AN ISO/IEC 27001:2013 Certified Company

OutsourceBiz India Private Limited

BusinessProcess **Evolution**

Business Continuity Plan

&

Disaster Recovery Plan

PURPOSE

The purpose of this business continuity plan is to prepare OutsourceBiz in the event of extended service outages caused by factors beyond our control (e.g. natural disaster, manmade events) and to restore services to the best possible operating condition within a minimum time. OutsourceBiz is expected to implement preventive measures whenever possible to minimize operational disruptions and to recover as rapidly as possible when an incident occurs. This plan identifies vulnerabilities and recommends necessary measures to prevent extended service out.

PLAN OBJECTIVES

1. Serves as a guide for the OutsourceBiz recovery team.
2. References and points to the location of critical data.
3. Provides procedures and resources needed to assist in recovery.
4. Assists in avoiding confusion experienced during a crisis by documenting, testing and reviewing recovery procedures.
5. Identifies alternate sources for supplies, resources and locations.
6. Documents storage, safeguarding and retrieval procedures for vital records.

ASSUMPTIONS

1. Key people (team leader or alternates) will be available following disaster.
2. A national disaster such as nuclear war is beyond the scope of this plan.
3. This document and all vital records are stored in a secure off-site location, not only survive the disaster but are accessible immediately following the disaster.
4. Each support organization will have its own plan consisting of unique recovery procedures, critical resource information and procedures.

DISASTER DEFINITION

Any loss of utility service (Power, Water), connectivity (Systems and Network) or catastrophic event (Weather, natural disaster, vandalism) that causes an interruption in the service provided by OutsourceBiz data operations. This plan identifies vulnerabilities and recommends measures to prevent extended service outages.

RECOVERY TEAMS

1. Emergency Management Team (EMT)
2. Disaster Recovery Team (DRT)
3. IT Technical Services (IT)

TEAM MEMBER'S RESPONSIBILITIES

1. Each team member will designate an alternate.
2. All of members should keep an updated calling list of their work team member's work, home and cellular phone numbers both at home and at work.
3. All team members should keep this plan for reference at home, in case the disaster happens outside normal work hours. All team members should familiarize themselves with the contents of this plan.

INVOKING THE PLAN

This plan becomes effective when a disaster occurs. Normal problem management procedures will initiate the plan, and remain in effect until operations are resumed at the original location or a replacement location and control is returned to the appropriate functional management.

DISASTER DECLARATION

The management team of OutsourceBiz, with input from the Emergency Management Team (EMT), Disaster Recovery Team (DRT) and Information Technology (IT), are responsible for declaring a disaster and activating the various recovery teams as outlined in this plan. In a major disaster situation affecting OutsourceBiz data operation facility area, the decision to declare a disaster will be determined by OutsourceBiz Management Team. The EMT and DRT will respond based on the directives specified by the Management.

NOTIFICATION

Regardless of the disaster circumstances, or the identity of the person(s) first made aware of the disaster, the EMT and DRT must be activated immediately in the following cases:

1. Two or more systems are down concurrently for three or more hours
2. Five or more systems are down concurrently for three or more hours
3. Any problem at any system or network facility that would cause either of the above conditions to be present or there is certain indication that either of the conditions are about to occur.

Emergency Management Standards

Data Backup Policy

OutsourceBiz Clients scan their claims and upload to OutsourceBiz Certified HIPAA Compliant FTP Server, located at Cogeco Peer Virginia Data Center, USA – very near Washington DC.

OutsourceBiz Secured FTP Server has adequate disk space for data storage. Cogeco Peer Facility in Virginia, USA is a professionally run Data Storage Center with its own backup systems as well as Disaster Recovery Plans in place. OutsourceBiz always keeps all the important data backup at its Virginia HIPAA Compliant Secured FTP Server (geographically separate location) along with local data backup as well as data secured on DVD disks stored at the OutsourceBiz India BPO Facility.

IT always follows these standards for its data backup and archiving.

EMERGENCY MANAGEMENT PROCEDURES

The following procedures are to be followed by OutsourceBiz management team in the event of an emergency. Where uncertainty exists, the more proactive action should be followed to provide maximum protection and personnel safety. In the event of any situation where access to a building is denied, OutsourceBiz Management personnel should report to alternate locations. Primary and secondary locations are listed below.

