Disaster Recovery Management Plan

I. Guidelines of the Disaster recovery system

1. Objective

The SMM Disaster Recovery Management Plan is designed to improve SMM's ability to respond to emergencies with a scientific, effective and responsive work mechanism. It ensures that the SMM price assessment team continues to operate normally under any circumstances, and minimises or avoids the impact of various emergencies.

2. Scope of application

This Management Plan is applicable to all SMM offices locally and regionally.

3. Requirements - working principles

Prevention-oriented: Protects the security of SMM, strengthens the early warning systems and indicators, focuses on protecting SMM's basic information network and important information systems. Take measures to consider the law, management, technology, and personnel from the perspective of precaution, monitoring, emergency treatment and insurance of all parties with a view to to maintaining secure systems and infrastructure.

Quick response: To response quickly in accordance with the Management Plan in the event of an emergency, to obtain sufficient, accurate and timely information through appropriate means, and to be decisive, handling situations in a quick and responsive manner so as to minimise any harm and negative impact.

Division of manpower: Establish and improve the department's systems for safety, accountability and joint action mechanisms in a top-down, small-to-large fashion, identify accountability and shared responsibility of each department, strengthen their coordination and collaboration to ensure joint actions for the effective management of emergency procedures.

Stay alert: Strengthen technical reserves, standardise emergency response measures and procedures, conduct pre-plan drills on a regular basis to ensure the effectiveness of emergency plans, and follow a set of scientific, formalised and standardised procedures to deal with network and information security emergencies.

II. Disaster impact assessment

The impact of an emergency is assessed on a scale of one to four – Extreme (Level 4), High (Level 3), Medium (Level 2), and Low (Level 1).

Extreme (Level 4): Disastrous impact

Including heavy storms, bomb explosions, shootings, catastrophic fires and terrorist activities.

High (Level3): Moderate-heavy impact

Including a large-scale fire in the workplace, continuous crashing of IT systems, workplace violence, epidemic diseases, failure to execute key processes in multiple departments, unexpected power failure for a prolonged period.

Medium (Level 2): Limited impact, normal business operation

Including an interruption in IT system, failure of conducting key processes in a department, fault, power failure for a short period, adverse weather conditions (no damage involved), and illnesses that affect a small proportion of the workforce.

Low (Level 1): Small impact, normal business operation

Including individual medical emergencies, small leakage in the workplace, short-time interruptions in IT applications

III. Emergency procedures activation, response, and contact guidance

Impact level	Severity	Whether to activate emergency procedures	Contact

Level 1	Small impact, normal business operation	No, manage as usual	Notify the person in charge.
Level 2	Limited impact, normal business operation	No, manage as usual	Notify the person in charge; Notify the Business Continuity Management (BCM) group; Incident Management Team (IMT) on standby.
Level 3	Moderate-heavy	Yes	Notify IMT to start emergency meeting Communicate with stakeholders; Communicate with stakeholder groups; Notify all staff; Communicate with major suppliers.
Level 4	Disastrous	Yes	Notify IMT to start emergency meeting Communicate with BCM Communicate with stakeholders; Communicate with stakeholder groups; Notify all staff; Communicate with major suppliers; .

IV. Disaster Recovery Procedures Activation

1. Activation process

Any member of the Incident Management Teams (IMT) can activate the IMT procedures based on their assessment of the impact of the current emergency.

As a guide, BCM and/or facilities teams will monitor building, site or weather related events and in most cases, these teams will escalate to the IMT.

To escalate to the IMT, the following methods are recommended:

1) The initiator uses the IMT distribution list to arrange an IMT meeting within 30 minutes and briefly describes the incident and its urgency.

2) Send over the timeline overview to members in the IMT contact list via email, voice or video, in the case whereby a meeting cannot be organised.

2. IMT meeting

The location of the meeting will depend on the time and nature of the incident. The principle is to gather all IMT contacts in a short time, regardless of when and where the meeting is held.

