POLICY

Policy on Business Continuity

RAM

Last reviewed date:
14 December 2021

Initial Approved date:
4 October 2011

Title	Policy on Business Continuity	Revision no.	3
Initial approved date	4 October 2011	Last reviewed date	14 December 2021 [Joint Board meeting (6/2021)]

Subject	Date	Remarks
1st approved	4 October 2011	
New Policy on Business Continuity	20 April 2020	• Put in place new provisions to reflect the requirements of SC's Guidelines on Management of Cyber Risks and Guiding Principles on Business Continuity. • Include detailed Disaster Recovery Plan and Pandemic Response Plan. • New Provision on Communications and Call Tree. • New Provisions on Monitoring Audit and Training.
Amendment	14 December 2021	• Amendment to the Call Tree, Appendix D following organizational restructuring of RAM Group 1 July 2021.

RAM

Title	Policy on Business Continuity	Revision no.	3
Initial approved date	4 October 2011	Last reviewed date	14 December 2021 [Joint Board meeting (6/2021)]

Content

RAM

Title	Policy on Business Continuity	Revision no.	3
Initial approved date	4 October 2011	Last reviewed date	14 December 2021 [Joint Board meeting (6/2021)]

OVERVIEW

1. Introduction

1.1 Policy on Business Continuity (BC) describes the processes and procedures that the RAM Group has put in place to ensure that essential functions can continue during a transition of management, a disaster or a widespread disease that causes serious illness. The Policy seeks to prevent the interruption of critical services and re-establish full functions as swiftly and smoothly as possible. The board of directors and senior management are accountable for the RAM Group's business continuity preparedness.

2. Objectives

2.1 This Policy has been formulated to meet the needs of the RAM Group as well as to comply with Securities Commission Malaysia (SC)'s Guiding Principles on Business Continuity (issued on 14 May 2019), including the relevant amendments. The primary objectives of this Policy are as follows:

|	
PROTECT	Protect our people, system and infrastructure
IDENTIFY AND MITIGATE	Identity and mitigate the risks to RAM's services to an acceptable level
MANAGE	Manage any disruption to minimize its impact
ENSURE	Ensure clients and customers receive our services, as intended

2.2 This Policy comprise the following areas:

(a) **Business Continuity Management (BCM)** that includes guidelines for establishing policy, standards and procedures for RAM Group to ensure that in the event of **service disruptions**, the critical business functions may continue and resume within an appropriate timeframe. In this, there is a need to:
- Identify critical activities
- Carry our business impact analysis
- Setting recovery objectives

(b) **Business Continuity Plan (BCP) shall include the following**:
   (i) **Succession Planning** will identify and develop internal people with the potential to fill key leadership positions within the RAM Group in the event of resignation or departure of senior management.

   (ii) **Disaster Recovery Plan** will specify the organisation's planned strategies for post-failure procedures on disaster recovery in the event of minor and extended service outages caused by factors beyond the

organization's control (e.g. natural disaster, man-made events), and to restore services to the furthest extend possible within a targeted minimum period. The aim to ensure the survival of the organization, facilitate the resumption of operations and protect the stakeholders.

(iii) **Pandemic Response Action Plan** will manage a pandemic to reduce the risks to employer's health and safety as well as to ensure sustained business operations.

(iv) **Communication Plan** includes ways of communication, internal and external, to relevant parties on a timely basis. The communication plan shall specify responsible persons, communication procedures and channels, disclosure levels, names and phone numbers of staff and relevant external parties which may be prepared in a form of a Call Tree.

(v) **Training Plan** will include regular trainings on Business Continuity for staff and relevant parties to ensure that staff and relevant parties understand their roles and responsibilities when such operational disruptions occur.

(c) **Follow-up testing and evaluation** which will include testing and reviewing of BCP.

