**SMART APPEX RESEARCH AND CONSULTANCY L.L.C**

**Business Continuity Plan**

**CONFIDENTIAL**

This Policy/Manual belongs to “SMART APPEX RESEARCH AND CONSULTANCY L.L.C”and is used for internal circulation. It is strictly prohibited to reproduce or copy this Manual in whole or in part without the Board's prior written approval.

**POLICY DOCUMENT REFERENCE**

|  |  |
| --- | --- |
| **ITEM** | **DESCRIPTION** |
| Document Title | Business Continuity Plan |
| Owner | Head of IT |
| Version | 1.0 |
| Approved By | The Board |
| Date Released | xxx |
| Classification (Internal/Confidential/ Private/ Public) | Internal |

**DOCUMENT VERSION CONTROL**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Name** | **Authorized By** | **Position** | **Signature** |
| 1.0 | xxx | Business Continuity Plan | The Board |  |  |

**DOCUMENT REVISION HISTORY**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Action** | **Amended By** | **Authorized By** |
| 1.0 | xxx |  |  |  |

**Authorized Signature Company Stamp**

**Table of Contents**

[HOW TO USE THIS PLAN 4](#_Toc193216108)

[1. INTRODUCTION 5](#_Toc193216109)

[**1.1 Objectives** 5](#_Toc193216110)

[**1.2 Scope** 6](#_Toc193216111)

[**1.3 Assumptions** 6](#_Toc193216112)

[**1.4 Changes to the Plan/Maintenance Responsibilities** 6](#_Toc193216113)

[2. BCP TEAM ORGANIZATION 7](#_Toc193216114)

[**2.1 Purpose and Objectives** 7](#_Toc193216115)

[**2.2 BCP Roles and Responsibilities** 7](#_Toc193216116)

[3. BUSINESS CONTINUITY STRATEGY 10](#_Toc193216117)

[**3.1 Introduction** 10](#_Toc193216118)

[**3.2 Critical Business Function Identification and Recovery** 10](#_Toc193216119)

[**3.3 Business Impact Analysis** 10](#_Toc193216120)

[**3.4 Business Recovery Strategy** 10](#_Toc193216121)

[**3.5 Relocation Strategy and Alternate Business Site** 10](#_Toc193216122)

[**3.6 Recovery Plan Phases** 10](#_Toc193216123)

[**3.7 Vital Records Backup** 11](#_Toc193216124)

[**3.8 Restoration of Hardcopy Files, Forms, and Supplies** 11](#_Toc193216125)

[**3.9 Online Access to Organization’s Computer Systems** 11](#_Toc193216126)

[4. BUSINESS CONTINUITY EVENT MANAGEMENT 11](#_Toc193216127)

[**4.1 Introduction** 11](#_Toc193216128)

[**4.2 Detection and Response** 12](#_Toc193216129)

[**4.3 Notification to Management/CMT, Preliminary Damage Assessment and Declaration Of Disaster** 12](#_Toc193216130)

[**4.4 Plan Activation** 13](#_Toc193216131)

[**4.5 Relocation to alternate site or remote working** 13](#_Toc193216132)

[**4.6 Implementation of interim procedures** 14](#_Toc193216133)

[**4.7 Establishment of connectivity and data** 14](#_Toc193216134)

[**4.8 Status reporting** 14](#_Toc193216135)

[**4.9 Deactivation** 15](#_Toc193216136)

[**4.10 BCP review and update** 15](#_Toc193216137)

[**4.11 Training and awareness** 15](#_Toc193216138)

[**4.12 Testing** 16](#_Toc193216139)

[5. RECOVERY PROCEDURES 16](#_Toc193216140)

[**5.1 Introduction** 16](#_Toc193216141)

[**5.2 Customer Service** 16](#_Toc193216142)

[**5.3 Client Onboarding** 20](#_Toc193216143)

[**5.4 Finance, Internal Audit and MIS** 23](#_Toc193216144)

[**5.5 Marketing & Sales** 25](#_Toc193216145)

[**5.6 Human Resources and Administration** 28](#_Toc193216146)

[**5.7 Legal and Compliance** 30](#_Toc193216147)

[**5.8 Business Continuity for Critical Infrastructure and its Applications** 32](#_Toc193216148)

[**5.9 Call Tree Management** 34](#_Toc193216149)

[**5.10 Desktop Computer Configurations** 34](#_Toc193216150)

[Appendix 1 35](#_Toc193216151)

# **HOW TO USE THIS PLAN**

In the event of a disaster that interferes with the Smart Appex Research and Consultancy L.L.C (“the Firm”, “Company”) ability to conduct business, this plan is to be used by the individuals responsible to coordinate the business recovery of their respective areas and/or departments. The plan is designed to contain, or provide reference to, all the information that might be needed at the time of a business recovery.

**Section I**, Introduction, contains general statements about the organization of the plan. It also establishes scope and assumptions of the Business Continuity Plan along with objectives of the business continuity plan.

**Section II**, BCP Team Organization, lists the Recovery Team functions, those individuals who are assigned specific responsibilities, and procedures on how each of the team members is to be notified.

**Section III**, Business Continuity Strategy, describes the strategy devised to identify critical business processes and high-level stages of recovery.

**Section IV**, Business Continuity Event Management, determines what activities and tasks are to be taken, in what order, and by whom to affect the recovery.

**Section V**, Recovery procedures, contains all the information needed to carry out the recovery plan for critical business processes. Other sections refer the reader to one or more Appendices to locate the information needed to carry out the Team Procedures steps.

# **INTRODUCTION**

## **Objectives**

The objective of the Business Continuity Plan is to coordinate the recovery of critical business functions in managing and supporting the business recovery in the event of facilities (office building) or business application-related disruption or disaster. This can include short or long-term disasters or other disruptions, such as fires, floods, earthquakes, explosions, terrorism, tornadoes, extended power interruptions, hazardous chemical spills, and other natural or man-made disasters.

A disaster is defined as any event that renders a business facility inoperable or unusable so that it interferes with the organization’s ability to deliver essential business services.

The priorities in a disaster situation are to:

* Ensure the safety of employees and visitors in the office buildings.
* Mitigate threats or limit the damage that threats can cause.
* Have advanced preparations to ensure that critical business functions can continue.
* Have documented plans and procedures to ensure the quick, effective execution of recovery strategies for critical business functions.
* Safeguard customer data and timely reporting to regulatory authorities.

