# <<Client Name>>
# IT Crisis Management Plan

V1.0

INTERNAL

## Document Approval

This document has been approved by the below-mentioned authorities.

| No. | Name | Designation | Date | Approval Status |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# IT Crisis Management Plan

**Document Abstract:**

This document specifies guidelines and requirements to address IT Crisis Management.

| | |
|---|---|
| **Document ID** | |
| **Document Title** | IT Crisis Management Plan |
| **Document Classification** | Internal |
| **Revision No.** | V1.0 |
| **Document Publish Date** | 02-11-2023 |
| **Latest Review Date** | |
| **Document Ownership** | CISO |
| **Document Change Reviewers** | |
| **Document Circulation List** | All Approvers |
| | All IT Personnel of <<Client Name>> |

| Revision History | | | | |
|---|---|---|---|---|
| **No.** | **Version** | **Date of Change** | **Author** | **Revision Description** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

INTERNAL

## Table of Contents

1. Introduction ........ 3
2. Objective ........ 4
3. Applicability ........ 4
4. Approach ........ 4
5. Responsibilities ........ 5

6. Crises Classification ..... 6
7. Crisis Response Plan ..... 9
7.1 Pre-crisis Preparation ..... 9
7.1.1 Forewarning ..... 9
7.2 During Crisis ..... 10
7.2.1 Crisis Assessment ..... 10
7.2.2 Invoke Business Continuity ..... 10
7.2.3 Return to normal (Restoration Process) ..... 11
7.2.3.1 Process to revoke Business Continuity (return to normal) ..... 11
7.2.3.2 Deactivation and Restoration ..... 12
7.3 Post Crisis ..... 13
7.3.1 Incident Logging ..... 13
7.3.2 Non-conformity and Corrective Action ..... 13
8. Maintenance ..... 13
9. Annexure ..... 14
Appendix 1: IT Crisis Management Team Contacts ..... 15
Appendix 2: IT Crisis Management Team – Meeting Agenda ..... 16

INTERNAL

## 1. Introduction

Crisis Management is the proactive process through which <<CLIENT NAME>> identifies and mitigates the impact of events that pose a threat to its well-being, stakeholders, and operations. This IT Crisis Management Plan delineates the guidelines for handling IT crises within <<CLIENT NAME>>. IT crises encompass an extensive spectrum of incidents, ranging from cybersecurity breaches to system outages and data breaches.

This Plan provides steps with defined roles and responsibilities to identify, review and stabilize such incidents until the situation returns to normal.

## 2. Objective

- Detect the incident.

- Respond to incident with appropriate preliminary plan of action.
- Declare disaster (if necessary)
- Communicate with various stakeholders; and
- Conduct root cause analysis to determine corrective actions to avoid re-occurrence of incident.

## 3. Applicability

The BCMS IT Crisis Management Plan shall be applicable to the organization.

The IT Crisis Management Plan encompasses the entire organization. However, some responsibilities may also be extended to the suppliers/third party employees working for or on behalf of <<CLIENT NAME>> on the discretion of the business functions. The term 'third party employees' mentioned in the document refers to employees, consultants, and representatives, of suppliers, who are in any way accessing, processing, storing, ortransmitting any business-related information to <<CLIENT NAME>>.

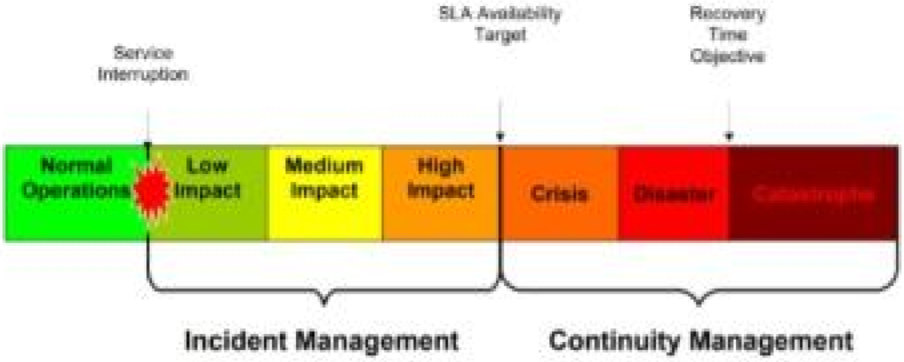
INTERNAL

## 4. Approach

This document provides a framework to identify an incident based on nature and impact. Incident response structure is divided into four phases summarized below.