Overview of Policy
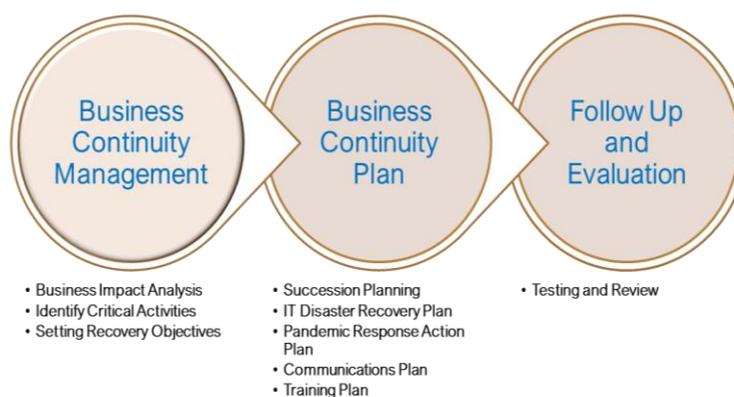
3. Scope of Policy

3.1 This Policy is applicable to RAM Holdings Berhad and its wholly owned subsidiaries (RAM Group) as well as their directors and employees (including full-time, probationary, contract and temporary staff) of the RAM Group.

4. Definition

4.1 "Alternate Site" means a substitute place or location for operation and business in case the main operational site is not available for operation as normal.

4.2 "Business Impact Analysis (BIA)" means a process of analysis and assessment of impact or business loss, both qualitative and quantitative, caused by operational disruptions.

4.3 "Critical Business Function" means a function once disrupted may cause significantly impact to the operation, business, reputation, status and performance of the company.

4.4 "Disaster" means defined as any event that significantly disrupts the normal operations of the RAM Group.

4.5 "Line Manager" includes heads of departments.

4.6 "Recovery Objective" means the setting up of a goal for operational recovery which consists of recovery time objectives and recovery strategies.

4.7 "Recovery Strategy" means a guideline to cope with the major operational disruptions.

4.8 "Recovery Time Objective" means an acceptable period for operational disruption.

4.9 "Senior Management" is defined as members of the senior management team of Grade E3 and above.

4.10 "Service disruptions" means any disruptive challenge that threatens personnel, buildings or RAM Group's operations which requires special measures to be taken to restore normal operations. Examples of service disruptions include the following:

- Major incident, national disaster, road closure, epidemic, pandemic, terrorist attack.

- Utility or service outages i.e. loss of water, including IT failure, hardware or software viruses, network outages, telephone systems, supply discontinuation.

- Fire, flood, extreme weather conditions.

- Major disruption of staffing i.e. as a result of industrial action, inability to recruit or mass resignation.

5. Policy Administration

5.1 The Board and Senior Management shall be responsible for drafting and implementing strategies and policy concerning Business Plan and shall allocate adequate resources to support the operations. The Board may delegate operational authority to the Senior Management. The Senior Management, led by the Administrator shall be responsible for setting out a clear structure, line of command and responsibilities of related parties in accordance with this Policy.

5.2 The Group Chief Executive Officer (CEO) shall be the overall administrator (Administrator) of this Policy. In the absence of the Group CEO, the Deputy Group CEO shall be the alternate in the administration of this Policy.

5.3 In the event of the declaration of a disaster or pandemic, the Group CEO shall take charge and work together with the management to ensure minimal disruption to the RAM Group's operations.

5.4 For the purpose of the Disaster Recovery Plan, the Chief Digital Officer and/or Head of the Information Technology Department are responsible for all data backups and record keeping of information in the RAM Group's servers.

5.5 In the event that the employee named as responsible person to perform any specific task is absent, the employee serving in and "Acting" capacity shall undertake the said task.

BUSINESS CONTINUITY MANAGEMENT

6. Business Continuity Management

6.1 In developing suitable Business Plan, RAM Group shall set up a Business Continuity Management Framework. In this, the Senior Management led by the Administrator shall:

(a) Conduct **Business Impact Analysis (BIA)** that analyses the activities of RAM Group and effects of service disruptions that would include the following:

   (i) Evaluation of all operations and functions and the impact of losing the operation or key function;

   (ii) Identify critical business functions and the duration that RAM Group an manage without the function;

   (iii) The types of service disruptions that threaten the delivery of the function (loss of staff, building, IT, utilities and third-party suppliers);

   (iv) The actions already in place to mitigate against any disruption; and additional actions that may be needed to further mitigate or reduce the consequence of a disruption; and

RAM

(v) The resources (employees, office space and IT) required to reinstate the critical business functions.

