

OEC Records Management Company Pvt Ltd**BUSINESS CONTINUITY PLAN****MASTER COPY OF OEC**

(Controlled Copy No: OEC/SEC/BCP-07)

| Version | Date | Prepared by | Verified by | Approved by |
|----------------|-------------|---|-----------------------|------------------------------------|
| 7.0 | 31-03-2016 | PRADEEP KOLATHERIL Sr Manager - Security | SUMANT MISRA C.O.O | VIRAL DOCTOR Executive Director |

"ORIGINAL SIGNED DOCUMENT IS A CONTROLLED DOCUMENT"

Revision History

| Revision | Issue | Date | Affected Section /Pages | Descriptions |
|----------|------------------------------|------------|--|--|
| 1 | OEC-SEC-BCP- 2009-F1, Rev.0 | 01/02/2009 | | |
| 2 | OEC-SEC-BCP- 2009-F1, Rev.01 | 05.01.2010 | Emergency Control Organization / 17 | Update name & Contact Numbers |
| | | 05.01.2010 | Business Continuity management Team / 21 | Update name & Contact Numbers |
| | | 05.01.2010 | Disaster Recovery Team | Update name & Contact Numbers |
| | OEC-SEC-BCP- 2009-F1, Rev.02 | 01.05.2010 | EPRP,DRP,BCP | Team Members & Correction |
| | OEC-SEC-BCP- 2009-F1, Rev.02 | 20.07.2010 | EPRP,DRP,BCP | Team Members & Correction |
| 3 | OEC-SEC-BCP-2009-REV-02 | AUG.2011 | EPRP,DRP AND BCP | Up date Name &Contact Nos. |
| | OEC-SEC-BCP-2009-REV-02 | Nov.2011 | BCP,DRP AND ERP | Update all the documents based on Table Top Exercise and changes in management structure |
| 4 | OEC-SEC-BCP-2009-Rev-03 | June 2012 | BCP,DRP AND ERP | Update all the documents based on Table Top Exercise and changes in management structure |
| 5 | OEC-SEC-BCP-2009-Rev-04 | June 2013 | 7.1, 8.4, 9 | BCP Management Team Name and Contact numbers updated |
| 6 | OEC/SEC/BCP-05-Rev-05 | 31-03-2014 | 7.1, 8.4, 9 | BCP Management Team Name and Contact numbers updated |
| | OEC/SEC/BCP-05-Rev-05 | 30-06-2014 | 7.1 | BCM Management Team name and contact number updated |
| 7 | OEC/SEC/BCP-06-Rev-06 | 31/8/2015 | 7.1, 8.4, 9 | BCP Management Team Name and Contact numbers updated |
| 8 | OEC/SEC/BCP-07-Rev-07 | 31/03/2015 | 7.1, 8.4, 9 | BCP Management Team Name and Contact numbers updated |

CONTENTS

| | | |
|-------|--|----|
| 1. | Introduction | 2 |
| 2. | Site Profile (Annexure-1) | 2 |
| 3. | Preamble | 3 |
| 4. | Corporate Policy | 3 |
| 5. | Process of Development | 5 |
| 5.1. | Readiness | 5 |
| 5.2. | Prevention | 5 |
| 5.3. | Response | 6 |
| 5.4. | Recovery & Resumption | 6 |
| 5.5. | Implementing & Maintaining the Plan | 6 |
| 5.6. | Evaluation & Maintenance | 6 |
| 6. | Risk Assessment(Annexure-II) | 7 |
| 7. | Team Overview | 9 |
| 7.1. | BCP Management Team | 9 |
| 8. | Emergency Preparedness and Response Plan | 10 |
| 8.1. | Purpose | 10 |
| 8.2. | General Information | 10 |
| 8.3. | Topics covered in Emergency Preparedness and Response Plan | 11 |
| 8.4. | Emergency Control Organization | 12 |
| 8.5. | ERP Document also covers | 12 |
| 8.6. | Emergency Handling Instruction for Employees | 12 |
| 9. | Disaster Recovery Plan | 13 |
| 10. | Implementing and Maintaining Plan | 15 |
| 10.1. | Educate and train teams | 15 |
| 10.2. | Educate & Train All Personnel | 15 |
| 10.3. | Test and Exercise scenarios | 15 |
| 10.4. | Test and Exercise Participation | 16 |
| 10.5. | Test and Exercise Evaluation | 16 |
| 11. | Evaluation and Maintenance | 17 |
| 12. | Standard Operating Procedures (SOP) | 18 |
| 12.1. | Operation | 18 |
| 12.2. | Security | 19 |
| 12.3. | Information Technology | 20 |

1. Introduction

Recent World events challenged us to prepare to manage previously unthinkable situations that may threaten an organization's future.

This new challenge goes beyond the emergency response plan or disaster management activities that we previously employed.

Organization now must engage in a comprehensive process best described generically as Business Continuity Plan.

It is no longer enough to draft response plan that anticipates naturally, accidentally or intentionally caused disaster or emergency scenarios.

Today's threats require the creation of an ongoing; interactive process that serves to assure the continuation of organization's core activities before, during and most critically after a major crisis scenarios.

Taking from these challenges, a Business Continuity Plan is prepared for the OECs one of the Old Branch Office at Vashi Site which not only defines various emergency plans but identifies the responsibilities to address the challenges we are in.

2. Site Profile

DEMOGRAPHICS

Navi Mumbai is a part of south Konkan coastline. This coastline joins Sahyadri mountain ranges in south and 50 to 100 m high hills in east. Navi Mumbai area lies between mountain ranges and coastline. Navi Mumbai is located between 19.5' and 19.15' latitude and 72.55' and 73.5' longitude.

CLIMATE

Navi Mumbai temperature varies from 17° C to 41 °. In winter, temperature is between 17°C to 30°C while summer temperature ranges from 36 °C to 41°C. Out of total rainfall, 90 % rainfall is experienced during June to September. Average annual humidity is 61-86%.

