <tr> <td>6. Important Information/Important Document</td> <td></td> <td></td> </tr> <tr> <td>7. Electrical System</td> <td></td> <td></td> </tr> <tr> <td>8. Waterworks System</td> <td></td> <td></td> </tr> <tr> <td>9. Information in the Computer System</td> <td></td> <td></td> </tr> <tr> <td>10. Others (please specify.....)</td> <td></td> <td></td> </tr> </tbody> </table>			Summary of the Impacts	Estimated Damage Value	Remark	1. Building Access and Damage			2. Damaged Area Impact			3. Damaged Area Recovery			4. Tools/Infrastructures			5. Operation			6. Important Information/Important Document			7. Electrical System			8. Waterworks System			9. Information in the Computer System			10. Others (please specify.....)		
Summary of the Impacts	Estimated Damage Value	Remark																																	
1. Building Access and Damage																																			
2. Damaged Area Impact																																			
3. Damaged Area Recovery																																			
4. Tools/Infrastructures																																			
5. Operation																																			
6. Important Information/Important Document																																			
7. Electrical System																																			
8. Waterworks System																																			
9. Information in the Computer System																																			
10. Others (please specify.....)																																			
Summary of the Overall Impacts																																			

 Assessor.....

(.....)

Assessment Date

Annex 4: Emergency Call Numbers

รวมเบอร์โทรฉุกเฉิน



Emergency Call

				
Emergency-Accident	1784 Disaster Prevention and Mitigation	191 Emergency Police Service	199 Fire-Fierce Animal Report	1195 Crime Suppression Division
	 1133 Search of TOT Telephone Numbers	 1546 Labor Protection		
	 1554 Vajira Hospital Emergency Medical Service	 1555 Bangkok Emergency Medical Service	 1646 Bangkok Erawan News	 1669 National Institute for Emergency Medicine
Resuscitation- Rescue	 1691 Police General Hospital Ambulance Service	 1860 National Disaster Warning Center		
	 1129 Provincial Electricity Authority	 1130 Metropolitan Electricity Authority	 1125 Provincial Waterworks Authority	 1662 Metropolitan Waterworks Authority