When the incident occurs during office hours, IMT members should activate IMT in meeting rooms in the workplace, and key personnel will be invited to a voice or video conference call if they are out of office.

When the incident occurs during non office hours, the initiator should initiate a group video conference in the IMT chat group on WeChat Work app.

If multiple workplaces are involved in the IMT escalation at the same time, a group video conference should be initiated in the IMT WeChat Work group as soon as possible.

For the above situations where IMT cannot be activated in the workplace office, please complete the following requirements and steps:

要求： Requirements:

1） All IMT members must always keep their mobile phones switched on
2） The Department of Human Resources and Administration must archive the emergency contact information of IMT members
   1)
3） The chairman of IMT has established an exclusive WeChat Work group for the "Emergency Incident Management System"

Step:

   1) The emergency call initiator clicks the "Meeting" button in the "Emergency Event Management System" WeChat Work group to initiate a group meeting invitation
   2) Any member of the meeting can call members who have not joined the meeting within 5 minutes, to notify him or her of the meeting through the shared "Key Contacts List"
   3) If the him or her cannot be reached, even through the emergency contact person, a co-worker at the same level or above in the same department can be invited to join the meeting instead
   4) If the person cannot be contactable, even through the emergency contact person, and if the uncontactable person is the department leader and there is no other personnel of the same level, the direct subordinate should attend the meeting on his behalf.

3. Evaluation of level of impact

An IMT event is triggered if all IMT members concur with the rating results of the incident evaluation.

In the case of inconsistent rating results, an IMT event is triggered if more than half of the IMT members agree to do so.

In the case of inconsistent rating results, an IMT event is not triggered if less than half of the IMT members agree to trigger an event. IMT members will remain on standby and observe any developments in the incident's impact. Another IMT meeting should be arranged to re-evaluate the impact if necessary.

V. Incident response

1. IT response

Preparation and prevention

To minimise system errors as much as possible, machines and application status should be inspected from the cloud environment on a daily basis. Status of the computer server room's infrastructure, servers, network equipment and monitoring system should be inspected twice a day, to ensure a favourable operating environment.

Detection and incident classification

In the event of a crisis or disaster, the ability to quickly recognise and classify the event is the crucial first step in the process, which is necessary for the timely response and communication strategy.

Response and relief

In order to quickly identify the level of the incident and accurately mobilise different resources to respond and solve the problem, the incidents are classified into four levels based on the severity and scope of the impact. On the basis of the feature of incidents of different levels, maintenance and operations personnel, as well as research & development staff, will be provided with different types of resource support.

a)   P0 incident: Failure of core business functions, affecting all user groups

This is the incident of the highest level and requires immediate responses. In a P0 incident, customers have no effective way to check quotations. The company will address the incident with all its resources, adopting methods including but not limited to temporarily increasing the server hardware resources, creating temporary access to websites, requiring analysts, salesperson and operations staff to publish prices in online chat groups, concentrating manpower and halting all R&D, operation and maintenance work. And after the incident is solved, it should be reported to the company within one working day. In case of a man-made incident, the main person in charge will be held accountable.

b)   P1 incident: malfunction of core businesses that affects internal users

When the P1 incident occurs, analysts are unable to provide the latest price offers to customers. Analysts should send urgent data through QQ or Wechat. Meanwhile, IT staff should work to fix the issue and report to the IT department within half a working day.

c)   P2 incident: The peripheral functions of core businesses are unavailable, which seriously affects customers experience.

Response time is less than 15 minutes. Quickly analyse the root causes that affect the customer experience, and make emergency repairs as soon as possible to ensure that there is no unpleasant experience in the process of data utliisation.

d)   P3 incident: Peripheral functions are unavailable, which slightly affects customer experience.

The response time is less than 4 hours, and the main person in charge will perform the functional repair as soon as possible.

e)   P4 incident: The peripheral functions are not available, but this basically does not affect the customer experience.