LOCATION Vashi

The Corporate Office of OEC Records Management Co. Pvt. Ltd. Loacated at Vashi is especially industrial zone occupied by Corporate Offices and residential zone. The place is pre planned and every structural building has enough places as built-up area and open area as well as open access to exit on external road network. The OEC record management company Pvt. Ltd. is located at Cyber One Building Office No.1902/1903 ,19 Floor ,Cyber, Vashi, Navi Mumbai. Near railway station which is a highest point accordingly to other location in Vashi from see level. Also the Office building flooring is at the 19th Floor from the ground level. Natural Disaster can affect in Vashi is a Flood, Lightening and earthquake. As per the previous record of natural disaster at Navi Mumbai in Vashi flood is major disaster impacting on surrounding population and property. As per the previous record the earthquake has not reached the level affecting a property and human casualties.

The OEC is in Record storage business. It conducts a physical record storage and supporting operations along with Administration, Purchases, IT, back office Processing, Xeroxing, & also have supporting services as Electrical maintenance, power generator, and general office equipment. The man made disaster can affect OEC are mainly Electrical short circuit, wrong handling equipment, Workplace violence, riot & social Violence, Fire and indiscipline in work. **OEC Records Management Co. Pvt. Ltd. Having 10 Branches across India .**

Khopoli

Pune

Kheda

Vadodara

Hyderabad

Chennai

Kolkata

Lucknow

Dharuhera (Delhi NCR)

Bhopal

3. Preamble

The process followed while developing the BCP is mainly consist of –

- Readiness
- Prevention
- Response
- Recovery / Resumption
- Test and Train
- Evaluate and Maintain

The level of disaster effect may vary widely but the basic approach of preparedness and response is constant.

In the simplest of terms, it is thought that it is a good business for OEC to secure its assets and with this in mind prepared BCP for OEC to budget for and secure the necessary resources to make it happen.

Appropriate administrative structures have been put in place to effectively deal with the crisis management. The personnel used for crisis management is assigned to perform those roles as part of their normal duties and not expected to perform them on a voluntary basis.

The contents of this BCP Documents are –

- Business Continuity Plan – Policy
- Development of Business Continuity Plan – Methodology
- Risk Assessment
- Emergency Response Plan
- Disaster Recovery Plan
- Implementing and Maintaining the Plan
- Evaluation and Maintenance
- Standard Operating Procedures

4. Corporate Policy

At Corporate level, BCP Policy has been prepared and is duly authorized by Chairman.

OEC Records Management Company Pvt Ltd BCM policy is applicable to all sites and offices of **OEC** located across the country.

The Policy has been drafted taking in to consideration main elements of BCP –

Readiness – Prevention – Response – Recovery & Resumption

It is committed to undertake all reasonable and appropriate steps to protect people, property and business interest. It also includes definition of crisis which is given below.

Definition of Crisis: ‘Crisis’ is any global, regional or local, natural or human caused event or business interruption that runs the risk of...

- Escalating in intensity.
- Adversely impacting organization’s financial position.
- Causing harm to people or damage to property.
- Falling under close media or statutory compliance.
- Interfacing with normal operations.
- Waste of significant time of senior management and / or financial resources.
- Jeopardizing the organization’s reputation, products and therefore negatively impacting its future.

The policy will be displayed at strategic places at the site for the effective communication to all the employees.

OEC will make all endeavours to ensure that during any training program for the employees, the elements of policy & the purpose will be explained to achieve ultimate aim as stated earlier.

The Corporate Policy of Business Continuity Plan is to –

- Develop & maintain procedure to deal with emergencies commensurate with the risk to business, people and the environment.
- Create an ongoing interactive process that serves to assure the continuation of our core activities before, during and most importantly after a major crisis event.
- Provide facilities, equipment and loss prevention measures to minimize the impact of every assessed emergency scenario.
- Provide appropriate Budget Allocation for development and maintenance of Business Continuity plan.
- Identify and train individuals with specific roles & responsibilities associated with business continuity management.
- Practice and test the emergency procedure & business recovery objectives at a set frequency to ensure the effectiveness in every stage of crisis/disaster management.
- Carry out Risk Assessment to eliminate or reduce the hazards as an ongoing activity.

The Policy is applicable to all sites and offices.

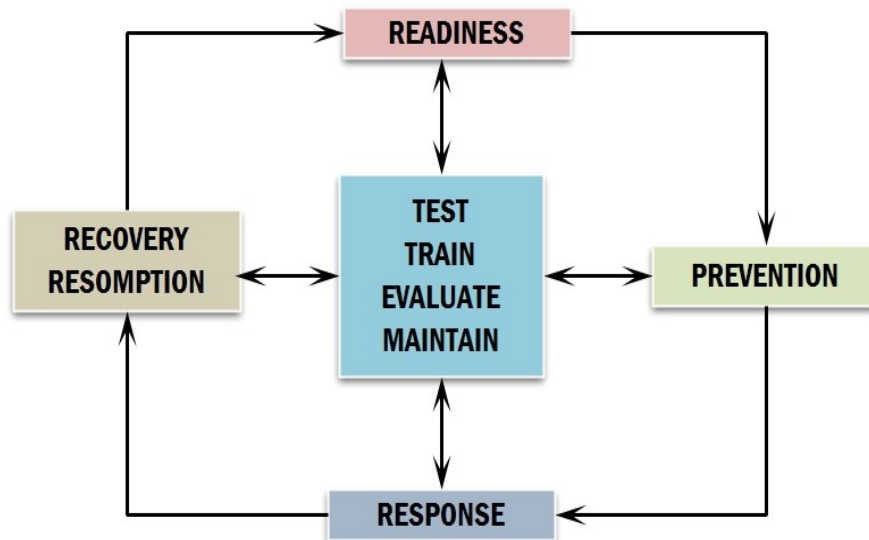
Chairman

Date: _____

Place: Mumbai

OEC Records Management Company Pvt Ltd

5. Process of Development



This section addresses the process of preparing business continuity plan (BCP) which includes –
Readiness – Prevention – Response – Recovery / Resumption – Implementation & Maintenance – Evaluation & Maintenance

5.1. Readiness

Objective: Address the preparatory steps required to provide a strong foundation on which to build a Business Continuity plan.

Steps –

- 1.1. Assign Accountability
- 1.2. Perform Risk Assessment
- 1.3. Conduct Business impact analysis
 - Identify critical process
 - Assess impact if crisis were to happen
 - Determine maximum allowable outage and recovery time objectives
 - Identify resources required for resumption & recovery
- 1.4. Agree on Strategic plans
- 1.5. Crisis Management & Response Team development

5.2. Prevention

Objective: Address those areas good planning will allow Organization to avoid, Prevent or limit the impact of a crisis occurring.

