Business Continuity Management Policy

Risk Management Department	Effective Date 11 August 2026	Version 1, Revision No. 00

Prepared by	Reviewed by	Approved by
Ms. Apichaya Phongpreecha	Mr. Cherdpong Siriwit	Mr. Prasert Bunsumpun
Risk Management Department	Chairman of the Risk Management Committee	Chairman of the Board of Directors

1. Introduction

Thoresen Thai Agencies Public Company Limited (the "**Company**") recognizes the importance of conducting its business without interruption and of being able to respond to events or incidents that may disrupt business operations, whether arising from factors internal or external to the Company. The Company has therefore established this Business Continuity Management Policy (BCMP) to serve as a framework for preventing, preparing for, responding to, and recovering its critical operations to normal status, or to a level the Company has determined to be acceptable, within an appropriate timeframe and in an effective manner, under appropriate risk management and in alignment with the Company's business objectives, applicable laws, and the expectations of its stakeholders.

2. Business Continuity Objectives

- To maintain preparedness for crises or threats that may disrupt operations, to enable critical work processes to be recovered within the defined timeframes, and to enable the Company to continue delivering services and meeting the needs of its stakeholders without interruption.
- To ensure that the Company's Business Continuity Management System (BCMS) is developed and improved in line with international standards and kept current with changing internal and external circumstances.
- To build knowledge and understanding of the operation of the Business Continuity Management System (BCMS) among the Company's key stakeholders.
- To build awareness of the importance of the Business Continuity Management System (BCMS) among management and all employees, leading to their participation in, support for, and compliance with the Company's Business Continuity Management Policy (BCMP), so that its objectives are achieved correctly and in a timely manner, with the welfare and safety of people treated as the foremost consideration.
- To ensure that the Business Continuity Management System (BCMS) established by the Company can be implemented effectively, with management and all employees able to perform the duties and roles assigned to them under the Business Continuity Management System (BCMS) fully and correctly, and with the system reviewed and kept up to date on a regular basis, so that critical operating processes, together with personnel, work premises, information technology systems, data, and other necessary resources, are ready and can be

deployed to support business operations in the event of an event or incident giving rise to a crisis or to threats of any kind.

3. Definitions

Term	Description
Business Continuity	The capability of the Company to continue operating at a level acceptable to the Company following an event that disrupts its operations.
Business Continuity Management (BCM)	A holistic management process that identifies potential threats to the Company and the impact of those threats on business operations, and that establishes an approach for building the Company's capability to respond to and recover from disruptive events, so as to protect the interests of key stakeholders, the reputation and image of the Company, and its value-creating activities.
Business Continuity Management System (BCMS)	That part of the overall management system comprising the planning, establishment, implementation, operation, monitoring, review, maintenance, and improvement of the Company's business continuity, and used to establish, implement, operate, monitor, review, maintain, and continually improve business continuity management.
Business Continuity Plan (BCP)	Documented procedures that guide the Company in responding to, recovering from, and continuing operations during a disruptive event, and in restoring operations to a predefined level.
Recovery Time Objective (RTO)	The target period, measured from the time of an event or incident that disrupts business operations, within which the relevant activities, processes, or resources must be recovered to the minimum level defined and accepted by the Company.
Maximum Tolerable Period of Disruption (MTPD)	The maximum period for which the Company can tolerate the disruption of a critical activity; beyond that period, the impact may reach a level the Company cannot accept.
Recovery Point Objective (RPO)	The target point in time to which information must be recovered following an event or incident that disrupts business operations. It defines the maximum volume of information the Company is prepared to lose, determined by the interval between the most recent data backup and the time of the event or incident.

Term	Description
Disaster Recovery Plan (DRP)	A recovery plan prepared by the Company to establish readiness to restore systems, data, or information technology infrastructure following an unexpected event or incident, such as fire, earthquake, flood, information system failure, or cyberattack, so that information technology systems and services can be returned to use within the defined timeframes and to the defined levels, and so as to reduce the potential impact.
Information Technology Business Continuity Plan (IT BCP)	A business continuity plan setting out the approach, roles, duties, and procedures required for critical information technology systems and services (Critical IT Services) to continue operating with minimal disruption, or to be recovered within the defined timeframes and to the defined levels, during or following a crisis.
Business Impact Analysis (BIA)	The process of analyzing the Company's activities and operating processes in order to assess the potential impact of disruption, determine recovery priorities, and define the target timeframes and the resources required to recover critical activities or operations.
Crisis	An event, incident, or disaster that may disrupt business operations or service delivery, and that may affect personnel, assets, systems, data, reputation, stakeholders, or the achievement of the organization's objectives.
Personnel	Employees, workers, and external service providers.