## **Scope**

The Business Continuity Plan is limited in scope to recovery and business continuance from a serious disruption in activities due to the unavailability of the Firm’s facilities and key applications. Each business process is dependent on enablers i.e. People, Vendor, Software, Hardware, Site to achieve the business objective. The Business Continuity Plan includes procedures for all phases of recovery as defined in the Business Continuity Strategy of this document which acts as a guideline. This plan is not intended to cover major regional or national disasters such as regional earthquakes, war, or nuclear holocaust. However, the document can be it can provide some guidance in the event of such a large-scale disaster.

## **Assumptions**

The viability of this Business Continuity Plan is based on the following assumptions:

* Each business process owner shall identify and periodically update enablers required for remote working or alternate space for relocation of departments which can be occupied in case the facilities are unavailable.
* That this plan has been properly maintained and updated as required.
* The functions and roles referenced in this plan do not have to previously exist within an organization; they can be assigned to one or more individuals as new responsibilities or delegated to an external third party if funding for such services can be arranged and allocated.
* Key people listed in this document will be available in case of disaster.

## **Changes to the Plan/Maintenance Responsibilities**

Maintenance of the Firm’s Business Continuity Plan is the joint responsibility of Senior Management, and the Business Continuity Coordinator from the information security team.

**Senior management is responsible for:**

* Periodically reviewing the adequacy and appropriateness of its Business Continuity strategy.
* Assessing the impact on the Business Continuity Plan of additions or changes to existing business functions, procedures, equipment, and facilities requirements.
* Keeping recovery team personnel assignments current, considering promotions, transfers, and terminations.
* Communicating all plan changes to the Business Continuity Coordinator so that the enablers required for respective recovery plans can be updated.

**The Business Continuity Coordinator is responsible for:**

* Keeping the organization’s Recovery Plan updated with changes made to respective enablers – software, hardware, people, applications etc.
* Coordinating changes among plans and communicating to Senior management when other changes require them to update their plans.
* Maintaining and/or monitoring offsite office space or remote locations sufficient for critical functions and to meet the facility recovery time frames.
* Communicating changes to business continuity plans to respective IT teams and functional recovery teams.

# **BCP TEAM ORGANIZATION**

## **Purpose and Objectives**

This section of the plan identifies who will participate in the recovery process for the Business Continuity Plan. The Operations Manager will drive the recovery process along with the BCP coordinator.

* 1. **BCP Roles and Responsibilities**

**Business Continuity Coordinator:**

In the event of a disaster, the Business Continuity Coordinator is responsible for ensuring that the following activities are successfully completed:

* Works with the Crisis Management Team (CMT)/Senior Management to officially declare a disaster and start the Disaster Recovery/Business Continuation process to recover organization’s business functions at an alternate site.
* Alert Senior Management that a disaster has been declared.
* Assist in the development of an official public statement if required concerning the disaster. The Operations Manager is the only individual authorized to make public statements about organizational affairs.
* Monitor the progress of all Business Continuity and Disaster Recovery teams daily.
* Present Business Continuity Plan recovery status reports to Senior Management daily.
* Interface with appropriate work management personnel throughout the recovery process.
* Communicate directions received from CMT to the other team members.
* Provide on-going support and guidance to the Business Continuity teams and personnel.
* Review staff availability and recommend alternative assignments, if necessary.
* Work with CMT to authorize the use of the alternate recovery site selected for re-deploying critical resources.
* Review and report critical processing schedules and backlog work progress, daily.
* Ensure that a record of all Business Continuity and Disaster Recovery activity and expenses incurred is maintained.

**Crisis Management Team or Senior Management**

The Crisis Management Team (CMT) is the group of Senior Management team members, which commands the resources needed to recover operations in the event of a BCP incident. Depending on the level of disaster and the premises affected, the CMT will operate from one of the premises at an alternate site or remotely to be decided at the time of the incident.

Key responsibilities include:

* Oversee implementation of business continuity planning implementations across the organization.
* Review & approve budgets for Business continuity objectives.
* Approve Recovery Drills and Tests
* Declares ‘Disaster’ for the Smart Appex Research and Consultancy L.L.C.
* Determines the appropriate course of action in the event of a major service interruption.
* Provides forward planning for returning to business as usual after the crisis has been resolved.
* Makes major financial and policy decisions during an extended business interruption.

|  |  |
| --- | --- |
| **Role/ Title** | **Name** |
| Operations Manager |  |
| Chief Financial Officer |  |
| Marketing Manager |  |
| Chief Investment Officer |  |
| Operations Admin |  |
| IT Manager | Blesy |
| Chief Compliance Officer |  |
| Chief Risk Officer |  |

**Crisis Communication Team**

This team is responsible for providing information regarding the disaster and recovery efforts to:

* Customers
* Vendors/Contracts
* Media
* Regulatory Agencies
* Other Stakeholders
* Employees and their families

The Crisis Communication Team shall consist of the human resources team.

**Operations Recovery Teams (ORT)**

This team consists of key members of the critical business processes responsible for:

* Enabling and implementing recovery strategy once BCP is invoked.
* Communication of BCP within the teams
* Notifying support teams such as administrators and IT teams regarding Business Continuity preparedness

**Departmental Recovery Teams**

|  |  |
| --- | --- |
| **Department/Position** | **Name** |
| Operations Manager |  |
| Marketing Manager |  |
| IT Manager | Blesy |
| Chief Compliance Officer |  |
| Operations Admin |  |
|  |  |
|  |  |

**Recovery Support Teams (RST) – Administration**

This team is responsible for:

* Providing Senior management with damage assessment reports and recommendations.
* Inspecting the physical structure and identifying areas that may have sustained damage.
* Ensuring the recovery/restoration personnel has assistance with clerical tasks, errands, and other administrative activities.
* Arranging for the availability of necessary office support services and equipment.
* Arranging travel for employees wherever required
* Tracking all costs related to the recovery and restoration effort.
* Identifying and documenting when repairs can begin and obtaining cost estimates.
* Determining where forms and supplies should be delivered, based on damage to the normal storage areas for the materials.
* Contacting vendors to schedule specific start dates for the repairs.
* Taking appropriate actions to safeguard equipment from further damage or deterioration.
* Coordinating the removal, shipment, and safe storage of all furniture, documentation, supplies, and other materials as necessary.
* Supervise all salvage and cleanup activities.
* Coordinating required departmental relocations to the recovery sites.
* Coordinating relocation to the permanent site after repairs are made.
* Assuring that arrangements are made for meals and temporary facilities, when required, for all recovery personnel.
* Assuring order placement for consumable materials (forms, supplies, etc.) for processing based upon input from the other teams.