- Incident Detection and Escalation
- Incident Response
- Invoke Business Continuity
- Return to Normal

The IT Crisis Management at high level consists of the Incident Management which operates from normal operations to high level impact incident is reported; and Continuity Management operates from the crisis occurence till the situation is back to normal.



## 5. Responsibilities

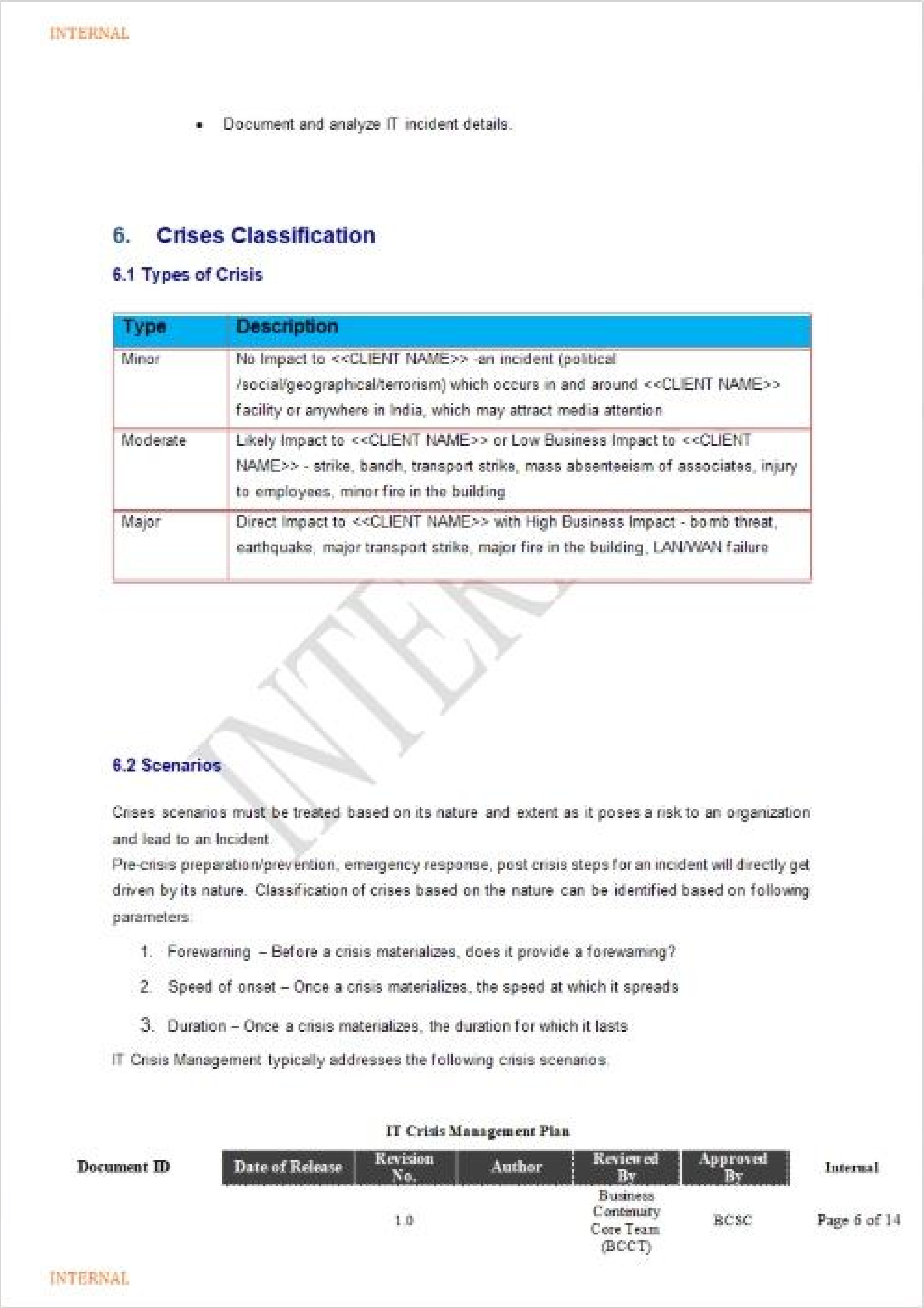
The responsibility for developing, maintaining, and exercising the IT Crisis Management Plan lies with Chief Information Security Officer (CISO). The BCM Head oversees this process and ensures its alignment with business continuity efforts.

