



Incident Response High Level Design Document

Version: 2.0

ABC Technologies Private Limited

ABC Towers Mumbai India

Date: 20/01/2012

Record of Revisions

The following is a list of revisions made to this document: **No index entries found.**

Rev	Date	Pages Affected	Reason	Summary of Technical Changes	Issued By	Approved By
1.0	10/01/2011	All	–	Initial document release.	Anuj Sharma	Anuj Sharma
2.0	20/01/2012	All		Final Document Release	Anuj Sharma	Anuj Sharma

Contents

Article I. Purpose of this document 4

Article II. Incident Categorization 5

Article III. Incident Severity Levels 6

Article IV. Global Impact Incident Response Team 7

Article V. Country Specific Impact 8

Article VI. Location Specific Impact 9

Article VII. Business Unit Specific Impact 10

Article VIII. Vendor Contact Information 12

Article IX. Global Command Centre 13

Article X. Incident Handling and Management Procedure 14

Article I. Purpose of this document

Incident can be regarded as any abnormal condition that can cause disruption in the day to day business operations of an organization. An incident may be defined as an event that may lead to a business disruption or a crisis situation. So an incident response plan is mandatory for the organizations to deal with incidents well with in timelines. . This document outlines the process to be followed for incident management. This document will contain the following:

- * Incident Categorization
- * Incident Prioritization
- * Incident Management and Handling Procedures

Article II. Incident Categorization

Type A

Global Impact

Incident in this category will be the incidents that can impact the global business of the company. For example, virus attack , data center outage, etc.

Type B

Country Specific Impact

Incident in this category will be incidents that impact the organization's business in the specific country. For example, political unrest, natural disasters, data center outages, etc.

Type C

Location Specific Impact

Incident in this category will be the incidents that impact the organization's business in the specific location. For example, political unrest, natural disasters, data center outage, fire, etc.

Type D

Business Unit Specific Impact

Incident in this category will be the incidents that impact the business activity of a specific business unit globally, countrywide or locally. For example, HR Portal Application Down, Payroll Application Down, etc.

Article III. Incident Severity Levels

After being categorized every incident will be assigned a severity level from the below levels

- * High
- * Medium
- * Low

The Levels will be decided by the Incident Response Team of the respective category.

Incident Priority	Response Time	Resolution Time
High	15 minutes	2 hours
Medium	30 minutes	4 hours
Low	90 minutes	6 hours

Article V. Country Specific Incident Response Team

Country: China							
Team Spoke Name: Sahil Sambyal							
Department: Strategy							
Emergency Contact Number: 9999999999							
Email ID: ss@abc.om							
Distribution List Email ID: git@abc.com							
Last name	First name	Title	Department/Location	Work phone	Home phone	Email	Pager/Cell phone
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666
Incident Handling and Management Team							
Team Spoke Name: Saurabh Sawhney							
Department: Design							
Emergency Contact Number:5555555555							
Email ID: ss@abc.com							
Distribution List Email ID: gitih@abc.com							
Last name	First name	Title	Department/Location	Work phone	Home phone	Email	Pager/Cell phone
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666

Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666

Incident Priority	Response Time	Resolution Time
High		
Medium		
Low		

The above information should be gathered for each country.

Article VI. Location Specific Incident Response Team

Country: China Location: Shanghai Team Spoke Name: Sahil Sambyal Department: Strategy Emergency Contact Number: 999999999 Email ID: ss@abc.om Distribution List Email ID: git@abc.com							
Last name	First name	Title	Department/Location	Work phone	Home phone	Email	Pager/Cell phone
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666
Incident Handling and Management Team. Team Spoke Name : Saurabh Sawhney Department : Design Emergency Contact Number :555555555 Email ID :ss@abc.com Distribution List Email Id:gitih@abc.com							

Last name	First name	Title	Department/Location	Work phone	Home phone	Email	Pager/Cell phone
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666

Incident Priority	Response Time	Resolution Time
High	15 minutes	2 hours
Medium	30 minutes	4 hours
Low	90 minutes	6 hours

Article VII. Business Unit Specific Incident Response Team

Business Unit: IT							
Countries Impacted: India , China							
Team Spoke Name: Sahil Sambyal							
Department: Strategy							
Emergency Contact Number: 999999999							
Email ID: ss@abc.om							
Distribution List Email ID: git@abc.com							
Last name	First name	Title	Department/Location	Work phone	Home phone	Email	Pager/Cell phone
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	888888888	777777777	aj@abc.com	66666666