**Recovery Support Teams (RST) - Information Technology Recovery Team**

This team is responsible for:

* Activating the IT Technology Recovery Plan
* Managing the IT disaster response and recovery procedures.
* Mobilizing and managing IT resources.
* Coordinating all communications related activities, as required, with telephone & data communications, PC, LAN support personnel, and other IT related vendors.
* Assisting, as required, in the acquisition and installation of equipment at the recovery site or remote sites.
* Ensuring that cellular telephones, and other special-order equipment and supplies are delivered to teams as requested.
* Participating in testing equipment and facilities.
* Coordinating and performing restoration or replacement of all desktop PCs, LANs, telephones, and telecommunications access at the damaged site.
* Coordinating Disaster Recovery/IT efforts between different departments in the same or remote locations.
* Training Disaster Recovery/IT Team Members.
* Keeping Senior Management and the Business Continuity Coordinator appraised of recovery status.

# **BUSINESS CONTINUITY STRATEGY**

## **Introduction**

This section of the Business Continuity Plan describes the strategy devised to identify critical business processes and the phases of recovery in case of a disruption.

## **Critical Business Function Identification and Recovery**

The recovery of critical business functions and processes shall be prioritized as per recovery time objectives in case of disruption or disaster.

The BCP team, consisting of the Director of Operations and the BCP Coordinator, are responsible for allocating sufficient resources to BCP development and ensuring BCP is kept up to date. This BCP shall be updated at least annually.

## **Business Impact Analysis**

The Business continuity coordinator is responsible for coordinating with department heads to conduct business impact analysis as per the information security policy requirements.

Business impact analysis shall be conducted to identify the key enablers for each business process and identify the recovery time objectives of the business process.

The recovery time objectives shall be finalized with Senior management & various stakeholders and shall be the basis for defining recovery strategies.

Based on the recovery time objectives, processes shall be determined to be critical and shall be prioritized in case of disruption.

Critical business functions for the purpose of this strategy shall mean critical operational or support activities without which the business would rapidly be unable to achieve its objectives”. These individual processes must be given preferential access to premises, staff, equipment, or records if an emergency restricted their overall availability.

## **Business Recovery Strategy**

Business continuity coordinator is responsible for coordinating with department heads to document recovery strategies which align with recovery time objectives defined for critical business processes.

## **Relocation Strategy and Alternate Business Site**

In the event of a disaster or disruption to the office facilities, the strategy is to recover operations by relocating to an alternate business site. The organization’s short-term strategies (for disruptions lasting two weeks or less) include working from home.

## **Recovery Plan Phases**

The activities necessary to recover from the disaster or disruption will be divided into four phases. These phases will follow each other sequentially in time.

* **Disaster Occurrence**

This phase begins with the occurrence of the disaster event and continues until a decision is made to activate the recovery plans. The major activities that take place in this phase include emergency response measures, notification of management, damage assessment activities, and declaration of the disaster.

* **Plan Activation**

In this phase, the Business Continuity Plans are put into effect. This phase continues until the alternate facility is occupied or critical business functions restored, and services restored as per requirement of critical business processes. The major activities in this phase include notification and assembly of the recovery teams, implementation of interim procedures, and relocation to the secondary facility/backup site, and re- establishment of services.

* **Alternate Site Operations**

This phase begins after alternate facility operations are established and continues until the primary facility is restored. The primary recovery activities during this phase are backlog reduction and alternate facility processing procedures.

* **Deactivation**

This phase consists of all activities necessary to make the transition back to a primary facility location and to deactivate BCP.

## **Vital Records Backup**

All vital records for the organization are maintained and controlled by either the Director of Operations or Senior IT Manager or any designated person who can assist in Disaster Recovery/IT Plan. Some of these files are periodically backed up and stored at an offsite location as part of normal operations.

When organization requires on-site file rooms, scanning, and organization offsite storage locations, best practices advise engaging any near-by secure site for vital records and data back-up. All vital documents are typically located in files within the office complex and the most current back-up copies are in a secure off-site storage facility.

## **Restoration of Hardcopy Files, Forms, and Supplies**

In the event of facilities disruption, critical records located in the Firm may be destroyed or inaccessible. In this case, the last backup of critical records in the secure warehouse would be transported to the secondary facility. The number of critical records, which would have to be reconstructed, will depend on when the last shipment of critical records to the offsite storage location occurred. Wherever feasible, the BCP Coordinator shall enforce storage of copies of electronic data on the cloud. This cloud storage shall be made accessible to key personnel in the event of a disaster or disruption.

BCP coordinator will arrange the frequency of rotation of critical records to the offsite storage site.

The following categories of information can be exposed to loss:

1. Any files stored on-site in file cabinets and control file rooms.
2. Information stored on local PC hard drives.
3. Documents in offices, work cubes and files.
4. Off-site records

## **Online Access to Organization’s Computer Systems**

In the event of facilities disruption, the recovery plan strategy should be to assist in re-establishing connectivity to the organization’s departments and to establish remote communications to any alternate business site location. Key personnel shall be provided with remote access to computer systems along with laptops and access to data wherever required.

# **BUSINESS CONTINUITY EVENT MANAGEMENT**

## **Introduction**

The essential feature of a BCP event is resources such as equipment, data, premises, people etc. become unavailable, thus seriously hampering continuity of business processes. The intensity of a BCP event is thus a function of which or how many of the critical business processes and resources are no longer available to the business. To help the planners and the Function Heads to formulate appropriate strategy, the analysis of possible BCP events was classified into four levels of intensity.

**Level I:**

Significant malfunction of / disruption of critical infrastructure supporting critical business process of a function. It is assumed that the usual office premises and people are available to the business.

**Level II**:

Significant malfunction of / or disruption to highly critical infrastructure, supporting operations across different functions. The level II BCP events also include the unavailability of people to perform one or more critical business process of a function. It is assumed that premises to perform the critical business processes are available.

**Level III:**

Unavailability of premises or Destruction of the building or total loss of the services within a building, requiring relocation or significant renovation of the facility or remote working, because of fire, building collapse, bomb explosions or any other disruptions etc. It is assumed that premises and equipment are inaccessible, but people can relocate to an alternate DR site elsewhere if required.

**Level IV:**

The employees are unable to reach offices or alternate office facilities due to riots, floods, or another major citywide catastrophe.

It may be appropriate to mention that in real life situations, the BCP event may not always strictly follow the classification mentioned above; this classification helps simplify how one addresses a certain BCP event.