IN THE EVENT OF NATURAL DISASTER

In the event of major catastrophe affecting OutsourceBiz data operation facility area, notify Emergency Management Team and Disaster Recovery Team of pending event - if time Permits If the impending natural disaster can be tracked, begin preparation of site within as soon as circumstances and situation permits, as follows:

1. In case of loss of electrical power, deploy portable generators.
2. Facilities department will be on standby for replacement shelters.
3. Basic necessities are acquired by support personnel.
4. Assure food and water supplies.
5. Create an image of the system and files.
6. Backup critical system elements.
7. Create backups of e-mail, file servers etc.

IN THE EVENT OF FIRE

If fire or smoke is present in the facility, evaluate the situation, determine the severity, categorize the fire as major or minor and take the appropriate action as soon as possible if the situation warrants it.

1. Personnel are to attempt to extinguish minor fires (e.g., single hardware component or paper fires) using hand-held fire extinguishers located throughout the facility at strategic locations. Any other fire or smoke situation will be handled by qualified building personnel until the local fire department arrives.
2. In the event of a major fire, call the Fire Brigade (Dial 101) and immediately evacuate the area.

3. In the event of any emergency situation, system security, site security and personal safety are the major concerns. If at all possible, the operations supervisor should remain present at the facility until the fire department has arrived.
4. In the event of a major catastrophe affecting the facility, immediately notify OutsourceBiz management team.

IN THE EVENT OF INTERNET SERVICES PROVIDER OUTAGE

In the event of internet service provider outage the guidelines and procedures in this section are to be followed.

1. Notify senior management of outage immediately.
2. Determine cause of outage and timeframe for its recovery
3. Whether it is a major outage and downtime will be greater than 12 hours
4. Remember, OutsourceBiz always maintains 2 Internet Service Providers simultaneously to have safe and uninterrupted operations - in case any one of the Service Provider has a problem. Switch all systems to the provider whose service has not been interrupted, while advising IT about the issue.

IN THE EVENT OF FLOOD OR WATER DAMAGE

In the event of a flood or broken water pipe within any computing facilities, the guidelines and procedures in this section are to be followed

1. Immediately notify all other personnel in the facility of the situation and be prepared to cease operations accordingly – if necessary.

2. Water detected below the raised floor may have different causes. If water is slowly dripping from an air conditioning unit and not endangering equipment, TURN OFF THE AFFTECTED UNIT and contact repair personnel immediately.

3. If water is of a major quantity and flooding beneath the floor (water main break) immediately follow power-down procedures. While power-down procedures are in progress, evacuate the area and follow management's instructions. Notify municipal authority if it on the main water system.

PLAN REVIEW AND MAINTENANCE

This plan must be reviewed annually and mock drills should be exercised on annual basis. The test may be in the form of a walk through, mock disaster, or component testing. The hard-copy version of the plan will be stored in a common location where it can be viewed by site personnel and the EMT and DRT. Electronic versions will be available at OutsourceBiz network resources as provided by IT.

IF FACILITY WILL BE UNAVAILABLE FOR A LONGER PERIOD

In the unlikely event of a Main Facility becoming unavailable for a longer period of time where it will be impossible to resume regular operation, implement the plan of using alternate locations. Senior Management members are aware of mutual understandings we have with a few Call Centers in the Salt Lake Electronics Complex which are operational only during nights. Also, limited number of remote workstations can be made available at OutsourceBiz's Dallas office – which are accessible through remote access, and can become operational on a very short notice. Arrangements can also be made to use several workstations at our Dallas based Accountants office as well.