Steps –

- 2.1. Compliance with corporate policy
- 2.2. Mitigation Strategies
 - Device Mitigation strategies
 - Resources needed for mitigation

- Monitoring systems & resources
- 2.3. Avoidance, Deterrence and Detection
 - Employee behaviour to support
 - Facility security programme

5.3. Response

Objective: Develop the steps that will be required to respond effectively, appropriately & timely if a crisis occurs.

Steps –

- 3.1. Potential Crisis recognition
 - Identification & Recognition of danger Signals
 - Responsibility to recognize & report potential crises
- 3.2. Notify the Team
- 3.3. Assess the situation
- 3.4. Declare Crisis
- 3.5. Execute the plan
- 3.6. Communication
 - Identify the Audience communicating with Audiences by Official spokesperson
- 3.7. Resource Management
 - Human element
 - Accounting for all individuals
 - Notification to next of Kin
 - Family representatives
 - Pay roll for Crisis Management Centre

5.4. Recovery & Resumption

Objective: Develop policies, Procedures & plans to bring the organization out of the crisis, Recover / resume critical Processes and finally return to normal operations.

Steps –

- Damage & impact Assessment
 - Crisis involving physical damage
 - Crisis not involving physical damage
- Resumption of Critical & Remaining processes
 - Process resumption prioritization
 - Resumption of critical processes
 - Return to normal operations

5.5. Implementing & Maintaining the Plan

Objective: Train and Educate team member as well as general employee Population and validate and enhance the Business Continuity Plan

Steps –

- Educate and train
- Test the Business continuity plan

5.6. Evaluation & Maintenance

Objective: Keep the Business Continuity Plan relevant to the organization using rigorous maintenance & evaluation Program

Steps –

- 6.1. Develop Business continuity Plan review
- 6.2. Develop Business continuity plan Maintenance Schedule
- 6.3. **Risk Assessment**

The Risk Assessment is simply a careful examination of what in the work could cause harm to people, property and asset so that one can weigh up whether enough precautions have been taken or should do more to prevent harm. Workers and others have right to be protected from harms caused by failure to take reasonable control measures.

In order to effectively assess and manage risk for which it has responsibility and over which it has control or influence OEC have identified and assessed that appropriate measures are in place to manage those risk and resources which are targeted where it will provide maximum benefit.

Five steps approach is adopted –

- 1) Identify the hazard.
- 2) Decide whom might be harmed and how. Assess associated risk in terms of severity of the harms that could result and likelihood of that harm. Work out risk significant rating.
- 3) Evaluate the risk and decide whether existing precautions are adequate or whether more should be done or select controls to minimize the overall risk according to the following hierarchy.
 - a. Elimination and substitution
 - b. Engineering and other control measures
 - c. Administrative Controls
- 4) Record the findings and prepare action plan with target date of completion based on priority-high, medium and low
- 5) Review the assessment and revised it, if necessary

Risk Assessment is not once-and-for-all activity, as work activity changes, knowledge and understanding of hazard and risk may develop over the time, OEC therefore, considered it as on-going activity and will review when –

 - α. Changes in work place activities
 - β. Whenever new hazard information available
 - χ. Following an adverse event
 - δ. Degree of risk changes

The detailed Guideline on risk assessment is available.

Using available information about known or anticipated risk, OEC Branch office at Vashi Site have carried out the risk assessment following the above guidelines and reviewed the risk that could possibly impact the business and rated the likelihood of each. A risk assessment matrix is attached separately and is taken as aid for identification for risk and prioritization mitigation/ planning strategies.

At Vashi site, safety audit was carried out in Jun 2007 which included electrical safety. Actions needing immediate attentions were completed. Follow up audit was also carried out.

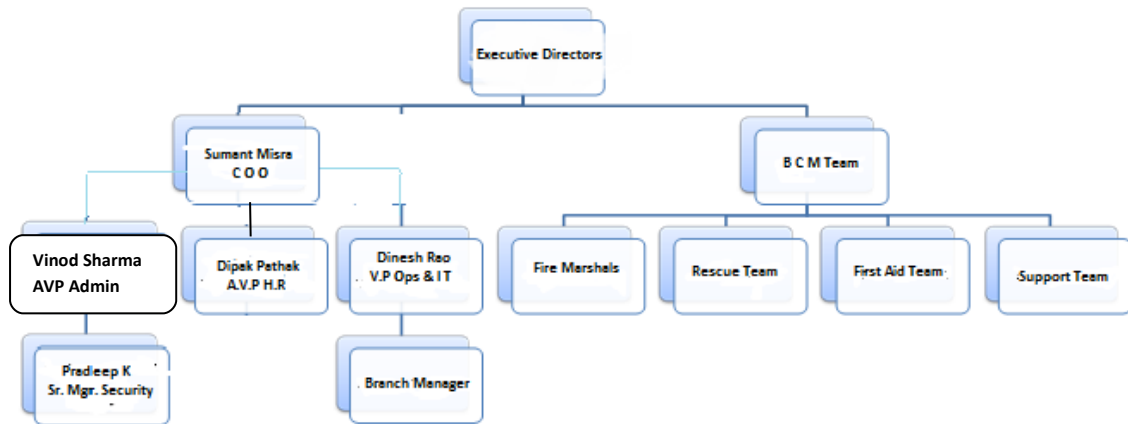
Vashi

| S No | Threat or Triggers | Likelihood x Impact | | = Risk Factor |
|---------|---|--------------------------------------|--------------------------------------|-----------------------------------|
| | | (Rate 1 – 5) | (Rate 1 – 5) | or Relative Weight |
| 1. | Earthquake | 1 | 2 | 2 |
| 2. | Power Failure | 2 | 1 | 2 |
| 3. | Fire | 3 | 4 | 12 |
| 4. | Hurricane | N/A | N/A | N/A |
| 5. | Flood | 2 | 2 | 4 |
| 6. | Bombing | 1 | 3 | 3 |
| 7. | NBC Attack | Cannot Predict for near Future | Cannot Predict for near Future | Cannot Predict for near Future |
| | – Nuclear | | | |
| | – Biological | | | |
| | – Chemical | | | |
| 8. | Sabotage | 1 | 2 | 2 |
| 9. | Law Suits | 1 | 2 | 2 |
| 10. | Hostile takeover | 1 | 1 | 1 |
| 11. | Work Stoppage | 1 | 2 | 2 |
| 12. | Work Place violence & Employee misbehaviour | 1 | 2 | 2 |
| 13. | Protest / Riots | 2 | 3 | 6 |
| 14. | Political Bandh / Strike | 2 | 2 | 4 |
| 15. | Security Failure | 1 | 2 | 2 |
| 16. | IT Failure | 1 | 5 | |
| 17. | Water Leakage | 3 | 2 | 6 |
| 18. | Drainage Choke up | 3 | 3 | 9 |
| 19. | Vehicle damage | 1 | 2 | 2 |
| 20. | Collapse of Racks | 1 | 1 | 1 |

| Likelihood rating | Impact rating |
|-------------------|-----------------|
| 1: Very Low | 1: Negligible |
| 2: Low | 2: Some |
| 3: Medium | 3: Moderate |
| 4: High | 4: Significance |
| 5: Very High | 5: Severe |