## **Detection and Response**

**Tasks**:

If any of the employees suspects that there is a potential or actual BCP event in progress, first inform the human resources (HR) team or administration (admin) team:

* HR / Admin will inform the appropriate emergency services depending on the type of incident depending on the initial assessment.
* HR/Admin teams quickly assess the damage whether an emergency response is required which may include evacuation of building or not, depending upon the nature of the disaster, the extent of damage, and the potential for additional danger. Notify government/emergency authorities as required.
* In case of evacuation required, recovery support teams and department recovery teams shall be notified via messengers and public address systems to evacuate.
* Quickly assess whether any personnel in your surrounding area are injured and need medical attention. If able to assist them without causing further injury or without putting oneself in further danger, then provide what assistance you can and call for help. If further danger is imminent, then immediately evacuate the building.
* If appropriate, evacuate the building in accordance with your building’s emergency evacuation procedures.
* Assembly point as the Emaar Square building 4 assembly point
* Ensure that all employees are accounted for.

## **Notification to Management/CMT, Preliminary Damage Assessment and Declaration Of Disaster**

**Tasks**:

* HR/Admin teams shall notify Crisis Management Team/Senior Management regarding the BCP incident along with preliminary information regarding the incident.
* CMT shall assess the BCP incident and may request HR/Admin/BCP Coordinator to perform damage assessment.
* Based on the damage assessment, Estimate extent of the situation and extent of disruption to the business.
* Based on the intensity of BCP event, the initial report of the Damage Assessment Team (DAT) and the expected time to recover normal operations, the CMT shall meet, analyze facts, intensity of the event and declare a disaster.
* CMT shall notify the BCP coordinator to invoke the Business Continuity Plan. BCP coordinator shall notify the Crisis Communication Team.
* A preliminary announcement is used to communicate, responsively and accurately, to Smart Appex employees immediately following the disruption.
* The Crisis Communication Team shall send the preliminary announcement to employees via messenger or email as required.
* Depending upon the time of the disaster, personnel are instructed what to do (i.e., stay at home and wait to be notified again, etc.)

## **Plan Activation**

**Tasks:**

* Inform the members of the Recovery Support Team (RST). Send the utility and IT support team to the affected location. Inform employees of remote working or alternate business recovery site to be prepared to recover the operations.
* Notify Operations Recovery Team (ORT) coordinators to report at assembly point or BCP Conference Bridge for briefing. Instruct the team leaders to inform team members.
* Provide a short briefing to the ORT coordinators which covers what has happened, damage assessment status and the strategy agreed and approved by the CMT.
* Commence operations recovery procedures.
* Identify the alternative site for the business functions to recover the operations if required or inform employees of remote work arrangements.
* Arrange for the transport of off-site storage material and backup tapes to the business recovery site, if required.
* Arrange call with ORT. They should be provided with the following information:
* Brief overview of the situation
* Give the address of the reporting place and time of reporting.
* Ask them to arrange to inform other members of the business function, to report / not to report.
* Instruct ORT members not to answer any questions from the media and refer it instead to the CMT members.
* Inform the technical team to forward all fixed line calls to new numbers as required.
* The Crisis Communication Team would play a crucial role in providing information proactively to employees, customers, and the public at large. All employees should be advised to call the help desk rather than operational staff or CMT members for the information.
* The Crisis Communication Team should help in deciding the contents of the message to be given to customers, press and public at large during the crisis and later. For this purpose, it would need to work in close contact with CMT.
* Communicate with customers, government authorities, utility organizations, vendors and communicate with BCP activity in the direction of the CMT.

## **Relocation to alternate site or remote working**

**Tasks:**

* When instructed by the Crisis Management Team, plan to commute or travel to the alternate site. The initial plan for the team would be to work from home. Senior Management will decide if the staff should work from home or from an alternate site depending on the nature and extent of damage.
* Senior Management needs to consult with the respective recovery support teams to determine if access can be gained to the primary (damaged) site to retrieve vital records and other materials.
* If allowed access to the primary site to retrieve vital records and other materials, perform some pre- planning to determine what is most important to retrieve. This may be necessary since the time you may be allowed access to the primary site may be minimal.
* Depending on the number of vital records and other materials you can retrieve from the primary site, plan to transport this material to the alternate site.
* Management and critical employees travel to alternate sites.

## **Implementation of interim procedures**

**Tasks**:

* Where the extent of damage requires staff to work from alternate sites or remote work, the procedures below will apply.
* After arrival at the alternate site, map out locations that can be used for workspace.
* Obtain additional tables and chairs, either from the office or from outside rental agencies to provide additional workspace.
* For remote work, ensure access to vital records, email, cloud storage and messenger communications between employees and remote access to applications.
* Determine flexible working schedules for staff to ensure that client and business needs are met, but also to enable effective use of space.
* Gather vital records and other materials that were retrieved from the primary site and determine appropriate storage locations, keeping in mind effectiveness of workgroups.

## **Establishment of connectivity and data**

**Tasks:**

* The IT Team shall reroute telephone communications and data traffic to the alternate site as required.
* Identify phone numbers to which the customer care numbers are to be redirected to.
* Redirect data communications and restore backups as required.
* Setup IT helpdesk for remote support as required.
* Provide privileged access to applications as required.

## **Status reporting**

**Tasks:**

CMT shall be in contact with the recovery teams via the BCP Coordinator for the following:

* Progress against Critical Timeframes.
* Schedule of subsequent actions.
* Assess known losses and damage and update the Initial Damage Assessment.
* Assess the morale of staff.
* Assess the adequacy of the site and necessary proximity to other teams.
* Assess the availability and performance of systems and telecom equipment.
* Identify current and anticipated resource needs. Contact the Help Desk to determine resource and service availability.
* Identify and prioritize future team activities.
* Assess current and anticipated problem areas.
* Release copies of the latest CMT statements to staff and third parties.
* Establish overall recovery progress.
* Review and adjust the Recovery Strategy.
* Work with the Alternate Site coordinators to control resource allocation.

1. Determine priorities for work backlogs to ensure the most critical backlogged tasks are resolved first. Report on the backlog status to Senior management regularly.
2. Liaise with the Operations Recovery Team Co-Ordinator’s to begin developing a long-term recovery plan. Convene a CMT meeting to confirm and communicate recovery objectives and strategies updates.
3. Assess recovery expenditure outlay to date and finalize Recovery action.

