Business Continuity and Disaster Recovery Plan

Prepared for

Revised: June 2024
Last Tested: April 10, 2024
Last Test Status: Successful

Overview

OutSolve's policy is to respond to a Significant Business Disruption (SBD) by safeguarding employees' lives and firm property, making an operational assessment, quickly recovering and resuming operations, protecting all of information assets and data, including client information, and meeting our clients' needs and requirements with minimal interruptions. In the event that we determine we are unable to continue our business, we will assure clients prompt access to their reports and data.

Significant Business Disruptions (SBDs)

Our plan anticipates two kinds of SBDs, internal and external. Internal SBDs affect only our firm's ability to communicate and do business, such as a fire in our building or pandemic. External SBDs prevent the operation of the area or region, such as a terrorist attack, a city flood, hurricane, or a wide-scale, regional disruption. Our response to an external SBD relies more heavily on other organizations and systems, such as our off-site backup provider and website host.

Approval and Execution Authority

Steven Claverie, Chief Technology Officer, is responsible for approving the plan and for conducting the required annual review. As such, Mr. Claverie has the authority to execute this BCDRP.

Plan Location and Access

Our firm will maintain copies of its BCDRP plan and the annual reviews, and the changes that have been made to it for inspection. An electronic copy of our plan is located on the shared drive at H:\Standards\Disaster Recovery\.

Business Description

Our firm conducts business in Affirmative Action planning and compliance as well as other human resource related reporting requirements. Our clients provide employee data, including race, gender, job title, salary, and employee name. Our firm provides consulting and summary reporting of this data, to provide client compliance with Executive Order #11246 (Equal Opportunity Employment). We provide our services to federal contractors who are required to comply with this order.

Office Locations

Our headquarters is located at 3330 West Esplanade Avenue, Suite 301, Metairie, Louisiana 70002. Its main telephone number is (888) 414-2410. All employees perform work onsite at an office location behind a WatchGuard firewall or via remote connection using secure VPN connection.

Alternative Physical Location(s) of Employees

In the event of an SBD, we will move our critical equipment and staff from the affected office to one of our satellite office locations. These offices are located at 455 University Ave., Suite 300, Sacramento, CA 95825; 1941 Bishop Lane, Suite 709, Louisville, KY 40218; 7001 West 43rd Street, Houston, TX 77092; and 4055 Faber Place Drive, North Charleston, SC 29405.

Customers' Access to AAPs and other reports

Our client portal website, located at https://clients.outsolve.com, is hosted on an OutSolve managed virtual server in the Microsoft Azure cloud environment. The host guarantees 99.9% uptime and is located in a separate geographic area from our firm's location. The client portion of our website houses the summary reports required by our clients. In the event of an SBD, all reports will continue to be available to our clients, even if the office is shuttered. Only registered website users will have access to the client section of the website, and granular access to client reports is only provided after a manual authorization process.

Data Back-Up and Recovery

Our firm maintains all of its information assets digitally. All data files and reports are stored at a TierPoint Datacenter located in Dallas, TX. All email is stored in Microsoft's Office 365 platform. Steven Claverie, Chief Technology Officer is responsible for the maintenance of these files and assets.

The firm backs up its electronic records daily by encrypted Network Attached Storage at the Tierpoint facility and keeps a hot backup/disaster recovery setup in Microsoft's Azure cloud environment. The off-site copy is synced every hour, and snapshots are available for a 90 day period.

In the event of an internal or external SBD that causes the loss of our virtual servers at our primary Tierpoint data center, we will roll over electronic operations to our disaster recovery site at the secondary Azure data center. If our primary office location site is inoperable for an extended period of time, we will continue operations from our alternate locations in Sacramento, Louisville, Houston, or North Charleston.

Pandemic Recovery

Pandemics are potentially disruptive situations which can occur at any time and affect normal business processes. Fortunately, the level of awareness of pandemics is higher now. By keeping a close eye on alerts and messages from the Centers for Disease Control (CDC), state and local emergency organizations, and local media reports, sufficient advance warnings should be possible. The focus here is on the level of business disruption which could arise from a pandemic.

Pandemic outbreaks have been assessed as follows:

Potential Disaster	Probability Rating	Impact Rating	Brief Description Of Potential Consequences & Remedial Actions
Pandemic outbreak	3	4	Loss of upwards of 40% of staff for 2-3 weeks; inability of company to function without staff in place

Probability: 1=Very High, 5=Very Low Impact: 1=Total destruction, 5=Minor annoyance

As with any other disaster or business outage, care should be taken to provide an adequate plan for pandemic response and recovery, however slight the risk or impact should be. OutSolve allows all employees the ability to connect remotely to servers at the Azure data centers. OutSolve will provide internal communication to all staff in the event a pandemic threat is assessed. As part of this communication, best practices are provided to prevent further spread of the pandemic amongst staff, as well as ways employees can work remotely in the event the office is closed. Senior management will determine any plan of action and what recovery steps will be needed, and OutSolve will coordinate with their third party IT-services firm, Restech, to enact a rollover or restore backups, if the pandemic threat necessitates.

In the event the pandemic worsens, to the impact level mentioned above, OutSolve will notify clients of the potential business impact, while still allowing for clients to access the OutSolve client portal to transfer data and access their existing reports, without the need of staff to manage. Once this stage of the pandemic threat is reached, the pandemic action, recovery, and remediation phases will follow a similar plan as any disaster, detailed further in this document.

Disaster Recovery

Computer systems and infrastructure are vital to the operation of virtually all-commercial enterprises. The loss of any component could cause a virtual shut down of most businesses. A systems disaster will also have the affect of trickling down to other related business partners and customers, which are not otherwise in-house system dependent.