6. Team Overview

6.1. BCP Management Team



| BCM Team Members | Mobile | Email address |
|-----------------------|------------|-----------------------------------|
| Mr Vishal Doctor | 9820353072 | vishal.doctor@oecrecords.com |
| Mr Viral Doctor | 9820353073 | viral.doctor@oecrecords.com |
| Mr Sumant Misra | 7498914210 | sumant.misra@oecrecords.com |
| Mr Dinesh Rao | 7498914211 | dinesh.rao@oecrecords.com |
| Mr Vinod Sharma | 9323471160 | vinod.sharma@oecrecords.com |
| Mr Pradeep Kolatheril | 7498914217 | pradeep.kolatheril@oecrecords.com |
| Mr Dipak Pathak | 9321470507 | dipak.pathak@oecrecords.com |

7. Emergency Preparedness and Response Plan

(Document No: OEC/SEC/EPRP-02)

7.1. Purpose

- 1) The OEC-Vashi Emergency Preparedness & response Plan is intended to:
 - Establish protocols to be followed when an emergency occurs;
 - Create a framework for the allocation and management of resources; and
 - Define roles and responsibilities in order to enable the site to effectively cope with a major site wide emergency.
- 2) The plan explains how departments should respond when a catastrophic emergency occurs. It includes how key organizations are expected to work together to minimize the impact of disaster on employees, the community and the environment. It also outlines how departments are to implement respective plans for full disaster recovery.
- 3) An emergency is defined as any unplanned event that jeopardizes the employees, the assets, and/or the physical structure of the building. The primary goal in this Emergency Preparedness & Response Plan is to reduce, minimize or eliminate the risk to employees or property through prevention, early detection, notification, evacuation, control and mitigation, and recovery. This plan will minimize or prevent disruptions to the continuity of essential facility operations throughout emergency situations. The basic information in this plan includes: organizational roles and responsibilities, communication and reporting.
- 4) This Emergency Preparedness & Response Plan addresses all issues associated with Emergency management; the event itself, along with any other associated issues. The plan is flexible enough to be easily used no matter what the actual situation is. However, every possible eventuality cannot be anticipated. To do so would result in plans that would not be reasonable to use. Consequently, a set of assumptions is used to guide the development of emergency response actions.

7.2. General Information

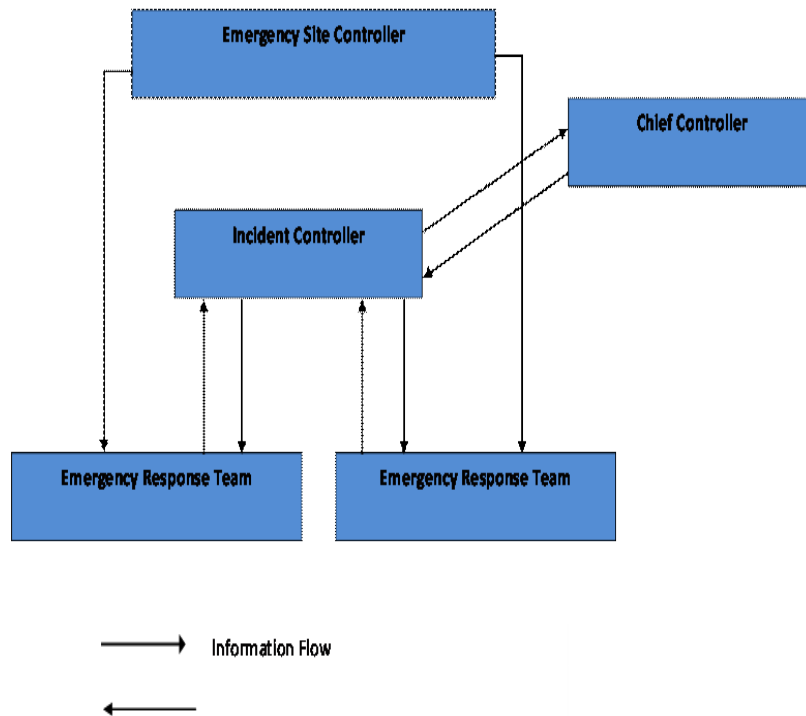
1. Emergency procedures have been devised after studying the processes and operations being carried out at the site and the risk, hazards associated.
2. EPRP contains procedures for responding to foreseeable natural and manmade emergencies.
3. EPRP contains procedures for emergency evacuation, fire prevention and response and making internal and external notifications.
4. EPRP and associated procedures shall be updated as required to reflect change in physical conditions, personnel, activities being carried out, external emergency response services and other factors.
5. An adequate alarm/communication system has been provided to alert site personnel of emergency situation occurred.

6. Alarm/communication systems are regularly tested at least annually and serviced and maintained by trained personnel.
7. Locations have been identified and assigned personnel responsibility for emergency response and First Aid.