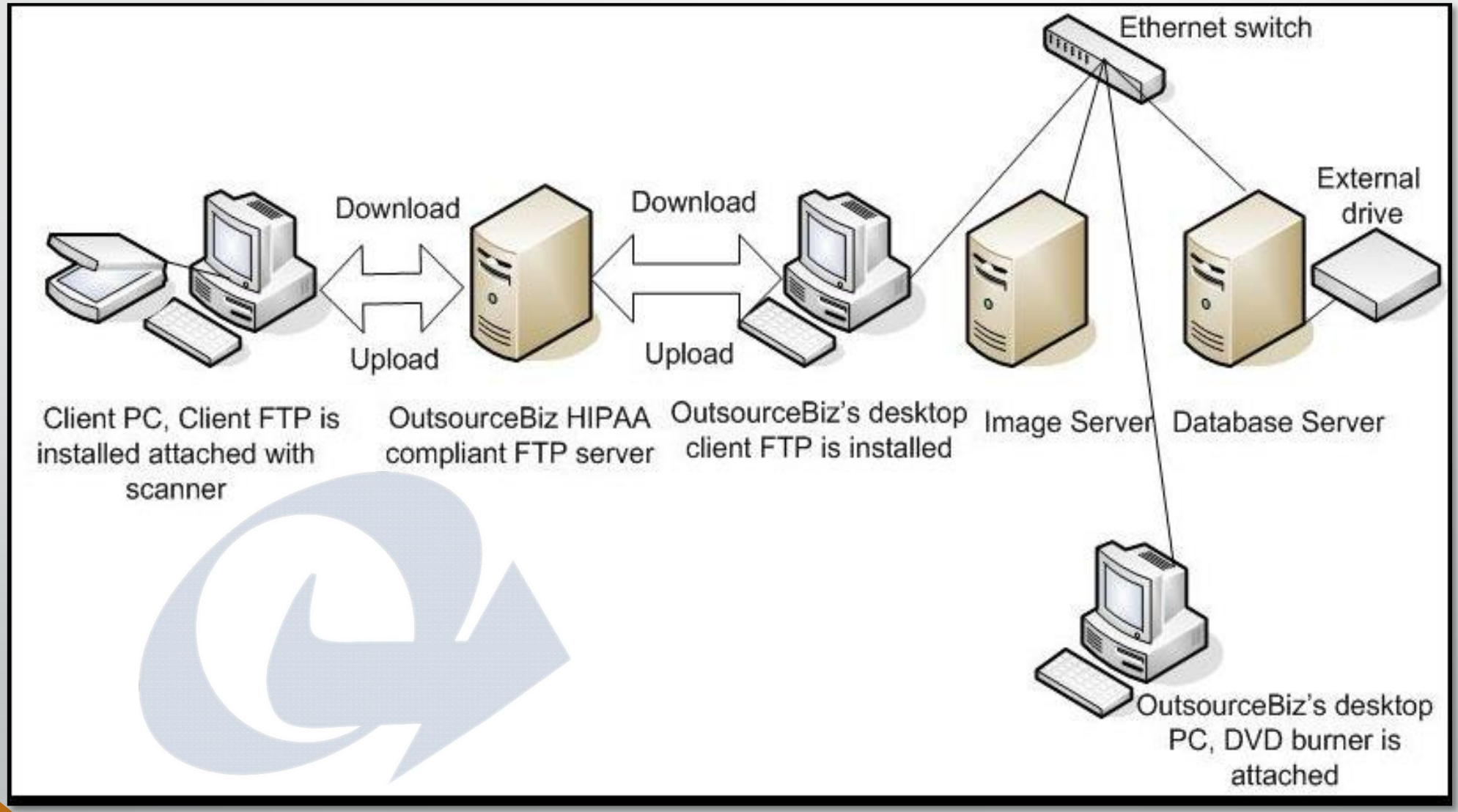
Diagram of data backup process including the path of Data from Client to OutsourceBiz India Pvt. Ltd.

OutsourceBiz Clients scan their claims and save the files in the formats of their choice (JPEG, PDF) and upload to OutsourceBiz' s HIPAA Compliant Secured FTP server using any client FTP software securely. OutsourceBiz's HIPAA Compliant Secured FTP server is situated in COGECO PEER1 Virginia facility, USA.

Customer data is downloaded to the local server at India facility. Here, dot net web based application (which is custom written and developed by OutsourceBiz's software development team) controls each part of data entry - up to the final output file generation.

All the data (scanned claims) is centrally distributed from the image server and stored in the Database by this application. Finally, OutsourceBiz Production Manager(s) uploads the output file (837 Format/or any other) to the Secured FTP server for the clients to download.

Provided below is a diagram of OutsourceBiz's data backup process including the path of data from Client to OutsourceBiz through HIPAA compliant FTP server at Virginia.



Please note that OutsourceBiz discourages and prohibits transmission of any secured data through email, except mutually agreed to and accepted secured email – ONLY IF SO REQUESTED BY THE CLIENT and ACCEPTED BY OUTSOURCEBIZ IN WRITING.

In the image server, there is an extra drive attached, which is mirrored with the drive where all the scanned claims are stored. Once all the processing for a batch of data is completed and sent to the client, this data is compressed and stored in another location of OutsourceBiz network and burned to DVD for future reference and safe keeping.

Database backup is taken daily from the direct access drive in database server.

All members of OutsourceBiz keep their important data on the File Server and OutsourceBiz IT support team periodically saves the data at another location of the OutsourceBiz Network.