## **Deactivation**

**Tasks:**

* The CMT shall define the BCP's deactivation based on the reports by the ORT and RST teams.
* The BCP coordinator shall coordinate with the IT Team to determine when the organization will return to the primary site. Verify they have a schedule to ensure that telephone and data communications are rerouted accordingly.
* Discuss when and how PCs, terminals, and printers, if brought into the alternate site, will be de-installed, moved back to the primary site, and re-installed.
* Determine how remote working will be disabled as required for critical applications.
* Determine which alternate site operating procedures will be suspended or discontinued and when.
* Communicate the changes in procedures to all affected staff.
* Inventory vital records, equipment, supplies, and other materials, which need to be transported from the alternate site to the primary site.
* Stakeholders, including clients, regulatory authorities, and business partners, are notified of the BCP's deactivation and the resumption of regular business activities.

## **BCP review and update**

**Tasks:**

* This plan is intended to be a living document and as such must be reviewed regularly. The plan will be reviewed annually and updated in the event of major change in organization structure or scope statement. The test may be in the form of a walk-through, mock drill, or component testing.
* The plan will be stored in a shared location where it can be viewed by system site personnel and all the teams.
* The BCP coordinator initiates a review of the entire BCP to incorporate any lessons learned from the recent event and ensure that it remains current and effective.
* A review of the recovery efforts undertaken during the activation of the BCP is conducted to assess their effectiveness and identify any lessons learned or areas for improvement. Feedback from employees and stakeholders may be solicited to inform future planning efforts.
* A formal debriefing session may be conducted with key stakeholders to discuss lessons learned from the event and identify opportunities for continuous improvement.

## **Training and awareness**

**Tasks**:

* Training and testing strengthen the team’s readiness to manage any major incident /disaster. Training shall be used to generate BCP awareness among stakeholders and drill shall be used to imbibe BCP/DR culture in day-to-day operations. Periodic training and drills shall also monitor
* The Firm will take measures as appropriate to ensure that its employees/staff are all aware of the firm’s BCP procedures. These measures may include:
* Ensuring all employees are aware of the building evacuation procedures.
* Participating in periodic mock fire drills.
* Regular testing of the BCP.
* Ensuring all employees are aware of/ have access to the following information:
* Staff Emergency Contacts.
* How they will be contacted in and out of working hours.
* Applicable contingency arrangements agreed; and
* Feedback from any previous BCP tests.

## **Testing**

**Tasks**:

* The BCP Coordinator, headed by the Operations Manager, is responsible for ensuring testing and ongoing review of the BCP. The BCP will be tested annually in addition to any ad-hoc testing that may be performed as and when required.
* BCP test scenarios shall be defined prior to the tests and shall include fire drills, site unavailability,
* The results should clearly indicate whether the test has been successful or not. Lessons learnt from the test results are to be documented and BCP Team should be educated. A knowledge base of lessons learnt should be created. The results of the test conducted for each of the test cases are documented and signed by BCP Team Leader.

# **RECOVERY PROCEDURES**

## **Introduction**

This section of the Business Continuity Plan describes the information needed to carry out the recovery plan for critical business processes and critical IT infrastructure.

## **Customer Service**

To ensure the recovery of critical Customer Service (CS) processes within the desired recovery time objectives and ensure continuity of processes to the required minimum level.

**Recovery Team Composition**

|  |  |
| --- | --- |
| **Primary Team Member(s)** | **Fallback Team Members** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Minimum Operating Requirements**

|  |  |
| --- | --- |
| **Requirements** | **Details** |
| Team Members | 6 (2-night shift) |
| Desks | 6 |
| Laptops/Desktops | 10 |
| Internet Connectivity | Yes |
| Access to Office Network | Yes |
| Access to desk phones/Company landlines | Yes |
| Remote Access to One Drive | Yes |
| Key Applications – |  |

**Alternate site requirements**

| **Location** | **Alternate Site** |
| --- | --- |
| Primary Location - | |
| Within City – Alternation site |  |
| Within City – if both primary and alternate site are unavailable |  |
| Outside region |  |

**Pre Crisis-Preparation**

| **Action Steps** | **Responsibility** | |
| --- | --- | --- |
|  | **Dept** | **Person(s)** |
| Laptops to be provided to key resources within the team with access to VPN to access key applications remotely | IT | Seyad |
| Customer Services files and data to be stored on one drive shared team folder and to be made accessible on the team via VPN/Internet | Customer Services | Shilpa |
| Calls on Customer contact numbers to be routed to mobile phones and Cisco Jaber to be installed on key resources mobile phones. Adequate licenses to be procured and provided to resources | IT | Susmitha |
| Applications – Skale, Fynxt and Metaquotes to be accessible via Internet/VPN | IT | Susmitha |
| Train resources from India region and onboarding team regarding customer support processes | Customer Services | Shilpa |
| DR and High availability infrastructure setup for key applications - Metaquotes | IT | Seyad |

**Business Recovery and Resumption**

|  |  |  |  |
| --- | --- | --- | --- |
| **Action Steps** | **Responsibility** | | **Remarks** |
|  | **Dept** | **Person(s)** |  |
| **Site** | | | |
| Relocate the Customer Support Team to alternate facility for Customer Services Process. Alternate facility to be defined based on extent of disruption. | Customer Services | Shilpa | None |
| Deliver the process from alternate facility and ensure continuity as per the defined Recovery Time Objective (RTO). | Customer Services | Shilpa | None |
| **People** | | | |
| Customer Services  In case of unavailability of customer services team, the resources from onboarding team to support with the customer support services. | Customer Services | Shilpa | None |
| Instruct the vendor /backup resources from India region to take over the process. | Customer Services | Shilpa | None |

**Post Recovery / Restoration and Return**

| **Action Steps** | **Responsibility** | | **Remarks** |
| --- | --- | --- | --- |
|  | **Dept** | **Person(s)** |  |
| **Site** | | | |
| Inform the Customer Services Team about restoration of main site and instruct to relocate to main site. | IT | Susmitha | None |
| **People** | | | |
| Inform the other team managing the customer services about the availability of the team. | Customer Services | Shilpa | None |
| Handover the process to main team | Customer Services | Shilpa | None |
| **Technology** | | | |
| Inform the Customer Support Team about restoration of IT applications. | IT | Seyad | None |

**Vital Records**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vital Record Description** | **Location of Vital Record** | **Media Type** | **Responsibility** | **Contact Details** |
| Customer data stored in One drive and CRMs. | One Drive | Softcopy | Customer Services | - |
| **Alternate Recovery Strategies for Vital Records** | | | |
| * Regular backup of One Drive to be taken by IT Team | | | |

**Vendor / Outsourced Agencies Contact Details**

| **Vendor / Outsourced Agency** | **Contact Person** | **Contact Details and Address** |
| --- | --- | --- |
| CRM vendors |  |  |
| XXXXX |  |  |

## **Client Onboarding**

To ensure the recovery of critical Client Onboarding processes within the desired recovery time objectives and ensure continuity of processes to the required minimum level.