The response time is less than 6 hours, and the person in charge of R & D is responsible for the functional repair.

During the occurrence of the incident, a discussion group will be established soonest. The committee includes the IT department, analysts, and key management personnel of the company. The committee will analyse the causes of incidents and countermeasures in a timely manner. For P0 and P1 level incidents, the repair plan and backup plan are launched at the same time, and the implementation status of each plan is reported.

Recovery and analysis

Once the incident is resolved, an incident analysis report should be issued to the relevant department personnel in a timely manner to include:

 • A report on experience and lessons learned: Participants reflections on how the incident happened and what was learned.

 • Action process descriptions: Including specific recommendations and a set of actions for improving the team's response to a specific incident.

This analysis report is designed to prevent the same crisis or emergency from happening again.

Escalation procedures:

As situations evolve from normal to urgent to potential crisis or even disaster level, action is taken to upgrade the equipment and strengthen the systems. This is to done to ensure the right knowledge and resources are utilised at the right time. At the same time, system vulnerabilities tracking and security updates will also be performed. Escalation management can be an urgent task and having a formal process in place will help to manage escalations as easily and effectively as possible.

2. Personnel administration

Workplace patrols are undertaken twice a day to ensure that basic office facilities are in good conditions.

Administrative warehouse stocktaking is done once a week to ensure adequate stockpiles of daily office supplies.

Each month, Mutual supervision is undertaken between IMT members,checking the operations of each business divisions, which will be reported at a meeting.

Impact level	Severity	Staff arrangement	Action
Level 1	Small impact, normal business operation	Continued daily work at the workplace	HR notifies the head of the department that resolved the incident point-to point,and supervises the handling
Level 2	Limited impact, normal business operation	Continued daily work at the workplace	HR notifies the head of the department that resolved the incident point-to-point and supervises the handling of the incident; and informs IT to prepare some personnel to work from home
Level 3	Moderate-heavy	Part or all staff working from home	HR supervises IT to conduct network and equipment testing within 1 hour; administrative notification to some employees to implement a remote office management system, for employees who do not have computer equipment at home, issue portable laptop computers; E-mail / Enterprise WeChat / SMM apps / encryption software) installation / version upgrade / test
Level 4	Disastrous	All staff working from home	HR supervises IT to conduct network and equipment testing within 1 hour; implements a remote office management system for all employees and issues required office laptops and other items

VI. Position and responsibilities of incident management team members

Position	Name	Responsibility
CEO	Adam Fan	Organising and hosting IMT meetings
		Passing on information to executives and management teams
Marketing Communications	Kelly Ma	Crisis incident response and communication
		Media monitoring and response
Administration	Cheng Ziyuan	Workplace hardware facility monitoring
		Arranging logistics and relocation as needed
Human Resources	Cheng Ziyuan	Personnel contact and arrangement
		Implementation and delivery of human resources policy
		Employee benefits management
Information Technology	Lin Jianye	IT impact assessment and response
		Providing disaster recovery services for IT assets
Financial affairs	Li Shiwen	Offering financial support
Person in charge of each business division	Logan Lu	Evaluation of the impact on departments
	Zhu Renjie	Business continuity management
	Dong Chen	Communicating with heads of business divisions and employees
	Shi Xiang	Communicating with heads of business divisions and employees

VII. Contact form of incident management team

Position	Name	Responsibility	Mobile phone
CEO	Adam Fan	Organising and hosting IMT meetings	
		Passing on information to executives and management teams	13801635107
Marketing Communications	Kelly Ma	Crisis incident response and communication	
		Media monitoring and response	13764003757
Administration	Cheng Ziyuan	Workplace hardware facility monitoring	
		Arranging logistics and relocation as needed	13918446069
Human Resources	Cheng Ziyuan	Personnel contact and arrangement	
		Implementation and delivery of human resources policy	13918446069
		Employee benefits management	
Information Technology	Lin Jianye	IT impact assessment and response	
		Providing disaster recovery services for IT assets	13810329795
Financial affairs	Li Shiwen	Offering financial support	13661764079
Person in charge of each business division	Logan Lu	Evaluation of the impact on departments	13761695913
	Zhu Renjie	Business continuity management	13482322608
	Dong Chen	Communicating with heads of business divisions and employees	18616097890