4. Scope

The Company has determined that every department within the Company falls within the scope of its Business Continuity Management System (BCMS). Each department must systematically analyze its operating environment and business impact in order to identify critical activities and operating processes and to establish measures for responding to events that give rise to a crisis or that disrupt business operations. The Company will identify, review, and group the activities and processes relevant to the Business Continuity Management (BCM) on a regular basis, or whenever a significant change occurs, based on the results of the Business Impact Analysis (BIA) and the related risk assessment. The activities and processes falling within the scope of the Business Continuity Management System (BCMS) for the year 2026 are as follows:

4.1 Departments within scope

- BPA & Consolidation
- Corporate Finance & Accounting
- Treasury and Investor Relations
- Business Development

- Corporate Affairs
- Corporate Administration
- CEO Office and Support Team
- Corporate Communications
- Corporate Human Resources
- Information Technology
- Internal Audit, Compliance & Risk Management
- Corporate Legal

4.2 Location

Thoresen Thai Agencies Public Company Limited is located at 26/26-27 Orakarn Building, 8th Floor, Soi Chidlom, Ploenchit Road, Lumpini Sub-district, Pathumwan District, Bangkok 10330.

5. Business Continuity Framework

The Company has applied the Plan-Do-Check-Act (PDCA) management cycle and the business continuity management lifecycle (BCM Lifecycle), in accordance with international standards and the Good Practice Guidelines (GPG), in developing its Business Continuity Management System (BCMS). The framework comprises the following principal stages:

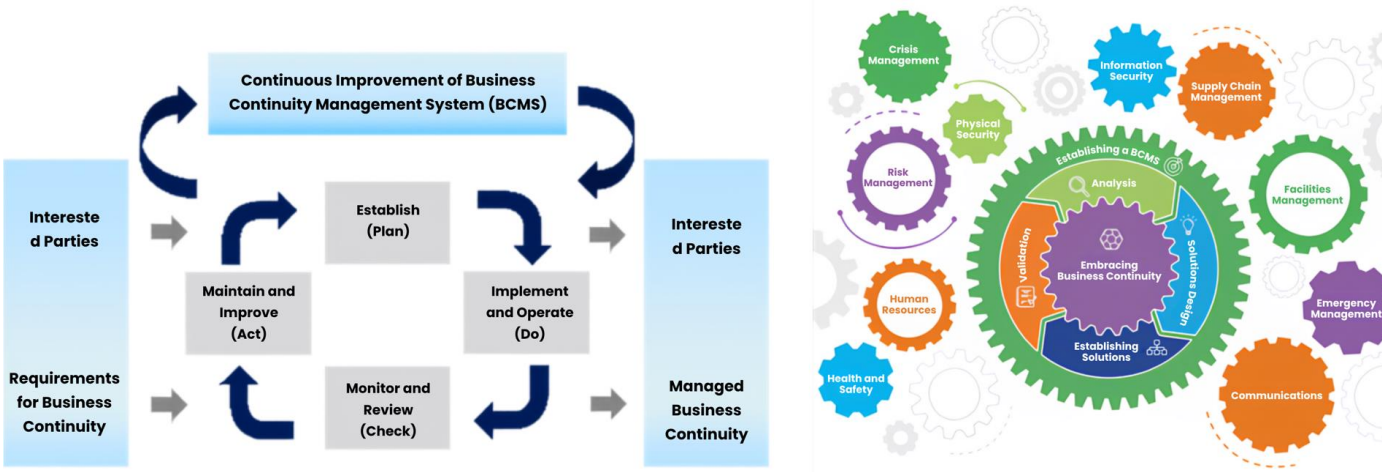
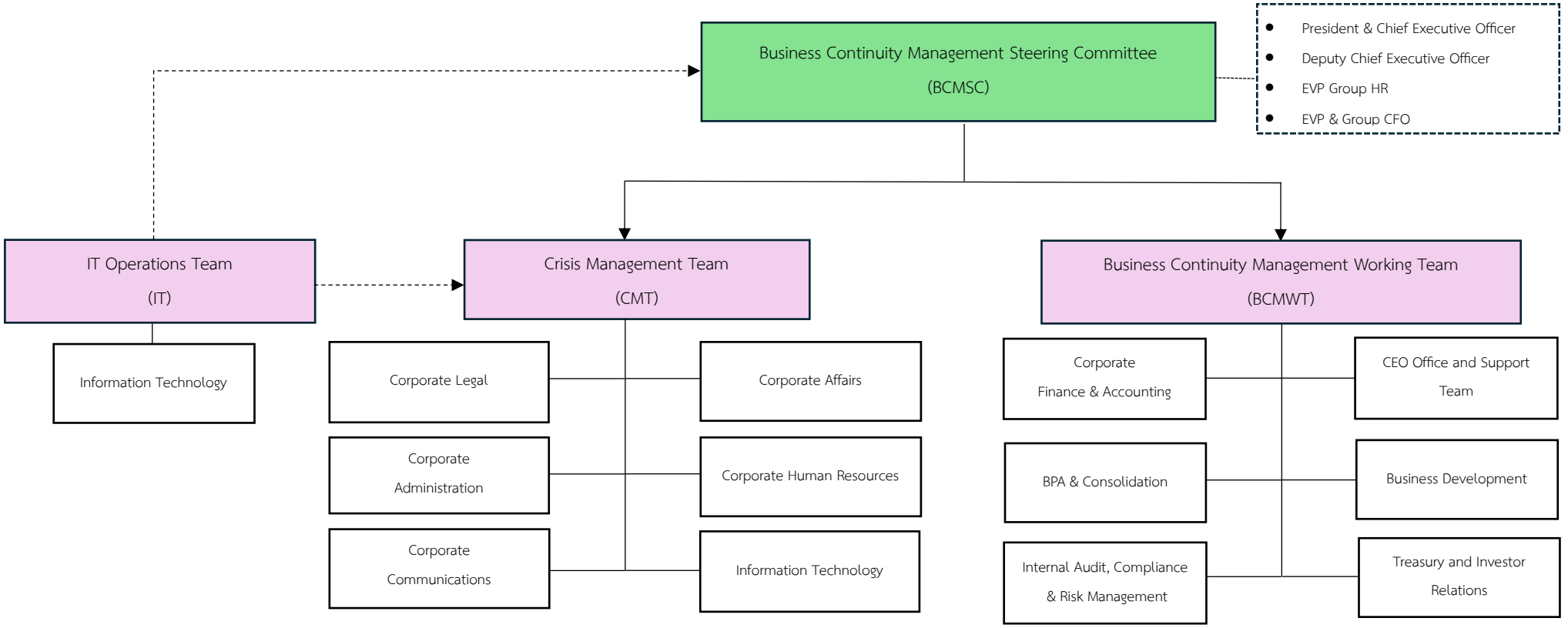


Figure 1: PDCA Model and BCM Lifecycle1

PDCA	Description	BCM Lifecycle
Plan	Establish the Business Continuity Management Policy (BCMP), together with the objectives, targets, controls, processes, and procedures relating to the development of business continuity, in alignment with the Company's overall policy and objectives.	▪ Establishing a Business Continuity Management System (BCMS) ▪ Embedding Business Continuity
Do	Implement the Business Continuity Management Policy (BCMP) and the related controls, processes, and procedures.	▪ Analysis ▪ Designing Solutions ▪ Enabling Solutions ▪ Validation
Check	Monitor and review performance against the policy and business continuity objectives, and report performance to management so that the effectiveness of the system can be assessed and corrective or improvement actions determined as appropriate.	▪ Performance Evaluation ▪ Internal Audit ▪ Management Review
Act	Maintain and improve the Business Continuity Management System (BCMS) by taking corrective and improvement actions based on the results of monitoring, auditing, and management review, and by reviewing the scope of the Business Continuity Management System (BCMS), the policy, and the business continuity objectives so that they remain suitable and effective on an ongoing basis.	▪ Improvement