7.3. Topics covered in Emergency Preparedness and Response Plan

1. Emergency Response Organization and Responsibilities of Personnel
2. Departmental Rolls & responsibility
3. Emergency Control Organization
4. Emergency Alerting Procedures
5. Emergency Handling Procedures
 - a. Medical Emergency
 - b. Explosion
 - c. Electrical Emergency
 - d. Fire
 - e. Bomb Threat and or any Natural Calamity
6. Emergency Evacuation Procedure
7. Incident / Emergency / Investigation
8. Dealing with media
9. Site Status
10. Drills & Plan Review
11. Annexure –
 - a. Emergency Phone Numbers
 - b. List of Emergency Team Members
 - c. List of First Aid Team Members
 - d. List of Fire Extinguishers
 - e. List of Location of First Aid Boxes
 - f. Incident report
 - g. Status and Action taken Report for Fire Team
 - h. Post Event Critic Guide
 - i. Assembly Point Plan
 - j. Bomb Threat Check List

7.4. Emergency Control Organization



| Emergency Organization Members | | Responsibility | Mobile |
|--------------------------------|--------|---|------------|
| Mr Vinod Sharma | [I] | Emergency Site Controller | 9323471160 |
| Mr Pradeep Kolatheril | [II] | Emergency Site Controller & Incident Controller | 7498914217 |
| Mr Satish Divekar | [I] | Incident Controller | 7498914213 |
| Mr Viral Doctor | [I] | Chief Coordinator | 9820353073 |
| Mr Sumant Misra | (I) | Chief Coordinator | 7498914210 |

7.5. ERP Document also covers

- 1) Post-event critique guide
- 2) Accident / Emergency Investigation
- 3) Dealing with Media

7.6. Emergency Handling Instruction for Employees

[separate document (OEC-SEC-EHIE-01) is prepared]

This contains what employees have to do for various types of identified emergency scenario. This document will be used for training as well as it is planned to prepare booklet or instruction boards which will remind employees continuously and will help organization to mitigate / respond to the emergency immediately.

8. **Disaster Recovery Plan**

Disaster Recovery Plan is prepared (Document No: OEC/SEC/DRP-07) which contains the policies & procedures to bring the organization out of the crisis, recover / resume the critical process and finally return to normal operations.

The Business Continuity Management team & Disaster Recovery team have been identified.

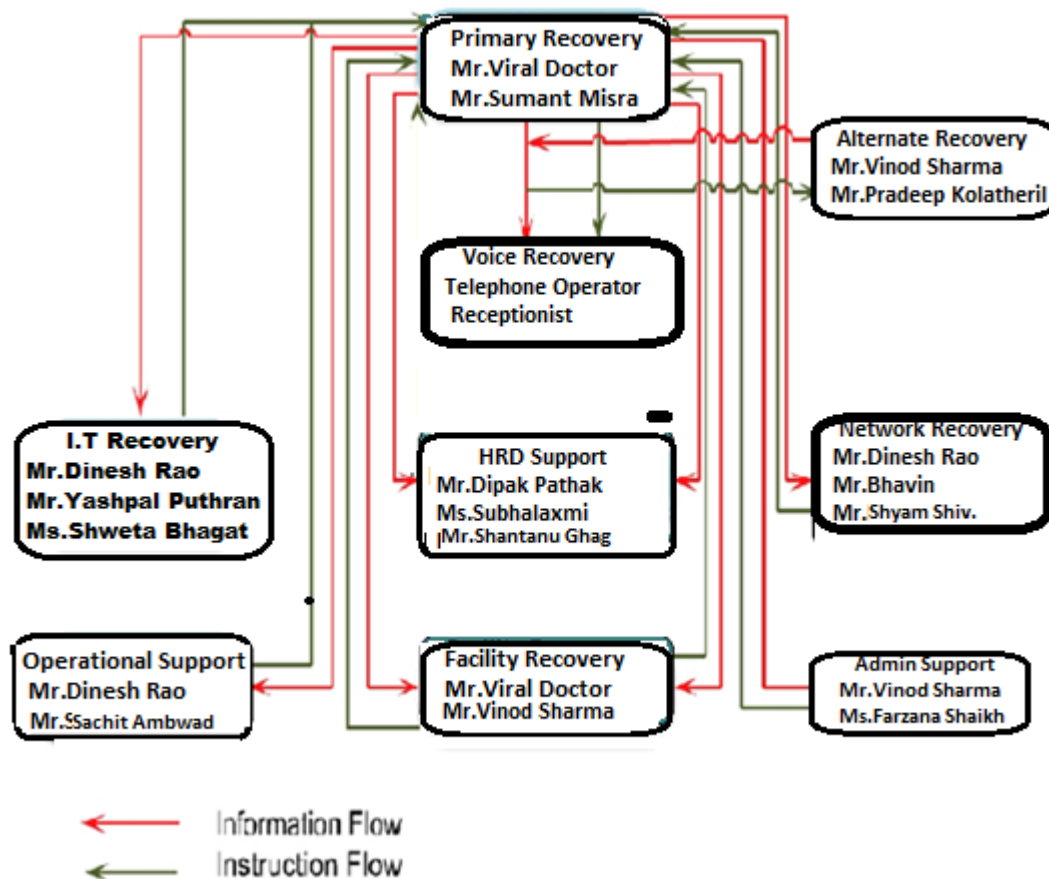
The disaster recovery plan outlines all the elements of recovery and resumption and the index of the document is as below –

- Recovery Objectives
- Activation Authorities
- Authorities Access List
- Disaster Impact and Recovery Assessment
- Recovery Strategy
- Team Overview
- Team Charters
- DRP Participants
- Recovery Strategy Overview
- Recovery Teams Check List
- Mobilization Time
- Alternate Site Setup
- Recovery Ranking
- Guideline & Formation of reporting teams

APPENDIX

- A. Definitions of Various Teams
- B. Vendors Dependency List
- C. DRP Change Management Form
- D. Status & Action taken report for DRP Team

CENTRAL DISASTER RECOVERY TEAM



| BCM Team Members | Mobile | Email address |
|-----------------------|---------------|--|
| Mr Viral Doctor | 9820353073 | viral.doctor@oecrecords.com |
| Mr Sumant Misra | 7498914210 | sumant.misra@oecrecords.com |
| Mr Dinesh Rao | 7498914211 | dinesh.rao@oecrecords.com |
| Mr Vinod Sharma | 9323471160 | vinod.sharma@oecrecords.com |
| Mr Dipak Pathak | 9321470507 | dipak.pathak@oecrecords.com |
| Mr Pradeep Kolatheril | 7498914217 | pradeep.kolatheril@oecrecords.com |
| Ms Farzana Shaikh | 7498914219 | admin.ho@oecrecords.com |
| Ms Subhalaxmi | 9324901867 | subhalaxmi.kadali@oecrecords.com |
| Mr Shantanu Ghag | 7498914201 | hr@oecrecords.com |
| Mr Bhavin Bheda | 7498914214 | bhavin.bheda@oecrecords.com |
| Mr Yashpal Puthran | 7498914215 | yashpal.puthran@oecrecords.com |
| Ms Sweta Bhagat | 9324132475 | sweta.bhagat@oecrecords.com |
| Mr Shyam Shivcharan | 7498914212/16 | tech.support@oecrecords.com |

9. Implementing and Maintaining Plan

This section of the guideline contains those functions and tasks required for the business continuity plan to remain a living document: one that grows and changes with the organization and remains relevant and actionable.