**Recovery Team Composition**

|  |  |
| --- | --- |
| **Primary Team Member(s)** | **Fallback Team Members** |
|  |  |
|  |  |
|  |  |
|  |  |

**Minimum Operating Requirements**

|  |  |
| --- | --- |
| **Requirements** | **Details** |
| Team Members |  |
| Desks |  |
| Laptops/Desktops |  |
| Internet Connectivity |  |
| Access to Office Network |  |
| Access to desk phones/Company landlines |  |
| Remote Access to One Drive |  |
| Key Applications – |  |

**Pre Crisis-Preparation**

| **Action Steps** | **Responsibility** | |
| --- | --- | --- |
|  | **Dept** | **Person(s)** |
| Laptops to be provided to key resources within the team with access to VPN to access key applications remotely | IT | Seyad |
| Client Onboarding files and data to be stored on one drive shared team folder and to be made accessible on the team via VPN/Internet | Client Onboarding | Shilpa |
| Applications – Skale, Fynxt and sumsub/worldcheck, Upro to be accessible via Internet/VPN | IT | Susmitha |
| Identify and train resources from India region regarding onboarding processes | Client Onboarding | Shilpa |
| DR and High availability infrastructure setup for key applications – Upro CRM, Fynxt, Skale | IT | Seyad |

**Business Recovery and Resumption**

|  |  |  |  |
| --- | --- | --- | --- |
| **Action Steps** | **Responsibility** | | **Remarks** |
|  | **Dept** | **Person(s)** |  |
| **Site** | | | |
| Relocate the Client Onboarding Team to alternate facility for Client Onboarding Process. Alternate facility to be defined based on extent of disruption. | Client Onboarding | Shilpa | None |
| Deliver the process from alternate facility and ensure continuity as per the defined Recovery Time Objective (RTO). | Client Onboarding | Shilpa | None |
| **People** | | | |
| In case of unavailability of client onboarding team, the resources from Backoffice India team to support with the client onboarding process. | Client Onboarding | Shilpa | None |
| **Technology** | | | |
| In case of unavailability of CRM- Maintain manual list of clients which have been approved and update on MetaQuotes or Principal platform from backend. | Client Onboarding | Shilpa | None |
| In case of unavailability of client portals, share manual forms with clients via email for individual, joint and corporate accounts. Additionally, perform worldcheck manually. Account creation shall be done manually on email approvals from respective parties | Client Onboarding | Shilpa | None |
| In case of unavailability of Internet in premises – access Internet over 5G dongles | Client Onboarding | Shilpa | None |
| In case of VPN unavailability, provide access to cloud VPN to access Upro CRM | IT | Susmitha | None |

**Post Recovery / Restoration and Return**

| **Action Steps** | **Responsibility** | | **Remarks** |
| --- | --- | --- | --- |
|  | **Dept** | **Person(s)** |  |
| **Site** | | | |
| Inform the Client Onboarding about restoration of main site and instruct to relocate to main site. | IT | Susmtiha | None |
| **People** | | | |
| Inform the other team managing the Client Onboarding about the availability of the team. | Client Onboarding | Shilpa | None |
| Handover the process to main team | Client Onboarding | Shilpa | None |
| **Technology** | | | |
| Inform the Client Onboarding about restoration of IT applications. | IT | Seyad | None |
| Inform Clients, Relationship Managers about the restoration of process | Client Onboarding | Shilpa | None |

**Vital Records**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vital Record Description** | **Location of Vital Record** | **Media Type** | **Responsibility** | **Contact Details** |
| Customer data stored in One drive and CRMs. | One Drive | Softcopy | Client Onboarding | - |
| **Alternate Recovery Strategies for Vital Records** | | | |
| * Regular backup of One Drive to be taken by IT Team | | | |

**Vendor / Outsourced Agencies Contact Details**

| **Vendor / Outsourced Agency** | **Contact Person** | **Contact Details and Address** |
| --- | --- | --- |
| CRM vendors |  |  |
|  |  |  |

## **Finance, Internal Audit and MIS**

To ensure the recovery of critical Finance, Internal Audit and MIS (Management Information System) processes within the desired recovery time objectives and ensure continuity of processes to the required minimum level.

**Recovery Team Composition**

|  |  |
| --- | --- |
| **Primary Team Member(s)** | **Fallback Team Members** |
|  |  |
|  |  |
|  |  |
|  |  |

**Minimum Operating Requirements**

|  |  |
| --- | --- |
| **Requirements** | **Details** |
| Team Members |  |
| Desks |  |
| Laptops/Desktops |  |
| Internet Connectivity |  |
| Access to Office Network |  |
| Access to desk phones/Company landlines |  |
| Remote Access to One Drive |  |
| Key Applications – |  |

**Pre Crisis-Preparation**

| **Action Steps** | **Responsibility** | |
| --- | --- | --- |
|  | **Dept** | **Person(s)** |
| Laptops to be provided to key resources within the team with access to VPN to access key applications remotely | IT | Seyad |
| Client Relations and Research reports, files, and data to be stored on one drive shared team folder and to be made accessible on the team via VPN/Internet | Sales | Shilpa |
| Applications access to be accessible via Internet/VPN | IT | Susmitha |

**Business Recovery and Resumption**

|  |  |  |  |
| --- | --- | --- | --- |
| **Action Steps** | **Responsibility** | | **Remarks** |
|  | **Dept** | **Person(s)** |  |
| **Site** | | | |
| Remote working for all client relations and research teams in case of site unavailability | Client Relations | Blesy | None |
| **People** | | | |
| Client relations backups to be identified wherever possible. | Client Relations | Blesy | None |
| **Technology** | | | |
| In case of unavailability of desk phones, utilize mobile phones as required | Sales | Shilpa | None |
| In case of unavailability of Internet in premises – access Internet over 5G dongles | Sales | Shilpa | None |
| In case of VPN unavailability, provide access to cloud VPN to access systems | IT | Seyad | None |

**Post Recovery / Restoration and Return**

| **Action Steps** | **Responsibility** | | **Remarks** |
| --- | --- | --- | --- |
|  | **Dept** | **Person(s)** |  |
| **Site** | | | |
| Inform the Client relations and research team about restoration of main site and instruct to relocate to main site. | IT | Seyad | None |
| **Technology** | | | |
| Inform the Client relations about restoration of IT applications. | IT | Susmitha | None |

**Vital Records**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vital Record Description** | **Location of Vital Record** | **Media Type** | **Responsibility** | **Contact Details** |
| Research reports. | One Drive | Softcopy | Client Relations and Research | - |
| **Alternate Recovery Strategies for Vital Records** | | | |
| * Regular backup of One Drive to be taken by IT Team | | | |

## **Marketing & Sales**

To ensure the recovery of critical Marketing & Sales processes within the desired recovery time objectives and ensure continuity of processes to the required minimum level.