6. Roles and Responsibilities

6.1 Business Continuity Management Governance Structure



6.2 Roles, Duties, and Responsibilities

6.2.1 Business Continuity Management Steering Committee (BCMSC)

1) Under normal conditions

- Oversee the business continuity management (BCM) process of every department within the Company so that it is carried out effectively.
- Establish the operating policy for the Company's Business Continuity Management System (BCMS), using ISO 22301 as the guiding standard.
- Approve and review the Company's Business Continuity Management System (BCMS), together with the approach for developing and improving it so that it remains current and consistent with changing circumstances.
- Support, assist, and provide recommendations on the development of the Business Continuity Management System (BCMS) and on preparedness for crises that may disrupt the Company's operations.
- Consider and approve the budget required to support the Company's business continuity management (BCM) activities so that their objectives are achieved.

2) During a crisis

- Consider and issue directions on the activation of, the execution of, and the stand-down from the Business Continuity Plan (BCP).
- The President & Chief Executive Officer has the authority to decide on the activation of, and the stand-down from, the Company's Business Continuity Plan (BCP). Where the President & Chief Executive Officer is unable to perform this duty, the Deputy Chief Executive Officer shall exercise that authority instead, unless the Company has designated another authorized person in writing.
- Assess the situation, set strategy, and issue further directions where an unforeseen event or incident occurs or where the situation differs from that contemplated in the Business Continuity Plan (BCP).
- Monitor and oversee the execution of the Business Continuity Plan (BCP) while the event or incident is ongoing, so that the impact of the situation can be controlled or mitigated promptly and so that the Company's critical operations can continue or be recovered within the defined timeframes and to the defined levels.

3) In the post-crisis phase

- Direct the restoration and refurbishment of the office so that it can be used as a normal workplace.
- Approve the office restoration plan so that the office can be used as a normal workplace.
- Oversee the recovery of the Company's operating processes, information technology systems, personnel, and critical resources to normal status or to a level the Company has determined to be acceptable.
- Require a review of the response to the event or incident, of the causes of the disruption, and of the problems and deficiencies identified, and require corrective measures and improvements to the Business Continuity Plan (BCP) in order to prevent recurrence.

6.2.2 Crisis Management Team (CMT)

1) Under normal conditions

- Consider and review threats annually, covering both physical and cyber security threats, and review and update the business impact analysis and the risk assessment so that they cover cyber threat risks such as ransomware, cyberattack, data breach, malware, and phishing, as well as disruption of information technology systems.
- Arrange exercises and tests of the Company's personnel evacuation plan for events or incidents that render the office unusable for normal work, and review and test the cyber security incident response plan jointly with the Information Technology department and other relevant departments. Such activities may take the form of a tabletop exercise and shall be conducted at least once (1) a year.
- Control and oversee the prevention and mitigation of public hazards, as well as the prevention of information technology and cyber security threats, in an efficient and effective manner.
- Monitor and assess situations that may arise, establish warning systems, and define measures for life-saving, rescue, evacuation, and assistance to the injured, as well as for cyber incident response.
- Coordinate with the Information Technology department and other relevant units in monitoring, detecting, analyzing, and responding to cyber security anomalies, and oversee the performance of data backups and the testing of data recovery capability at the defined intervals.

2) <u>During a crisis</u>

- Coordinate requests for assistance from external agencies, such as the fire station, police station, hospitals, information technology service providers, cloud / data center service providers, and the relevant regulatory authorities.
- Inspect and carry out an initial damage assessment of the office, information technology systems, network systems, databases, and information assets when a crisis affects the office or when a cyber security incident occurs, such as a cyberattack, ransomware, malware, phishing, data breach, system intrusion, or leakage of sensitive information, as well as disruption of information technology systems.
- Assess the severity of the situation, the impact on the Company, and the harm to personnel, critical processes, the primary work premises, facilities, and information technology systems, together with the extent of the damage and the severity level of the incident, including cyber security incidents such as cyberattack, ransomware, malware, phishing, or data breach, and disruption of information technology systems, and report to the Business Continuity Management Steering Committee (BCMSC).
- Report the results of the damage assessment, together with recommendations and proposed courses of action, to the Business Continuity Management Steering Committee (BCMSC) for its consideration in activating the Business Continuity Plan (BCP).
- Evacuate employees to the assembly point, provide first aid to the injured, and coordinate the prompt transfer of injured or ill persons for medical treatment.
- Direct, control, and monitor the progress of recovery activities, and report periodically to the Business Continuity Management Steering Committee (BCMSC).
- Monitor the situation until the crisis or incident has been controlled or resolved, and communicate progress to the Company's employees and personnel through the channels and in accordance with the communication criteria prescribed by the Company.
- Prepare and maintain a record of events, decisions, directions, and related actions (Incident Log), and report progress to the Business Continuity Management Steering Committee (BCMSC).
- In the event of ransomware or a data breach, the Information Technology department shall contain the incident, carry out an initial assessment of its scope and impact, and report it to the Crisis Management Team (CMT) immediately and in any event within one (1) hour of becoming aware of it. The Crisis Management Team (CMT) shall coordinate with the