	Shi Xiang			13916663520	

IIX. List of key contacts

Position	Name	Mobile phone/Wechat number	Fixed phone	Home address
CEO	Adam Fan	13801635107	51550022	Room 701, No. 5, Lane 99, West Ronghua Road, Changning District, Shanghai
Marketing Communications	Shen Xiujuan	15221529683	51666827	Shanghai
	Qiu Jiani	13564986047	51595822	Room 403, No. 2, Lane 201, Qianxi Road, Shanghai
Administration	Liu Xiaochun	15201881021	51595965	Room 602, No. 12, Lane 1086, Dongxiu Road, Pudong New District, Shanghai
	Chen Tian	15900494546	51666778	No. 21, Lane 621, Siping Road, Hongkou District, Shanghai
Human Resources	Cheng Ziyuan	13918446069	51666968	Room 403, No. 1, Lane 200, Second Ruijin Road, Luwan District, Shang-hai
	Guan Mengjiao	13120906562	51666990	Lane 126, Shunhe Road, Pudong New District, Shanghai
	Yang Wen	18516147591	51666977	No. 4312 Caoan Highway, Jiading District, Shanghai
Information Technology	Lin Jianye	13810329795	51666722	Room 302, No. 50, Lane 20, Lancun Road, Pudong New District, Shanghai
	Fang Jinpeng	18621579915	51666725	Room 502, No. 36, Lane 4567, Gaoqing Road, Beicai Town, Pudong New District, Shanghai
Finance Matters	Li Shiwen	13661764079	51666958	Room 2802, No. 7, Lane 658, Xikang Road, Shanghai
	Wang Yaping	13681721934	51666960	Room 101, No. 5, Lane 1389, Changyang Road, Yangpu District, Shang-hai
Big Data	Logan Lu	13761695913	51595830	Pudong New District, Shanghai
	Ye Jianhua	15021503422	51666848	Building 601, Meichuan Road, Putuo District, Shanghai
	Frank Liu	15021973263	51666821	No. 800 Dongchuan Road, Minhang District, Shanghai
Marketing/e-commerce operations	Kelly Ma	13764003757	51595806	Room 201, No. 18, Lane 521, Jingyuan Road, Jiading District, Shanghai
Product	Zhu Renjie	13482322608	51666906	Room 501, No. 9, Lane 460, Maotai Road, Changning District, Shanghai
Finance	Dong Chen	18616097890	51666800	Room 202, No. 128, Lane 1033, Laifang Road, Jiuting Town, Songjiang District, Shanghai
Securities/Legal	Cai Ying	13916165930	51666967	No. 15503 Lane 350, Minxing Road, Shanghai
Foshan office	Zhang Fangliang	18665496647	51595817	Zhaoxiang Road, Zumiao Street, Chancheng District, Foshan City
Yantai office	Zhou Zhiqiang	18563857007	51595848	No.9 South Tongshi Road, Zhifu District, Yantai City, Shandong Province

The above key contact lists (except office desk phones) are only open to IMT members.

IX. Contact form update

Incident management team contact form: If there are personnel changes, the human resources department will update the form and send it to IMT members.

List of key contacts: Updated monthly by the human resources department and informed to each member of IMT

All IMT members have their independent chat group on WeChat/WeChat Work.

All IMT members and key contacts have their independent chat group on WeChat/WeChat Work.

Each business division has a chat group for the management and a group for the entire staff.