(b) Establish recovery objectives, recovery strategy as well as recovery time objectives and ensure adequate arrangement are in place; and

(c) Ensure that the Critical Business Functions identified in the BIA are reviewed periodically to ensure arrangements are in place to mitigate against the consequences of a disruption and to decide if a specific BCP is required. In this, the respective heads of department as owners or critical activities and events identified in the BIA will be expected to take the lead in the event of a disruption.

Please refer to **Appendix A** for sample of Business Impact Assessment.

SUCCESSION PLANNING

7.   Business Continuity Management

7.1   The Board of Directors and the Senior Management shall oversee the development and management of Human Resource Policies within the RAM Group. The key objectives are to ensure that the RAM Group's compensation, Human Resource programmes and practices can attract, manage and retain talented employees to develop RAM as a performance-driven organization as follows:

(a) Succession planning and development ensure that employees are identified, developed and ready to fill key leadership positions within the RAM Group, as and when the position become vacant.

(b) All employees are to be appraised based on their performance. Talented employees shall be mentored and given adequate training and opportunities to develop versatile career paths within the RAM Group, to enable them to be ready for leadership positions.

(c) All senior appointments shall comply with the *SC's Guidelines on Registration of Credit Rating Agencies.*

DISASTER RECOVERY PLAN

8.   Risks of a Disaster

8.1   A disaster incapacitates a business, interrupts normal operations and impacts its bottom line. A Disaster Recovery Plan is gear towards mitigating the possible negative impact on the RAM Group's business operations.

RAM

8.2 Each department and/or business unit is to develop its own Business Recovery Plan to ensure prompt resumption of and a return to normal operations within the targeted recovery schedule of the BCP.

9. Steps of Disaster Recovery Plan

9.1 This Plan delineates the RAM Group's policies and procedures on technology disaster recovery, as well as our process-level plans in managing critical technology platforms and IT infrastructure.

9.2 This plan shall be activated in the event of a disaster. In this, the Administrator shall set up a **Disaster Recovery Management Team (DRMT)** comprising the Chief Digital Officer and/or the Head of Information Technology department as its tea leader, and other members of the Senior Management. The Disaster Recovery Management team's responsibilities include the following:

(a) Assess the disaster and initiate this Disaster Recovery Plan.

(b) Coordinate the DRMT in activating the plan and notify key management contacts; redirect server operations to the Disaster Recovery Site (Alternate Site).

(c) Liaise with the Head of Administration on the extent of damage for insurance reporting and procurement of new equipment, if necessary.

(d) Activate the VPN, VOIP or laptop/remote desktop availability or set up suitable IT infrastructure.

(e) Ensure that all networks, servers, routers and switches are reconfigured while software and data are reinstalled, and workstations are set up for resumption of normal operations.

(f) Provide periodic updates to the Administrator and Head, Group Communications

(g) on the progress of recovery phases, as set out in para 10.1 below.

10. Disaster Recovery Phases

10.1 The disaster recovery process consists of four (4) phases.

(a) **Phase 1: Disaster Assessment**
The disaster assessment phase lasts from the inception of the disaster until it is under control and the extent of the damage can be assessed.

(b) **Phase 2: Disaster Recovery Activation**
When the decision is made to move the primary processing server (RAM's server is located within its office premises) to another location, this phase begins. The Disaster Recovery Management Team shall call upon team members to perform their assigned tasks. The most important function is to

fully restore operations at a suitable location and resume normal functions. Once normal operations are established at the alternative location, Phase 2 is complete.

(c) **Phase 3: Alternate Site/Data Centre Rebuild Phase**
This phase involves continuing operations at the alternative location. In addition, the primary site shall be restored.

(d) **Phase 4: Return to Office**
This phase involves the reactivation of the primary data center at either the original or possibly new location.

At the end of this phase, the disaster recovery process shall be thoroughly reviewed. Any deficiency in this plan can be corrected by updating it.

Please refer to **Appendix B** for the Disaster Recovery Plan.

10.2 For the purpose of this Policy, the Recovery Time Objective (RTO) shall be no longer than 72 hours to resume basic operations following a disaster. The Recovery Point Objective (RPO) is to not lose more than 24 hours of back-up data in the event of a disaster.