Information Technology, Corporate Legal, and Corporate Communications departments in order to act in accordance with the Incident Severity Levels (P1-P4), and shall immediately notify the Data Protection Officer (DPO) where a personal data breach occurs or is suspected, including any loss of, or unauthorized or unlawful access to, use of, alteration, amendment, or disclosure of, personal data. The Corporate Legal department, the Data Protection Officer (DPO), and the relevant departments shall jointly assess the nature, scope, and risk level of the incident and shall ensure that the Company notifies the Office of the Personal Data Protection Committee of the breach without delay and, where feasible, within seventy-two (72) hours of the Company becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Where the breach is likely to result in a high risk to the rights and freedoms of individuals, the Company shall also notify the data subjects of the breach and of the remedial measures without delay. All of the foregoing shall be carried out in accordance with applicable laws and regulations.

3) *In the post-crisis phase*

- Inspect and assess damage to the office building, as well as to information technology systems, network systems, databases, and information assets, following a crisis or a cyber security incident.
- Coordinate and oversee the restoration or repair of the damaged office building so that it is returned to a safe and normally usable condition, or to a level acceptable to the Company, and oversee the recovery of information technology systems, critical systems, and information so that they can be returned to use within the defined timeframes and to the defined levels, together with verification of the accuracy, completeness, integrity, and security of the systems and data following recovery.
- Report the results of the assessment of the usability of the office building and of the information technology systems, as well as the readiness of personnel, operating processes, and critical resources, to the Business Continuity Management Steering Committee (BCMSC) for its consideration in standing down the Business Continuity Plan (BCP).
- Prepare lessons learned from the event, and review and update the cyber incident response plan and the cyber security controls so that they are appropriate to and consistent with the risks encountered, and follow up on the remediation of the deficiencies identified through to completion.

6.2.3 Business Continuity Management Working Team (BCMWT)

1) Under normal conditions

- Establish, oversee, and review the business continuity management (BCM) process so that it remains current and responsive to changing circumstances, convening sub-group meetings as appropriate in order to submit results and recommendations to the Business Continuity Management Steering Committee (BCMSC) for its approval.
- Support the establishment, implementation, review, and improvement of the Company's Business Continuity Management System (BCMS).
- Oversee the testing and exercising of departmental Business Continuity Plans (BCP), report the exercise results and any problems or obstacles to the Business Continuity Management Steering Committee (BCMSC), and follow up on the remediation of the deficiencies identified.
- Communicate the Company's Business Continuity Plan (BCP) to employees and personnel within their respective lines of command so that they are informed of it, appreciate its importance, and apply it consistently.
- Publicize and promote knowledge, understanding, and awareness of business continuity management (BCM) among all employees and personnel of the Company.
- Coordinate with the relevant units in preparing and reviewing the Business Impact Analysis (BIA), the risk assessment, and each department's business continuity plan so that they remain current.

2) During a crisis

- Convey and communicate the direction activating the Business Continuity Plan (BCP), together with the guidance issued by the Business Continuity Management Steering Committee (BCMSC), to employees and personnel within their respective lines of command so that they are informed and can act correctly and in a timely manner.
- Assign work in accordance with roles, duties, and responsibilities to personnel within their line of command, and monitor compliance with the relevant plans and directions.
- Provide work equipment and information technology equipment to support those concerned when working from their place of residence.
- Monitor the progress of coordination and report performance in accordance with the working arrangements and work locations prescribed by the Company during a crisis.