INTERNAL

**Roles and Responsibilities**

1. CISO:
    - Oversee cybersecurity measures and efforts to protect IT assets and data.
    - Collaborate with IT teams to ensure IT security.
    - Ensure compliance with security standards and regulations.
    - Conduct cybersecurity training and awareness programs.

2. BCSC (CMT):
    - Provide strategic direction for IT crisis management.
    - Approve IT-CMP policies and procedures.
    - Allocate resources for IT crisis response.
    - Review and update the IT Crisis Management Plan regularly.
3. BCCT:
    - Activate and manage the IT-CMP during crises.
    - Coordinate IT crisis response efforts.
    - Communicate with stakeholders during IT incidents.



- Document and analyze IT incident details.

# 6. Crises Classification

## 6.1 Types of Crisis

| Type | Description |
|---|---|
| Minor | No Impact to <<CLIENT NAME>> -an incident (political /social/geographical/terrorism) which occurs in and around <<CLIENT NAME>> facility or anywhere in India, which may attract media attention |
| Moderate | Likely Impact to <<CLIENT NAME>> or Low Business Impact to <<CLIENT NAME>> - strike, bandh, transport strike, mass absenteeism of associates, injury to employees, minor fire in the building |
| Major | Direct Impact to <<CLIENT NAME>> with High Business Impact - bomb threat, earthquake, major transport strike, major fire in the building, LAN/WAN failure |

INTER

## 6.2 Scenarios

Crises scenarios must be treated based on its nature and extent as it poses a risk to an organization and lead to an Incident.

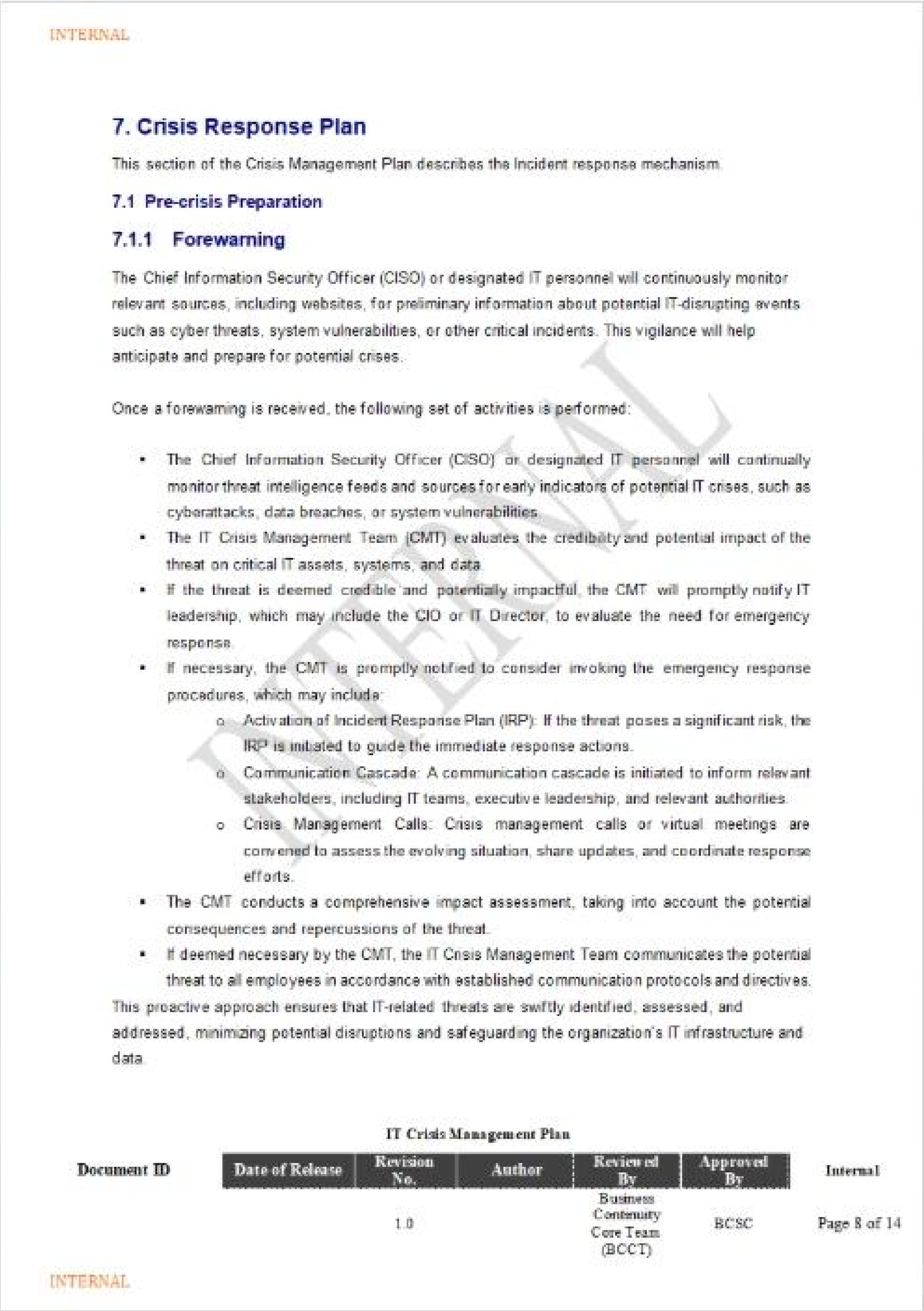
Pre-crisis preparation/prevention, emergency response, post crisis steps for an incident will directly get driven by its nature. Classification of crises based on the nature can be identified based on following parameters:

1. Forewarning – Before a crisis materializes, does it provide a forewarning?
2. Speed of onset – Once a crisis materializes, the speed at which it spreads
3. Duration – Once a crisis materializes, the duration for which it lasts

IT Crisis Management typically addresses the following crisis scenarios.

| Sr | Threat | Threat | | |
|---|---|---|---|---|
| | | Forewarning | Speed of onset | Duration |
| 1 | Disclosure of sensitive information | No or Forewarning is available only 0-2 hrs. before the threat materializes | Sudden (Within 24hrs) | Greater than 24 hrs. |
| 2 | Software failure | No or Forewarning is available only 0-2 hrs. before the threat materializes | Sudden (Within 24hrs) | Greater than 24 hrs. |
| 3 | Cyber crime | No or Forewarning is available only 0-2 hrs. before the threat materializes | Sudden (Within 24hrs) | Greater than 24 hrs. |
| 4 | Loss of records or data | No or Forewarning is available only 0-2 hrs. before the threat materializes | Sudden (Within 24hrs) | 24 hrs or less |
| 5 | Natural disasters affecting IT infrastructure | No or Forewarning is available only 0-2 hrs. before the threat materializes | Sudden (Within 24hrs) | 24 hrs or less |
| 6 | System outages | No or Forewarning is available only 0-2 hrs. before the threat materializes | Sudden (Within 24hrs) | 24 hrs or less |
| 7 | Malware infections. | No or Forewarning is available only 0-2 hrs. before the threat materializes | Sudden (Within 24hrs) | 24 hrs or less |
| 8 | Insider threats | No or Forewarning is available only 0-2 hrs. before the threat materializes | Sudden (Within 24hrs) | 24 hrs or less |

INTERNAL



# 7. Crisis Response Plan

This section of the Crisis Management Plan describes the Incident response mechanism.

## 7.1 Pre-crisis Preparation

### 7.1.1 Forewarning

The Chief Information Security Officer (CISO) or designated IT personnel will continuously monitor relevant sources, including websites, for preliminary information about potential IT-disrupting events such as cyber threats, system vulnerabilities, or other critical incidents. This vigilance will help anticipate and prepare for potential crises.

Once a forewarning is received, the following set of activities is performed:

- The Chief Information Security Officer (CISO) or designated IT personnel will continually monitor threat intelligence feeds and sources for early indicators of potential IT crises, such as cyberattacks, data breaches, or system vulnerabilities.
- The IT Crisis Management Team (CMT) evaluates the credibility and potential impact of the threat on critical IT assets, systems, and data.
- If the threat is deemed credible and potentially impactful, the CMT will promptly notify IT leadership, which may include the CIO or IT Director, to evaluate the need for emergency response.
- If necessary, the CMT is promptly notified to consider invoking the emergency response procedures, which may include:
  - Activation of Incident Response Plan (IRP): If the threat poses a significant risk, the IRP is initiated to guide the immediate response actions.
  - Communication Cascade: A communication cascade is initiated to inform relevant stakeholders, including IT teams, executive leadership, and relevant authorities.
  - Crisis Management Calls: Crisis management calls or virtual meetings are convened to assess the evolving situation, share updates, and coordinate response efforts.
- The CMT conducts a comprehensive impact assessment, taking into account the potential consequences and repercussions of the threat.
- If deemed necessary by the CMT, the IT Crisis Management Team communicates the potential threat to all employees in accordance with established communication protocols and directives.