10.3 The Chief Digital Officer and/or the Head of the Information Technology Department shall perform the following;

(a) Establish a Disaster Recovery Site (Alternative Site) at a location not less than 25 kilometers from the primary server.

(b) Ensure that all servers and IT systems at the Alternative Site can be activated at all times.

(c) Maintain the Backup Strategy stated in RAM's IT Policy.

PANDEMIC RESPONSE ACTION PLAN

11. Risks of a Pandemic

11.1 All businesses are exposed to the risk of a pandemic. In addition to the threat to human health, the economic impact of a pandemic, including absenteeism in the workplace or the imposition of travel restrictions that will affect business operations.

12. Pandemic Response Action Plan (PRAP)

12.1 This PRAP outlines the RAM Group's measures to safeguard employees' health and well-being during a pandemic while ensuring the organization's ability to maintain essential operations and continue providing essential services to our

customers. In addition, it provides guidance on how we intend to respond to specific operational and human resources issues in the event of a pandemic.

12.2 In event of a pandemic, the Administrator shall have the authority to:

(a) Establish a Pandemic Response Action Plan as set out in **Appendix C**.

(b) Set up a Pandemic Response Team comprising Senior Management personnel.

(c) Establish mechanisms to allow employees to work from home and restrict non-essential travel.

(d) Establish contingency plans to maintain delivery services during times of significant and prolonged absenteeism.

(e) Maintain communication lines to keep all stakeholders and employees informed and updated on the pandemic.

(f) On IT-related issues:

(i) Put in place VPN, including the ability to offer voice over IP and laptop/remote desktop availability.

(ii) Allow increased use of virtual meeting tools – video conferencing and desktop sharing.

COMMUNICATIONS

13. Communications and Contact Points

13.1 It is imperative that all key employees remain contactable during a disaster and/or pandemic. The Administrator of this Policy shall ensure the following:

(a) The database of contact numbers and addresses of all employees is maintained and updated. The Human Resource Manager or such personnel as may be determined by the Administrator shall keep the database updated and establish a Call Tree – Please refer to **Appendix D**.

(b) Ensure these contact numbers and addresses are made available to the Senior Management and the Line Manager.

13.2 Contact Points & Notification

In the event of a disaster or when the PRAP is triggered, the Head of Group Communications is designated as the principal contact with the media, government agencies and stakeholders including shareholders and clients. The Chief Compliance Officer shall be the designated principal contact with the SC.

RAM

13.3 Upon the occurrence of a disaster:

(a) The Group CEO shall notify the Board, issue a declaration of disaster and activate the Disaster Recovery Plan set out in Para 9.

(b) The Chief Compliance Officer shall as soon as reasonably possible, inform the SC in accordance with the incident report template pursuant to the *SC's Guiding Principles on Business Continuity or SC's Guidelines on the Management of Cyber Risk*.

(c) The Group Communications shall inform all stakeholders (including shareholders and clients) and members of the public as well as provide regular updates to the stakeholders for as long as the declaration of disaster of the PRAP is in effect, until business operations have resumed.

13.4 Upon the triggering of the PRAP:

(a) The Administrator shall notify the Board when the pandemic has reached Code Orange - Tier 2 status.

(b) When it has reached Code Red:

(i) The Chief Compliance Officer shall inform the SC in accordance with the incident reporting template pursuant to the *SC's Guiding Principles on Business Continuity.*

(ii) The Group Communications Officer shall inform all stakeholders (including shareholders and clients) and members of the public as well as provide regular updates to the stakeholders for as long as the Code Red is in effect, unit the pandemic has passed.

13.5 Upon resumption of normal operations, the Administrator shall, with the consent of the Board, formally revoke the declaration of disaster. The PRAP shall be terminated when the pandemic is no longer deemed so.

MONITORING, AUDIT AND TRAINING

14. Monitoring, Audit and Training

14.1 The Audit and Risk Management Committee (ARMC) shall be responsible for monitoring the effectiveness of this Policy and to submit an annual report to the Board on its compliance.

14.2 There shall be a minimum of one (1) annual test conducted and regular updates of business continuity documents and process by internal or relevant external parties.