- Coordinate with the relevant units so that critical operating processes can continue or be recovered within the defined timeframes and to the defined levels.

3) In the post-crisis phase

- Prepare the Company's restoration plan together with the relevant departments and submit it to the Business Continuity Management Steering Committee (BCMSC) for approval.
- Carry out the restoration plan approved by the Business Continuity Management Steering Committee (BCMSC) and report progress at the defined intervals.
- Monitor the progress of coordination and report on the return to work at the primary work premises or the return to normal operations, and compile any problems and obstacles for submission to the Business Continuity Management Steering Committee (BCMSC) for its information.
- Compile performance results, deficiencies, and lessons learned from the event in order to propose corrective actions and improvements to the Risk Assessment (RA), the Business Continuity Plan (BCP), and the related measures, as appropriate.

6.2.4 IT Operations Team

1) Under normal conditions

- Participate in testing the Company's Business Continuity Plan (BCP).
- Prepare, review, and update the information technology recovery plan, and ensure that the Business Continuity Plan (BCP) and the Disaster Recovery Plan (DRP) remain consistent with one another at all times.
- Regularly verify the readiness of the hardware, software, and equipment used to operate the various systems, so as to support working from the alternate work site, from a place of residence, or from any other location designated by the Company.
- Maintain and test the information technology business continuity plan and disaster recovery plan (BCP-ITS-001) at least once (1) a year, verify that the test results meet the Recovery Time Objectives (RTO) established in the Business Impact Analysis (BIA), and coordinate with the responsible persons in each department to confirm system priorities and recovery requirements.
- Verify and test data backups, data recovery capability, and the readiness of backup systems, infrastructure, service providers, and other necessary resources at the intervals prescribed by the Company.

2) <u>During a crisis</u>

- Prepare the hardware, software, and equipment needed to operate the various systems in order to support working from the alternate work site, from a place of residence, or from any other location designated by the Company.
- Determine system priorities in order to enable, disable, suspend, or restrict the use of each system as necessary, giving precedence to the systems supporting critical business processes and acting in accordance with the priorities set by the established Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).
- Ensure that sufficient information technology personnel are available for system recovery and for operations during the crisis or incident.
- Establish the communication channels needed for coordination and system recovery. Communication with external stakeholders shall be carried out jointly with the Corporate Communications department, the Corporate Legal department, and the other relevant departments in accordance with their respective authority.
- Establish communication channels for cases in which some employees or personnel must work away from the primary work premises, including work at the alternate work site, at a place of residence, or at any other location designated by the Company.
- Prepare and maintain a record of events, decisions, system changes, and related actions (Incident Log), and report progress to the Crisis Management Team (CMT) and to the Business Continuity Management Steering Committee (BCMSC) in accordance with the reporting hierarchy and the urgency of the situation.
- For P1-P2 level events, the Head of IT Operations Team has the authority to activate the Disaster Recovery Plan (DRP) and to establish an incident coordination center (War Room) immediately, in accordance with the criteria and the scope of authority prescribed by the Company, and must report to the responsible executive and to the Crisis Management Team (CMT) immediately, providing the estimated time to recovery and the status of the systems within one (1) hour of activating the Disaster Recovery Plan (DRP). Where the event involves, or may involve, a personal data breach, the Data Protection Officer (DPO), the Corporate Legal department, and the other relevant departments must be notified immediately so that the matter can be assessed and handled in accordance with applicable laws and regulations.

- Contain, isolate, recover, and verify systems in accordance with the established procedures, having regard to the preservation of digital evidence, the security of the systems, and the prevention of any further escalation of the event.

3) *In the post-crisis phase*

- Assess damage to information technology equipment and systems once the event giving rise to the crisis or incident has subsided or normal conditions have been restored.
- Support the restoration of information technology systems, and verify the accuracy, completeness, integrity, and security of the systems and data following recovery, before the systems are returned to use.
- Prepare a Post-Incident Report within a period appropriate to the severity level of the event, and in any case within four (4) weeks of the event being controlled or resolved, unless there is a necessary reason approved by the responsible executive, and submit it to the Business Continuity Management Steering Committee (BCMSC).
- Follow up and remediate the deficiencies identified from the event and from the system recovery, and update the Disaster Recovery Plan (DRP), the operating procedures, system configurations, controls, and related contact information so that they remain current.