Incident Handling and Management Team

Team Spoke Name: Saurabh Sawhney

Department: Design

Emergency Contact Number: 5555555555

Email ID: ss@abc.com

Distribution List Email ID: gitih@abc.com

Last name	First name	Title	Department/Location	Work phone	Home phone	Email	Pager/Cell phone
Jamwal	Arvind	Mr.	Strategy / China	8888888888	7777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	8888888888	7777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	8888888888	7777777777	aj@abc.com	66666666
Jamwal	Arvind	Mr.	Strategy / China	8888888888	7777777777	aj@abc.com	66666666

Incident Priority	Response Time	Resolution Time
High	15 minutes	2 hours
Medium	30 minutes	4 hours
Low	90 minutes	6 hours

The above information should be gathered for each of the Business Units.

Article IX. Global Command Centre

Location :	United States
Address :	ABC Towers Newyork
Hotline Number :	+112345689
Email Id :	gcc@abc.com
Global Command Centre Spoke :	Name:- Henry Thomas Contact Number:767676767 Email Id :-ht@abc.com
Global Command Centre Distribution List Email Id:-	gcc@abc.com

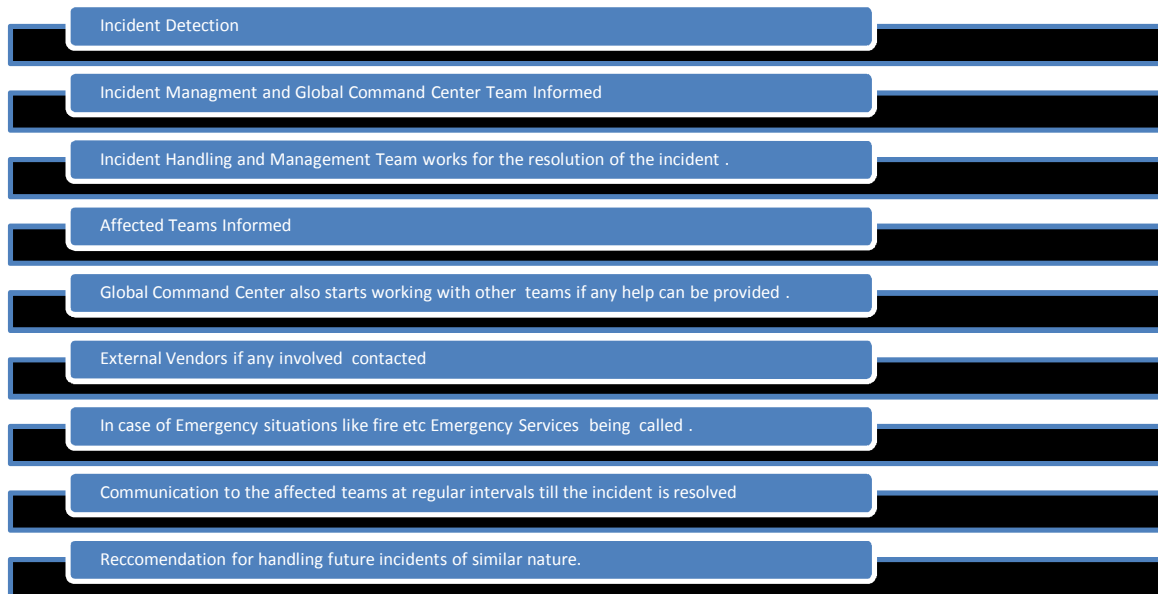
Article X. Emergency Services Contact

Country :	India
Location :	100
Police :	111
Fire Services :	123
Ambulance :	122

The above information should be collected for each location.

Article XI. Incident Handling and Management Procedure

- * Once all the above information is in place, incident detection and management teams will work together to resolve the incident, as per the defined priority levels.
- * Incident detection team will inform the Global Command Centre, as well as keep the affected and involved parties informed about the progress of the incident until resolution.
- * Any third part vendors involved should be contacted.
- * In case of emergency situations like Fire, Earthquake, etc Emergency Services should be called in.
- * If email communication cannot be made, then affected parties should be informed via telephonic calls.



Article XII. Recommendations Template

Incident Number	12735753
Incident Category	Location Specific
Incident description	Internet Connectivity Down for 1 Hour
Incident Severity	1
Impacted Teams	All the teams working from Shanghai Office
Teams Involved	IT , ISP Vendor
Recommendation for future incidents of the same type	Office was dependent on only one ISP. Other ISP should also be involved. Two ISP services should be used for redundant purposes.