RAM

14.3 Training session on the key aspects of business continuity shall be held at least once a year.
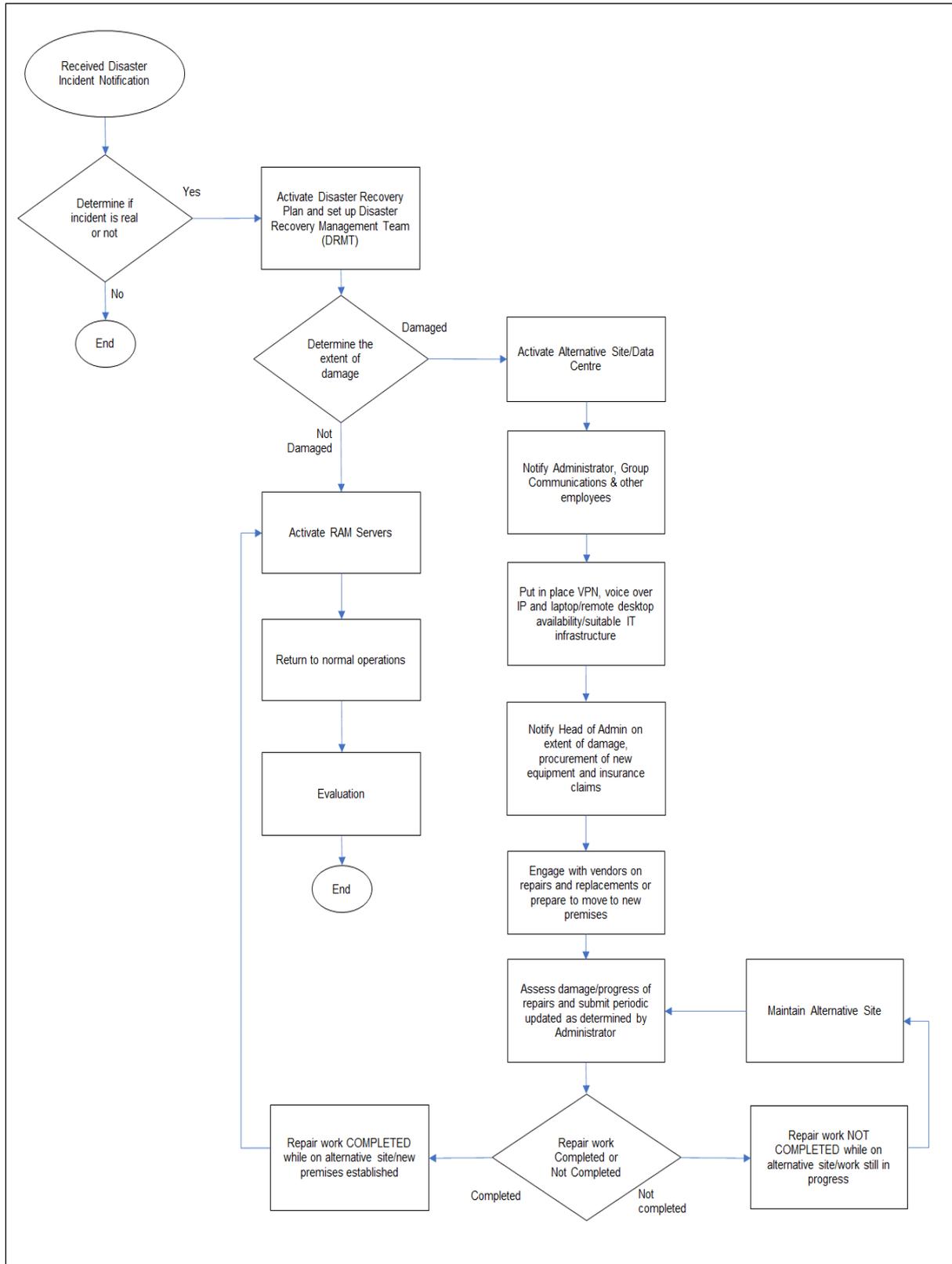

REVIEW

15. Review

15.1 This Policy shall be reviewed annually by the Board. Earlier review may be required in response to exceptional circumstances, organizational changes or relevant changes in legislations or guidelines.