7. Incident Severity Levels

Level	Description	Examples	Response
P1 - Critical	An event or incident that disrupts critical business processes or systems entirely or on a broad scale, such that operations cannot continue at the minimum level acceptable to the Company, or that causes or is likely to cause severe impact on personnel, assets, data, reputation, legal compliance, or the Company's stakeholders.	Earthquake, fire, flood, epidemic, civil unrest, or other events with severe impact on operations, including ransomware / cyberattack that encrypts or renders core systems, such as SAP Production or file servers, unusable on a broad scale, or a high-risk data breach.	Respond and report immediately, and assess the need to activate the Disaster Recovery Plan (DRP) and/or the Business Continuity Plan (BCP) according to the nature and impact of the event.

Level	Description	Examples	Response
P2 - High	A critical process is disrupted, but the core business can still operate at a limited level or on a temporary basis, with a risk that the impact will spread or exceed the period acceptable to the Company.	Protests affecting access to the work premises; broad-scale failure of M365 / email or of a file server where temporary alternative channels or working methods remain available.	Acknowledge, assess, and begin action within two (2) hours of becoming aware of the event, and escalate to P1 if the impact spreads, cannot be controlled, or is likely to exceed the thresholds set for P1.
P3 - Medium	Affects a limited number of users, or a non-critical support system, without significant impact on critical business processes, and appropriate alternative working methods are available.	Failure of the SAP development and test systems (SAP QAS / SAP DEV); systems running slowly but still usable.	Acknowledge, assess, and begin action within four (4) business hours of becoming aware of the event.
P4 - Low	Affects one to two (1-2) users, or a minor problem with an immediate workaround, without impact on the continuity of critical business processes.	Printer failure; software installation request; user password reset request.	Acknowledge and begin action within eight (8) business hours of becoming aware of the event.

The severity level of an event shall be determined by reference to its nature, scope, and duration, and to the impact that has occurred or is expected to occur on personnel, business processes, information technology systems, data, assets, reputation, legal compliance, and the Company's stakeholders. The event types and examples set out in the table are provided as guidance only.

The Company may raise or lower the severity level of an event in light of new information and changing circumstances, and any such change must be reported immediately to the authorized persons and the relevant working teams.

8. Review of the Policy, of Roles, Duties, and Responsibilities, and of the Business Continuity Management Framework (Continual Improvement of Business Continuity Management)

The Business Continuity Management Steering Committee (BCMSC) shall review the policy, the roles, duties, and responsibilities, and the business continuity management framework, together with the Business Continuity Plan (BCP) and related plans, once (1) a year and whenever a significant change or event occurs. The review shall take into account inputs

such as plan test results, past disruptive events, the Risk Assessment (RA), and the Business Impact Analysis (BIA), as well as changes in the business, in technology, and in legal or other applicable requirements.

The results of the review must be used to improve the policy, the plans, and the related processes, with a clearly defined action plan, responsible persons, and implementation timeframes, together with follow-up and reporting to senior management at appropriate intervals. Records and related evidence must be documented and retained as input for the next review cycle, so that review and improvement continue on an ongoing and effective basis.

Note:

- Management and employees at all levels shall participate in supporting and driving the Company's awareness of, and commitment to, operating in accordance with the Business Continuity Management System (BCMS).
- All employees and personnel have a duty to study, understand, and comply with this Business Continuity Management Policy (BCMP), including the roles, duties, and responsibilities applicable to them.

9. Reference Documents

No.	Document Code	Reference
1.		Company organizational structure chart, dated 1 October 2025
2.	RM003	Business Continuity Plan
3.	BCP-ITS-001	Business Continuity Management and IT Disaster Recovery Plan
4.	SOP-ITS-001	Business Continuity Management and IT Disaster Recovery Procedure
5.		Incident Response Plan
6.		Business Impact Analysis Report
7.		Risk Assessment Report

10. Revision History

Revision History			
Version	**Date**	**Prepared / Revised by**	**Content / Reason for Revision**
1	11 August 2026	Risk Management Department	Initial issue