9.1. Educate and train teams

The Business Continuity Management and response teams will be educated about their responsibilities and duties. Check lists of critical actions and information to be gathered are valuable tools in the education and response processes. Teams will be trained at

least annually and new members will be trained when they join. These teams will also be trained with respect to prevention of crisis.

9.2. Educate & Train All Personnel

All personnel will be trained to perform their individual responsibilities in case of a crisis. They will also be briefed on the key components of the BCP, as well as the response plans that affect them directly. Such training could include procedures for evacuation; check in processes to account for employees, arrangements at alternate worksites.

9.3. Test and Exercise scenarios

Testing scenarios will be designed using the events identified in the risk assessment, whichever is suitable for OEC operation including time frame as per requirements.

| TYPE | ORIENTATION (Introductory, overview or education sessions) | TABLETOP (Practical or simulated exercise) |
|-----------------|---|--|
| Goal | Provides overview of plan to motivate and familiarize participants with team roles, responsibilities, expectations, and procedure. Useful when implementing new plan or adding new staff / leadership | Present limited simulated scenario (presented in narrative format) to evaluate plans, procedure, co-ordination and assignment of resources. Addresses one issue at a time and allows breaks for discussion. Familiarizes participants with specific roles. |
| Benefits | Informal, easy to conduct and low stress | Practices team building and problem solving. |
| Issues | | Somewhat detailed with a medium stress level. |
| Needs | 30 days planning cycle 1 hour duration | 2-3 months planning cycle, 2-3 hours duration and 30-60 minutes debriefing. |

| TYPE | FUNCTIONAL (walk-through or specialized exercise) | FULL SCALE (live or real-life exercise) |
|-----------------|---|---|
| Goal | | Deploys personnel, equipment, and resources to a specific location for the real time, real-life simulation of a scenario, incorporates as many BCP function as possible to test the entire BCP. |
| Benefits | | Evaluates operational capabilities in an interactive manner, facilitates communication and coordination across organization and public private sector. |
| Issues | | Detailed, expensive and highly stressful. |
| Needs | | 6-8 months planning cycle ,6-8 hours duration plus 60-90 minutes debriefing |

9.4. Test and Exercise Participation

Various groups from the organization itself, as well as from the public sector if found necessary will participate in the tests.

Department:

- Security
- Operations
- Facilities
- Human Resources
- Legal
- Finance
- Information Systems
- Logistic

Public Sector:

Police, Fire, Emergency Medical Services

9.5. Test and Exercise Evaluation

After completion, the test will be critically evaluated. The evaluation will include, among other things, an assessment of how well the goals and objectives of the test were achieved, the effectiveness of participation, and whether the BCP itself will function as anticipated in the case of a real crisis. Future testing, as well as the BCP itself, will then be modified as necessary based on the test results.

10. Evaluation and Maintenance

10.1. Develop BCP Review Schedule

The BCP will be regularly reviewed and evaluated. Reviews would occur according to a pre-determined schedule, and documentation of the review will be maintained as necessary. The following factors can trigger a review and will otherwise be examined once a review is scheduled.

- **Risk Assessment:** The BCP will be reviewed every time a Risk Assessments is completed for the organization. The results of the Risk Assessment can be used to determine whether the BCP continues to adequately address the risks facing the organization.
- **Sector / Industry Trends:** Major sector / industry initiatives should initiate a BCP review. General trends in the sector/industry and in business continuity planning techniques can be used for benchmarking purposes.
- **Regulatory Requirements:** New regulatory requirements may require a review of the BCP.
- **Event Experience:** A review will be performed following a response to an event whether the BCP was activated or not. If the plan was activated, the review will take into account the history of itself, how it worked, why it was activated, etc. If the plan was not activated, the review will examine why and whether this was an appropriate decision.
- **Test / Exercise Results:** Based on test / exercise results, the BCP will be modified as necessary.

10.2. Develop BCP Maintenance Schedule

Regular maintenance of the BCP cannot be over emphasized, clear responsibilities for BCP maintenance will be assigned. Maintenance can be either planned or unplanned and will reflect changes in the operation of the organization that will affect the BCP. The following are examples of procedure, systems, or processes that may affect the plan:

- Systems and application software changes
- Changes to the organization and its business processes
- Personnel changes (employees and contractors)
- Supplier changes
- Critical lessons learned from testing
- Issues discovered during actual implementation of the plan in a crisis
- Other items noted during review of the plan and identified during the Risk assessment

11. Standard Operating Procedures (SOP)

11.1. Operation

The departments have prepared SOPs on the topics related to OEC, operations at Vashi which is to be followed strictly to achieve organization's objective of ZERO-ERROR or ZERO-COMPLAINT from the clients. To ensure this continuous monitoring by operational head is being done besides. 'On the Job' training is also given to all those involved in the operations. The lists of SOPs are attached.

The copies of SOPs are maintained in respective operational areas.