RAM

Business Impact Assessment

No	Services	Critical Business Function	Specific impact of disruption	Recovery Time
1	Ratings Operations	Rating Committee Meeting	Independent RC members are down will illness and no quorum	
		Servicing client		
		Timely reporting		
2	Sustainability Services	Servicing client		
		Timely reporting		
3	IT Services	Data Feed		
		Virtual Private Network (VPN)		
		Servers		
		Grandstream (IP calls)		
4	Accounts & Financial Services	Procurement		
		Treasury		
		Collections and Payments		
5	Human Resources & Payroll	Payroll		
		Recruitment		
		Resignation		
6	Administration	Maintenance of Boulevard Office		
7	Marketing and Business Development			
8	Publication			
9	Communications			
10	Legal & Corporate Affairs	Advisory		
		Monitoring		
		Documentation		
11	Training Services			
12	Compliance	Reporting to Securities Commission		

RAM

Disaster Recovery Plan

RAM's Pandemic Response Action Plan

Codes	Descriptions	Cumulative Actions	Employees & HR Matters
Green	Diseases is mild with no widespread transmission/easily treatable	• Minimal disruption, cautious approach but business as usual. • Take daily preventive measures to help stop the spread of germs, consuming antiviral medication if prescribed.	• Sick employees must stay home (with MC). • Upon returning to work, employees must wear masks.
Yellow	Disease is severe and spreads easily	**STOP THE SPREAD** • Good personal hygiene and regular cleaning. • Make available hand sanitisers and face marks while minimizing personal contact. • Stock up on critical supplies (face masks, sanitisers, disinfectants). • Subject to HOD's clearance, impose travel restrictions. • Staff to alert HR when they travel (for official and personal reasons). • Look out for health advisories.	• Employees who are ill must stay home. • If anyone at home shows symptoms, all must be screened; employee must stay away from the office until they are cleared. • Employees who are exposed to higher-risk areas or endemic countries must be **quarantined for at least 14 days**. • Work from home + VPN access + voice and video calls.
Orange -Tier 1	Disease is severe and spreads easily/human to-human transmission	**STOP OR LIMIT SPREAD FROM LOCAL CLUSTER** • Impose temperature screening. • Front-line employees need to wear masks. • Impose travel restrictions. • Minimize meetings in the office (Mercu 2 of The Boulevard) and also outside. • Monitor employees' movements.	• Employees who are ill must stay home. • If anyone at home shows symptoms, all must be screened. • Encouraged to bring notebooks home. • Employees who are exposed to higher-risk areas or endemic countries must be **quarantined for at least 14 days**. • Work from home + VPN access + voice and video calls.
Orange -Tier 2	Disease is severe and widespread with imminent declaration of Code Red	• Inform the Board and activate Call Tree.	• Employees to bring notebooks home and be ready to work from home. • All departments to prepare for full implementation of Code Red.
Red	Disease is severe, spreading widely and has spread to the Office	**REDUCE IMPACT THROUGH SOCIAL DISTANCING** • Inform the Board and stakeholders. • Activate Call Tree. • Restrict travel. • Close offices in Mercu 2 and The Boulevard for cleaning and disinfection. • Cancel all public engagements and meetings/events.	• Close offices in Mercu 2 and The Boulevard for cleaning and disinfection. • If necessary, access will be granted to enter the premises. • Work from home + VPN + voice and video calls. • Open VPN to all staff. • Monitor employees.

RAM

Guidelines on RAM Call Tree

(a)   The Call Tree coordinates data gathering with Human Resources, as contact data typically comes from that department. The Call Tree shall be managed by Administrator, together with Group Human Resource.

(b)   Each listed employee may have several contacts, including office, home and mobile numbers, and an email address. The list of contacts, and sequence of notification, is then approved by Group Human Resource. The Call Tree may utilize email, OneDrive or any free-to-use mobile application such as Whatsapp or Microsoft TEAMs.

(c)   The emergency Call Tree should be available in several locations, such as the Company Intranet, emailed to HODs as well as in hard-copy format. For this purpose, Group Human Resource should keep the information up to date. For this, RAM Group shall use a manual Call Tree in which each person who receives a call is responsible for calling others in the Tree.