**Recovery Team Composition**

|  |  |
| --- | --- |
| **Primary Team Member(s)** | **Fallback Team Members** |
|  |  |
|  |  |
|  |  |
|  |  |

**Minimum Operating Requirements**

|  |  |
| --- | --- |
| **Requirements** | **Details** |
| Team Members |  |
| Desks |  |
| Laptops/Desktops |  |
| Internet Connectivity |  |
| Access to Office Network |  |
| Access to desk phones/Company landlines |  |
| Remote Access to One Drive |  |
| Key Applications – |  |

**Pre Crisis-Preparation**

| **Action Steps** | **Responsibility** | |
| --- | --- | --- |
|  | **Dept** | **Person(s)** |
| Laptops to be provided to key resources within the team with access to VPN to access key applications remotely | IT | Seyad |
| Marketing materials to be stored on one drive/hard drives and to be made accessible on the team | Marketing |  |
| Access to marketing accounts to be provided to multiple stakeholders | Marketing |  |

**Business Recovery and Resumption**

|  |  |  |  |
| --- | --- | --- | --- |
| **Action Steps** | **Responsibility** | | **Remarks** |
|  | **Dept** | **Person(s)** |  |
| **Site** | | | |
| Relocate the Marketing to remote location | Marketing |  | None |
| **People** | | | |
| In case of unavailability of personnel, identify secondary resources and additional third-party resources as and when required. | Marketing |  | None |
| **Technology** | | | |
| In case of unavailability of Internet in premises – access Internet over 5G dongles | IT | Susmitha | None |
| In case of VPN unavailability, provide access to cloud VPN to access design desktops | IT | Blesy | None |

**Post Recovery / Restoration and Return**

| **Action Steps** | **Responsibility** | | **Remarks** |
| --- | --- | --- | --- |
|  | **Dept** | **Person(s)** |  |
| **Site** | | | |
| Inform the Marketing Teams about restoration of main site and instruct to relocate to main site. | IT | Blesy | None |
| **Technology** | | | |
| Inform the Marketing teams about restoration of IT applications. | IT | Seyad | None |

**Vital Records**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vital Record Description** | **Location of Vital Record** | **Media Type** | **Responsibility** | **Contact Details** |
| Marketing spends and creatives. | One Drive | Softcopy | Marketing Team | - |
| **Alternate Recovery Strategies for Vital Records** | | | |
| * Regular backup of One Drive to be taken by IT Team | | | |

## **Human Resources and Administration**

To ensure the recovery of critical Human Resources and Administration processes within the desired recovery time objectives and ensure continuity of processes to the required minimum level.

**Recovery Team Composition**

|  |  |
| --- | --- |
| **Primary Team Member(s)** | **Fallback Team Members** |
|  |  |
|  |  |
|  |  |
|  |  |

**Minimum Operating Requirements**

|  |  |
| --- | --- |
| **Requirements** | **Details** |
| Team Members |  |
| Desks |  |
| Laptops/Desktops |  |
| Internet Connectivity |  |
| Access to Office Network |  |
| Access to desk phones/Company landlines |  |
| Remote Access to One Drive |  |
| Key Applications – |  |

**Pre Crisis-Preparation**

| **Action Steps** | **Responsibility** | |
| --- | --- | --- |
|  | **Dept** | **Person(s)** |
| Laptops to be provided to key resources within the team with access to VPN to access key applications remotely | IT | Seyad |
| HR documentation to be stored on one drive/hard drives and to be made accessible on the team | Human Resources | Blesy |
| Access to UPro to be provided via VPN | IT | Susmitha |
| Identify emergency response personnel for facility and the keep emergency contact numbers handy along with contact points for insurance agencies | Administration |  |
| List of key building management contacts and their agreements | Administration |  |
| Periodic checks of fire systems and site CCTV systems | Administration |  |
| Train select employees with emergency drills, firefighting equipment | Administration |  |

**Business Recovery and Resumption**

|  |  |  |  |
| --- | --- | --- | --- |
| **Action Steps** | **Responsibility** | | **Remarks** |
|  | **Dept** | **Person(s)** |  |
| **Site** | | | |
| Relocate the HR and Admin to remote location or alternate location | HR |  | None |
| **People** | | | |
| In case of unavailability of personnel, identify secondary resources and additional resources as part of the accounts/India back-office team as and when required. | HR |  | None |
| **Technology** | | | |
| In case of unavailability of Internet in premises – access Internet over 5G dongles | IT | Susmitha | None |
| In case of VPN unavailability, provide access to cloud VPN to access Upro data | IT | Seyad | None |

**Post Recovery / Restoration and Return**

| **Action Steps** | **Responsibility** | | **Remarks** |
| --- | --- | --- | --- |
|  | **Dept** | **Person(s)** |  |
| **Site** | | | |
| Inform the HR and Admin teams about restoration of main site and instruct to relocate to main site. | IT | Blesy | None |
| **Technology** | | | |
| Inform the HR teams about restoration of IT applications. | IT | Susmitha | None |

**Vital Records**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vital Record Description** | **Location of Vital Record** | **Media Type** | **Responsibility** | **Contact Details** |
| Employee data and Site related data | One Drive | Softcopy | Human Resource Team | - |
| **Alternate Recovery Strategies for Vital Records** | | | |
| * Regular backup of One Drive to be taken by IT Team | | | |

## **Legal and Compliance**

To ensure the recovery of critical Legal and Compliance processes within the desired recovery time objectives and ensure continuity of processes to the required minimum level.