The SOPs are revised annually or earlier if there is any change in operations as per client's requirements.

| No | Process Note | Code |
|-----|--|----------------------|
| 1. | TELEPHONE AND MOBILE POLICY | OEC-ADMIN |
| 2. | INSTRUCTION - PURCHASE MATRIX | OEC-MR-PU-I-01 |
| 3. | FORM - VENDOR SERVICE PROVIDER REVIEW FORM | OEC-MR-PU-F-01 |
| 4. | FORM - VENDOR COMPARISON MATRIX | OEC-MR-PU-F-02 |
| 5. | POLICY FOR PURCHASE | OEC-ADM-PU-P-01 |
| 6. | PURCHASE PROCESS. | OEC-ADM-PU-P-02 |
| 7. | VENDOR REGISTRATION FORM | OEC-ADM-PU-F-03 |
| 8. | INTERNAL AUDIT POLICY AND PROCEDURE | OEC-IAD-IA-P-01 |
| 9. | ISO 9001:2015 | Cert No. IND16.3164U |
| 10. | COLLECTION POLICY | OEC-COLL-0 |
| 11. | FORM - CUSTOMER COMPLAINT REGISTER | OEC-CSD-CM-F-01 |
| 12. | CUSTOMER COMPLAINT MANAGEMENT PROCESS | OEC-CSD-CM-P-01 |
| 13. | FORM - CUSTOMER FEEDBACK FORM | OEC-CSD-CF-F-01 |
| 14. | CASH AND BANK POLICY | OEC-Fin |
| 15. | PURCHASE PROCEDURE | OEC-Fin |
| 16. | DEBTORS WRITE OFF POLICY | OEC-ACC-WO-P-02 |
| 17. | EARNED LEAVE POLICY | OEC-HR |
| 18. | ATTENDANCE POLICY | OEC-HR |
| 19. | SEXUAL HARASSMENT POLICY | OEC-HR |

| | | |
|-----|--|-----------------|
| 20. | HR-TRAVEL POLICY | OEC-HR-005 |
| 21. | EMPLOYEE PROBATION & CONFIRMATION POLICY | OEC-HR-006 |
| 22. | EMPLOYEE SEPARATION & TERMINATION POLICY | OEC-HR-007 |
| 23. | ON-BOARDING POLICY | OEC-HR-008 |
| 24. | PERFORMANCE APPRAISAL POLICY | OEC-HR-009 |
| 25. | SALARY ADVANCE POLICY | OEC-HR-010 |
| 26. | EMPLOYEE GRIEVANCE POLICY | OEC-HR-011 |
| 27. | EQUAL OPPORTUNITY POLICY | OEC-HR-012 |
| 28. | KRA VARIABLE PAYOUT POLICY | OEC-HR-013 |
| 29. | INSURANCE POLICY - GROUP MEDICLAIM & ACCIDENTAL POLICY | OEC-HR-014 |
| 30. | FORM - PERSONAL DEVELOPMENT PLAN | OEC-HRD-TR-F-01 |
| 31. | FORM - TRAINING RECORD | OEC-HRD-TR-F-02 |
| 32. | TRAINING PROCESS | OEC-HRD-TR-P-01 |
| 33. | RECRUITMENT POLICY & PROCESS | OEC-HRD-RE-P-01 |
| 34. | EMPLOYEE PROMOTION POLICY | OEC-HR-EP-P-16 |
| 35. | INFORMATION SECURITY POLICY | ISPOL |
| 36. | IT PROCEDURE | OEC-IT-PRO |
| 37. | IT REQUISITION FORM | OEC-IT-F05 |
| 38. | FORM - CORRECTIVE ACTION NOTE | OEC-MR-CA-F-01 |
| 39. | FORM - CORRECTIVE ACTION TRACKER | OEC-MR-CA-F-02 |
| 40. | FORM - DOCUMENT CHANGE TRACKER | OEC-MR-DC-F-01 |
| 41. | FORM - NON-CONFORMING PRODUCT SERVICE REGISTER | OEC-MR-NC-F-01 |
| 42. | DATA ANALYSIS PROCESS | OEC-MR-DA-P-01 |
| 43. | DOCUMENT CONTROL PROCESS | OEC-MR-DC-P-01 |
| 44. | MEASUREMENT PROCESS | OEC-MR-ME-P-01 |
| 45. | CORRECTIVE ACTION PROCESS | OEC-MR-CA-P-01 |
| 46. | RECORD CONTROL PROCESS | OEC-MR-RC-P-01 |
| 47. | MANAGEMENT REVIEW PROCESS | OEC-MR-MR-P-01 |
| 48. | NON CONFORMANCE MANAGEMENT PROCESS | OEC-MR-NC-P-01 |

| | | |
|-----|---|-----------------|
| 49. | INTERNAL QUALITY AUDIT PROCESS | OEC-IAD-IA-P-01 |
| 50. | FORM - INTERNAL QUALITY AUDIT PLAN | OEC-IAD-IA-F-01 |
| 51. | FORM - LIST OF INTERNAL QUALITY AUDITORS | OEC-IAD-IA-F-02 |
| 52. | FORM - INTERNAL QUALITY AUDIT SCHEDULE | OEC-IAD-IA-F-03 |
| 53. | FORM - INTERNAL QUALITY AUDIT REPORT | OEC-IAD-IA-F-04 |
| 54. | FORM - SUMMARY OF INTERNAL QUALITY AUDIT FINDINGS | OEC-IAD-IA-F-05 |
| 55. | FORM - QUALITY OBJECTIVE & PERFORMANCE MEASUREMENT REPORT | OEC-MR-ME-F-01 |
| 56. | INSTRUCTION FOR NUMBERING OF DOCUMENTS | OEC-MR-DC-I-01 |
| 57. | PROCESS FOR MANAGING PICKUP | OEC-OPS-PP-P-01 |
| 58. | REFILE PROCESS (INTERNAL & EXTERNAL) | OEC-OPS-RF-P-04 |
| 59. | DESTRUCTION & RETENTION PROCESS | OEC-OPS-DR-P-02 |
| 60. | PERMOUT PROCESS | OEC-OPS-PR-P-03 |
| 61. | RETRIEVAL PROCESS | OEC-OPS-RT-P-05 |
| 62. | SCANNING PROCESS | OEC-OPS-BS-P-06 |
| 63. | PICKUP REQUEST INSTRUCTION | OEC-OPS-PP-F-01 |
| 64. | TRANSMITTAL FORM | OEC-OPS-PP-F-02 |
| 65. | LIST OF AUTHORIZED PERSONS | OEC-OPS-PP-F-03 |
| 66. | CHECKLIST OF RESTRICTIONS | OEC-OPS-PP-F-04 |
| 67. | MASTER SCHEDULE | OEC-OPS-PP-F-06 |
| 68. | PICKUP SHEET | OEC-OPS-PP-F-07 |
| 69. | DELIVERY CHALLAN | OEC-OPS-PP-F-08 |
| 70. | PICKUP CHECKLIST | OEC-OPS-PP-F-09 |
| 71. | LOGISTICS CHECKLIST | OEC-OPS-PP-F-10 |
| 72. | GUIDELINES FOR ASSESSMENT OF RECORD | OEC-OPS-PP-I-01 |
| 73. | SITE ASSESSMENT REPORT | OEC-OPS-PP-F-11 |
| 74. | OPERATING PROCEDURE FOR AOD MANAGEMENT (BARCLAYS) | OEC-OPS-AM-P-07 |
| 75. | OPERATING PROCEDURE FOR AOD MANAGEMENT (HDFC) | OEC-OPS-AM-P-08 |
| 76. | OPERATING PROCEDURE FOR AOD MANAGEMENT (KMBL) | OEC-OPS-AM-P-09 |