This proactive approach ensures that IT-related threats are swiftly identified, assessed, and addressed, minimizing potential disruptions and safeguarding the organization's IT infrastructure and data.

INTERNAL

## 7.2 During Crisis

### 7.2.1 Crisis Assessment

1. When an IT incident occurs, the Chief Information Security Officer (CISO) or designated IT personnel will inform the IT Crisis Management Team (CMT) and the Crisis Assessment Team (CAT). They may convene virtually or at a designated Command Centre (CC) to assess the situation.
2. The IT-CMP will include a reference to past IT incidents and an incident tracker containing historical data. The CMT, along with the CAT, will review these records to identify any similarities or recurring patterns with the current incident and take appropriate action.
3. If the situation warrants, the CMT may initiate an employee communication cascade to ensure that all relevant personnel are informed of the incident.
4. The crisis assessment will consider several factors, including:
   - Impact of the incident on IT systems, data, and operations.
   - Inputs from partner or vendor teams, if applicable, regarding the extent of the incident.
   - Discussion within the CMT to assess the likelihood and potential impact of the incident.
   - Results of the communication cascade, including employee safety and health status updates (if invoked).
5. Based on the crisis matrix defined in the IT-CMP, as well as the assessment conducted, the CMT will determine whether to invoke Business Continuity Plan (BCP). Typically, BCP activation occurs for Moderate or Major IT crises.
6. If the CMT determines that there is no need to invoke business continuity measures, they will provide directives to the respective IT teams to resume normal IT operations.

INTERNAL

### 7.2.2 Invoke Business Continuity

Following actions are performed during the invocation of business continuity:

1. CMT to invoke appropriate business continuity plan, as per the impact.
2. BCCT to inform respective IT process/application owners and ensure their movement to the recovery location or home.
3. Process/Application to initiate operations recovery from the alternate site / work from home as per the defined business continuity plan; and necessary technology requirements to be arranged for all employees for ex. dongles/data cards.

4. CMT to invoke the communication procedure: Internal and External stakeholders (instruct the required vendors/suppliers/partners, if required, about what has happened, damage assessment status and the recovery strategy agreed and approved by the CMT.).

5. CMT to keep monitoring the situation and oversee whether,

- Teams have sufficient resources
- Teams are working as per the plan to meet time objectives; and
- Any support required in the process of recovery

Site movement snapshot:

| Scenario | Office Location | Alternate Recovery Site |
|---|---|---|
| | | |
| | | |
| | | |

INTERNAL

### 7.2.3 Return to normal (Restoration Process)

#### 7.2.3.1 Process to revoke Business Continuity (return to normal)

Steps to be taken post a Crisis to revoke the IT Business Continuity and resume business as usual:

1. The CMT will determine and specify the order in which each IT business process will return to normal operation and the timing for each. This prioritization considers resource availability and dependencies to ensure a smooth transition back to regular IT activities, preventing potential issues.
2. The Chief Information Security Officer (CISO) or designated IT personnel, often referred to as the Business Continuity Management Representative (BCMR), will inform all IT operations and support teams about the revocation of the IT Business Continuity Plan (BCP).
3. Respective IT Process/Application owners will communicate with their counterparts at any alternate or secondary IT sites, informing them of the revocation of the BCP and the resumption of operations at the primary IT site.
4. The IT Process/Application owners, in coordination with other IT staff, will begin the process of resuming operations at the primary IT site following the specified order determined by the CMT.
5. The IT Business Continuity Management (BCM) team and Crisis Assessment Team (CAT) will oversee the orderly resumption of all IT operations at the primary IT site, ensuring a seamless transition.

6. The IT team will closely monitor network bandwidth as operations resume at the primary IT site, addressing any reported issues promptly to ensure efficient closure.

### 7.2.3.2 Deactivation and Restoration

To assess, whether the business is ready to return to normal, following points should be considered:

1. The IT-CMP will assess whether the necessary resources for normal IT operations are available again. This includes people, technology infrastructure, and the primary IT site.
2. Dependencies between IT business processes will be analysed to ensure a smooth transition back to normal operations. This assessment ensures that IT systems can function cohesively.