**Recovery Team Composition**

|  |  |
| --- | --- |
| **Primary Team Member(s)** | **Fallback Team Members** |
|  |  |
|  |  |

**Minimum Operating Requirements**

|  |  |
| --- | --- |
| **Requirements** | **Details** |
| Team Members |  |
| Desks |  |
| Laptops/Desktops |  |
| Internet Connectivity |  |
| Access to Office Network |  |
| Access to desk phones/Company landlines |  |
| Remote Access to One Drive |  |
| Key Applications – |  |

**Alternate site requirements**

| **Location** | **Alternate Site** |
| --- | --- |
| Primary Location - | |
| Within City – Alternation site |  |

**Pre Crisis-Preparation**

| **Action Steps** | **Responsibility** | |
| --- | --- | --- |
|  | **Dept** | **Person(s)** |
| Laptops to be provided to key resources within the team with access to VPN to access key applications remotely | IT | Seyad |
| Compliance files and data to be stored on one drive shared team folder and to be made accessible on the team via VPN/Internet | Compliance | Shilpa |
| Applications – Skale, Fynxt and sumsub/worldcheck, Upro to be accessible via Internet/VPN | IT | Susmitha |
| DR and High availability infrastructure setup for key applications – Upro CRM, Fynxt, Skale, Digicomply | IT | Seyad |

**Business Recovery and Resumption**

|  |  |  |  |
| --- | --- | --- | --- |
| **Action Steps** | **Responsibility** | | **Remarks** |
|  | **Dept** | **Person(s)** |  |
| **Site** | | | |
| Relocate the Legal and Compliance to alternate facility. Alternate facility to be defined based on extent of disruption. | Compliance |  | None |
| Deliver the process from alternate facility and ensure continuity as per the defined Recovery Time Objective (RTO). | Compliance |  | None |
| **Technology** | | | |
| In case of unavailability of CRM- Maintain manual list of clients which have been approved and update on MetaQuotes or Principal platform from backend. | Compliance | Susmitha | None |
| In case of VPN unavailability, provide access to cloud VPN to access systems – Digi comply, worldcheck | IT | Seyad | None |

**Post Recovery / Restoration and Return**

| **Action Steps** | **Responsibility** | | **Remarks** |
| --- | --- | --- | --- |
|  | **Dept** | **Person(s)** |  |
| **Site** | | | |
| Inform the Legal and Compliance about restoration of main site and instruct to relocate to main site. | IT | Blesy | None |
| **Technology** | | | |
| Inform the Legal and Compliance about restoration of IT applications. | IT | Seyad | None |

**Vital Records**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vital Record Description** | **Location of Vital Record** | **Media Type** | **Responsibility** | **Contact Details** |
| Compliance checks performed; transaction analysis; Legal contracts and NDAs. | One Drive | Softcopy | Legal and Compliance Team | - |
| **Alternate Recovery Strategies for Vital Records** | | | |
| * Regular backup of One Drive to be taken by IT Team | | | |

## **Business Continuity for Critical Infrastructure and its Applications**

**Power**

* The Power Management System includes the mains electricity supply provided by the building management for the office. The incoming supply is received through redundant pathways.
* For data center we have redundant UPS supply from building management 17.5 KV and can provide backup up to 8 hours.

**Telecom Connectivity**

* The telecom connectivity system consists of a supply of incoming fiber from Telecom Service Providers. The incoming cables are routed through a redundant path.
* These service providers install their end equipment in telephone rooms located on each floor. The built-in redundancy of cable route and the equipment assures high availability of connectivity.
* 4G/5G routers are available as backup Internet.

**Server room and Cloud Infrastructure**

* We utilize cloud infrastructure – Microsoft Azure and AWS for hosting servers and applications, data backups and network security – active directory.
* Server rooms and Cloud Infrastructure are monitored by IT operations teams with support from external vendors
* Alerting mechanisms to identify any failures and high utilization of infrastructure have been configured and are received by key IT stakeholders depending upon the alerts.

**Environmental controls**

* Fire detection mechanisms have been installed in server rooms and firefighting equipment have been installed and are periodically checked – every 3 months.
* CCTV systems are installed in entire office premises and have backup of recordings stored for up to 180 days.
* Fire detectors and sprinklers are installed in the entire office and connected to building fire systems.
* Exit and entry doors are protected by access control systems.
* Emergency exits are defined and displayed in the office areas.
* Environment monitoring – such as temperature, moisture and water level detection are installed in the server rooms.

**Application and trading related infrastructure redundancy**

* Office 365 – Email, Storage, messenger, and office desktop applications
* Email services are provided by Microsoft through exchange online.
* Storage for individual users and teams are available on One Drive and SharePoint
* Messenger is available on MS Teams
* Office applications are available through Microsoft.
* Backups are stored in cloud infrastructure of Microsoft for 90 days- daily backup.
* Corporate file servers
* Corporate file servers are hosted in server rooms.
* Backup is performed daily in XXXX storage – encrypted ransomware-protected storage.
* Secondary backup is offsite on XXXXX
* CRM and IB portals
* Hosted in server room, with back up taken daily in XXXXX storage.
* XXXX -code repository to be backed up on GitHub code repository and local file servers.
* Liquidity Providers and Bridges
* There are multiple levels of redundancy in liquidity providers with connectivity to multiple bridges.
* Bridges are hosted in Microsoft Azure along with high availability and cloud backup.
* Other Principal data
* Client onboarding data for other principals are stored in Microsoft Azure environments.
* Call Recording data
* Hosted in server room, with back up taken daily in XXXX storage along with backup storage on XXXX.

## **Call Tree Management**

* Smart Appex Crisis Management Team shall maintain the call tree for business continuity and shall be updated periodically.

## **Desktop Computer Configurations**

Description of Desktop: Dell, etc.: Dell AIO

Used By: All Employees

Business Activity Supported:

Connected to Which LAN’s: Yes, and Wi-Fi

Used for Host Access (Which Applications): network printing. Yes (Uniflow)

Special Features, Boards, Memory Size, etc.: over 20 Gigs HD, over 128MB Memory

Over 850 MHz Processor(s) 256 GB HD, 16 GB RAM

Ethernet Net Cards, Fax/Modems Yes

Proprietary Software required (indicate release number, version and/or level, as applicable: NA

**Smart Appex BCP Test Template**

**Business Continuity Plan**

# **Appendix 1**

Business Continuity Plan testing/Cascade Call executing analysis

|  |  |  |  |
| --- | --- | --- | --- |
| **Document prepared by:** | | |  |
| **Date:** | | | **Time start:**  **Time end:** |
| **Participants:** |  | | |
|  | | |
|  | | |
|  | | |
|  | | |
|  | | |
| **Issue identified** | | **Proposed Action** | |
| Stress Tests, failover Testing, Load testing, and BCP situations were identified and tested. | |  | |
| Power Outage, Remote Connectivity | |  | |
| Data Failover and Connectivity. | |  | |
| Phone Line Failover and Switchover. | |  | |
| Network Connectivity | |  | |