| | | |
|------|--|-----------------|
| 77. | OPERATING PROCEDURE FOR ARCHIVAL AND STORAGE OF ECBOP-AODS | OEC-OPS-AS-P-10 |
| 78. | OPERATING PROCEDURE FOR AVAILING AUDIT FACILITY BY CUSTOMER | OEC-OPS-AF-P-11 |
| 79. | OPERATING PROCEDURE FOR DATA ENTRY FOR RECORDS - FILE MANAGEMENT | OEC-OPS-DE-P-12 |
| 80. | OPERATING PROCEDURE FOR NDML-KRA DATA ENTRY, SCANNING AND STORAGE PROJECT | OEC-OPS-NP-P-14 |
| 81. | RECONCILIATION PROCEDURE OF HDFC BANK RETAIL LIABILITY ACCOUNT OPENING FORMS (AOD) | OEC-OPS-AR-P-13 |
| 82. | SITE ASSESSMENT SCHEDULE | OEC-OPS-PP-F-13 |
| 83. | SITE ASSESSMENT TRACKER | OEC-OPS-PP-F-12 |
| 84. | OPERATING PROCEDURE FOR RAO DOCUMENT MANAGEMENT @ HDFC | OEC-OPS-DM-P-15 |
| 85. | OPERATING PROCEDURE FOR STRAPPING OF BOXES AT WAREHOUSE | OEC-OPS-SB-P-16 |
| 86. | FACILITY VISIT | OEC-OPS-FV-F02 |
| 87. | TABLE OF CONTENTS | OEC-MR-QS-M-01 |
| 88. | CHAPTER 1 - INTRODUCTION | OEC-MR-QS-M-01 |
| 89. | CHAPTER 2 - POLICY & OBJECTIVES | OEC-MR-QS-M-01 |
| 90. | CHAPTER 3 - CONTEXT OF ORGANISATION | OEC-MR-QS-M-01 |
| 91. | CHAPTER 4 - LEADERSHIP | OEC-MR-QS-M-01 |
| 92. | CHAPTER 5 - PLANNING | OEC-MR-QS-M-01 |
| 93. | CHAPTER 6 - SUPPORT | OEC-MR-QS-M-01 |
| 94. | CHAPTER 7 - OPERATION | OEC-MR-QS-M-01 |
| 95. | CHAPTER 8 - PERFORMANCE EVALUATION | OEC-MR-QS-M-01 |
| 96. | CHAPTER 9 - IMPROVEMENT | OEC-MR-QS-M-01 |
| 97. | ANNEXURE 2 | OEC-MR-QS-O-02 |
| 98. | ANNEXURE 3 | OEC-MR-QS-O-03 |
| 99. | ANNEXURE 1 | OEC-MR-QS-O-01 |
| 100. | CIF - CUSTOMER INFORMATION FORM | OEC-SAL-SP-F-01 |

| | | |
|------|--|-----------------|
| 101. | SALES POLICY AND PROCESS. | OEC-SAL-SP-P-01 |
| 102. | SECURITY SOP | OEC-SEC-00 |
| 103. | DISASTER RECOVERY PLAN | OEC-SEC-DRP-07 |
| 104. | EMERGENCY PREPAREDNESS & RESPONSE PLAN | OEC-SEC-EPRP-07 |

11.2. Security

Security department have prepared standard operating procedures with aim to protect the assets of the OEC establishments and ensure management of security operations are carried out in systematic and consistent manners during working hours, non working hours and holidays. The list of topics on SOPs have been made is attached. The training is being conducted both on the job and classrooms exercises.

The copies SOPs are maintained in respective dept. The SOPs are revised annually.

STANDARD OPERATING PROCEDURES

1. Duties
 - 1.1. Main Gate
 - 1.2. Patrolling And Inspection
 - 1.3. Routine Patrolling
 - 1.4. Security Control Room
2. Control Of Access
 - 2.1. Personal Recognition
 - 2.2. Visitor / Contractors Pass System
 - 2.3. Electronic Access Control System
 - 2.4. Employee Access
 - 2.5. Contractor's Access
 - 2.6. Visitor Access
3. Parking Of Vehicles And Vehicle Record
4. Worked And Maintenances By Contractors
5. Dispatch Of Finished Goods
6. Acceptance Of Incoming Goods
7. Search Procedures
 - 7.1. Search Procedure – Personal
 - 7.2. Search Procedure – Lockers & Belongings
 - 7.3. Refusal to be searched
 - 7.4. Search Records
 - 7.5. Finding Property
 - 7.6. Using Scanners
8. Safe Opening Procedures
9. MDT Transfers from Location to Safe
10. Waste Removal
11. Emergencies Procedure
 - 11.1. Type of Emergency
 - 11.2. Fire
 - 11.3. Forcible Attack or Intrusion
12. MDT Transportation from Site to the Safe

13. Access of Family Members and Relatives
14. Training Program for a Security Guard
15. Bomb Threat
 - 15.1. Response To The Bomb Threat During Working Hours
 - 15.2. Response During Non Working Hours
 - 15.3. Evacuation
 - 15.4. Authority To Evacuate
16. Bomb-Postal Parcel
17. Bomb Threat Over Telephone
18. Response to a Bomb Threat
19. Verbal Communication
 - 19.1. Behaviour Code
 - 19.2. Ethics Code
 - 19.3. Professional Behaviour And Responsibilities
20. Unauthorized Personnel Inside The Security Control Room
21. Entry to OEC During Non-Working Hours/Overstaying at Work
22. Employee Identification / Access Cards
23. Procedure to Answer the Telephone and to take Messages
24. Control of Company Vehicles
25. Emergency Procedures-Riots/Social Unrest, Terrorist Threat
26. Crime Prevention & Investigation
27. Workplace Violence
28. Mobile Authorization
29. Diesel Generator Operations

11.3. Information Technology