The return to normal operations should proceed in an orderly manner to avoid discrepancies between or in the business processes. CMT to end the state of emergency by deactivating business continuity plans. This phase involves transferring all processes back to their normal state.

1. The Crisis Management Team (CMT) will formally end the state of emergency by deactivating IT Business Continuity Plans (BCP). This phase involves transferring all IT processes and systems back to their normal state.
2. IT Process/Application owners will analyze and report any work backlog that may have accumulated during the crisis. They will specify the requirements for addressing these backlogs to respective reporting managers and IT Directors.
3. The IT-CMP will ensure that the Function Directors are provided with the information on work backlogs, and appropriate resources will be allocated to the respective IT teams as needed.
4. When creating a plan to work off the backlog, factors such as the current pending workload, the workload during emergency operations, and any legal restrictions will be taken into account.

The post-crisis restoration tasks will be supervised by the Crisis Assessment Team (CAT) and the Business Continuity Management Representative (BCMR). The BCMR will share regular updates on the status of IT business restoration with the CMT.

INTERNAL

## 7.3 Post Crisis

### 7.3.1 Incident Logging

While responding to an emergency or a crisis, sequence of events, all important actions taken and all decisions made by the CMT and IT Process/Application owners must be recorded.

1. During the response to an IT emergency or crisis, all sequences of events, significant actions, and decisions made by the IT Crisis Management Team (CMT), Crisis Assessment Team (CAT), and IT Process/Application owners will be meticulously recorded.
2. The Business Continuity Management Representative (BCMR) will conduct root cause analysis for the incident to identify the underlying issues and factors contributing to the crisis.

3. To determine the true extent of business disruption, an analysis will be conducted to assess the impact on customers. This analysis is crucial for calculating the accurate business loss resulting from the disruption.
4. Relevant information regarding the damage caused by the incident, whether it's a cyberattack, system failure, or data breach, will be meticulously collected as evidence of the event leading to the IT crisis.
5. The BCM Team will be responsible for reporting and logging the incident, collecting input from the respective IT teams involved in the crisis response. IT Management will oversee the implementation of corrections and corrective actions based on the incident analysis.

BCM Team will report the incident taking inputs from respective teams involved. <<CLIENT NAME>> Management to ensure implementation of Corrections and Corrective actions.

### 7.3.2 Non-conformity and Corrective Action

The analysis should be performed by the BCMR with the persons responsible from business continuity response, and if necessary, in co-operation with the crisis action teams of the affected areas. In the event of an incident that results in the invocation of the BCP, a post-incident review shall be undertaken to suggest improvements to be undertaken. The output of this review process will trigger non-conformity and corrective actions emerged from the incident or crisis.

INTERNAL

## 8. Maintenance

This document shall be reviewed and updated on annual basis or as and when there are significant changes.

## 9. Annexure

**ABBREVIATIONS**

| | |
|---|---|
| BAU | Business As Usual |
| BCCT | Business Continuity Core Team |
| BCM | Business Continuity Management |
| BCMR | Business Continuity Management Representative |
| BCMS | Business Continuity Management System |
| BCP | Business Continuity Plan |
| CC | Command Centre |
| CMT | Crisis Management Team |

| | |
|---|---|
| DR | Disaster Recovery |
| DAT | Damage Assessment Team |
| MTPD | Maximum Tolerable Period of Disruption |
| RTO | Recovery Time Objective |
| SPOC | Single Point of Contact |

## Appendix 1: IT Crisis Management Team Contacts

| Sr | Role / Function | Name | Mobile | Email address |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

INTE

## Appendix 2: IT Crisis Management Team – Meeting Agenda

| | |
|---|---|
| **Incident Name:** | |
| **Date of incident:** | |
| **Time of incident:** | |
| **Meeting participants:** | |

**Standing Agenda:**

1. Review situation assessment or status update
   - ❑ Discuss facts
   - ❑ Discuss assumptions
   - ❑ Review previous decisions and actions (as applicable)
2. Ascertain Technology impact.
3. Discuss realized or anticipated impacts.
4. Discuss and reach consensus regarding <<CLIENT NAME>>'s response and recovery strategy.
5. Discuss and provide input to the Business Continuity and IT DR Teams regarding <<CLIENT NAME>> response and recovery priorities.
6. Review IT crisis communications efforts to date; identify upcoming, required communications to key stakeholders.
7. Agree on next CMT meeting time.

INTERNAL

************************************End of the document************************************