To prevent this from happening, OutSolve requires an adequate disaster recovery plan. A disaster recovery plan (DRP) is a formal plan that specifically addresses how to prepare for disasters and how to restore systems once a disaster strikes. This disaster recovery plan addresses three phases:

- general protection,
- specific protection, and
- recovery.

In the general protection phase of a disaster recovery plan; steps are taken to minimize the effects of a disaster. Steps include backup procedures, off-site storage setup, stockpiling of hardware, and alternative plans for employee worksites. Regardless of the type of disaster, these steps will prove effective in restoring systems to pre-disaster operations.

In the specific prevention phase, steps are taken to eliminate possible threats to the computer systems. Computer viruses, hacking, and information theft are just a few of the threats that face systems on a daily basis. By implementing various security measures, the technology resources have a better chance of being protected from malicious attacks.

The third phase of a DRP is to plan for the recovery of the systems or infrastructure when a disaster does occur. Recovery comes in two stages:

1) The analysis of the damage

2) The repair of the damage.

To speed recovery, teams are organized in advance and are ready to be deployed when needed. The names and numbers of both vendors and repair companies are kept organized and up-to-date for fast and reliable reference.

Even with a great deal of planning and layered protection procedures, computer systems are still more vulnerable than necessary until all measures are implemented. The various lists and appendices included in this plan are updated on a yearly basis to ensure their accuracy.

A well thought out and executed disaster recovery plan will keep systems well protected and provide for efficient recovery in the event of a disaster.

I. General Protection

a) Backup Policy

- **Server Backup Protection Policy**
  The following procedure is utilized to ensure maximum backup protection.

  1. Daily – A daily backup of the file servers are made each night on an encrypted NAS device. Transactional backups are also sent every hour to the off-site data center in Azure.

  2. Rolling 90-days – The most recent 90 days of changes are kept via our NAS device as well as the off-site data center. OutSolve can go back to a specific moment in time in the previous 90 days to pull a snapshot of that time period's backup state.

- **Workstation Backup Protection Policy**
  The office has several workstations in use. The main network backup may not automatically back up these workstations. Therefore, all documents are stored in the appropriate location within the appropriate file server. Only files stored on a file server will be recovered and restored.

b) Power Surge Protection

Surges can cause serious damage to both hardware and software. All equipment connected to the workstations and critical electronic equipment (such as external switches, printers, and copiers) are connected to the proper surge protection equipment. Lines leading to and from network devices have surge protection. This includes both the data and communications lines for total protection. Equipment will never be plugged directly into an outlet under any condition since surges in the line could destroy the equipment as well as any connected equipment. The following guides on surge protection are followed to the letter for total protection.

- All switches are connected into an uninterruptible power supply

- Workstations and all peripheral equipment connected to the workstations, such as monitors and printers are plugged into high quality surge protectors or uninterruptible power supply.

c) Password Security

All passwords, including server passwords and workstation passwords, are changed on a three month basis. Users are prompted to change their passwords at the three month interval, automatically by the authenticating server on the network. The passwords must meet a minimum length of eight characters and meet the minimum complexity requirements set forth by Microsoft Entra.

d) Replacement Parts Stockpiling

This phase is defined as an on-going policy dealing with maintaining a small inventory of replacement equipment in the event of a disaster. Maintaining a computer equipment inventory allows for faster recovery by keeping the most commonly used parts on hand. The CTO is responsible for determining a list of valid equipment that is purchased and used in the event of an emergency. Such equipment includes, but not limited to, surge protectors, data storage devices, workstations, etc. Whenever a part from this inventory is used, it is logged so that it may be promptly replaced and made available for the next incident.

e) Pre-Disaster Assessment

The purpose of the pre-disaster assessment phase of the DRP is to examine a situation and determine if a disaster needs to be declared. A disaster is defined as serious damage or loss of equipment that hinders OutSolve from performing its day-to-day operations. This step is taken in the event of both foreseen and unforeseen disasters. A foreseen disaster includes a disaster for which an early warning is available. Anticipated disasters include hurricanes, some severe thunderstorms, and flooding. In the event of an unforeseen disaster, assessment is made at the disaster site. Unanticipated disasters include hacker attacks, lightning strikes, computer viruses, fire, and theft. Once a disaster has been declared, the notification phase is implemented.

f) Notification

The notification phase is implemented when a disaster has been declared. The phase will start with notifying the people on the contact list (Appendix 1) of the disaster and its impact. A rough estimate of the damage is given (ex. was the building flooded, was there a fire, etc.) and a determination of how the disaster affected operations is made. Once the people on the contact list have been notified the reaction and recovery phase of the DRP begins.

g) Equipment Availability Assessment

The availability of all equipment that may need replacement is assessed as part of the notification phase. The goal is to determine which suppliers are able to handle replacement orders. In the event of a disaster, this information will speed equipment delivery and installation.

h) Reaction

The reaction phase of the recovery plan is used to prepare for a foreseen disaster. When a foreseen disaster is declared, the steps of the reaction phase are put into effect.

- Disaster preparation backups are made of the entire network emphasizing servers (web, database, and file) for storage both on and off site if time allows.

- In the event of severe storms, all equipment is shutdown and disconnected from power, phone and network cables to further isolate against direct electrical strikes.

- If flooding from rising water or window breakage is possible, all equipment is elevated as high as possible to lessen the chance of flood damage. All equipment located in offices with windows will be moved to a place within a hallway, or away from windows to prevent damage to the equipment in the event of window breakage.

i) Mobilization

The mobilization phase is implemented after a disaster has occurred.
The steps of mobilization are:

- The deployment of the Disaster Recovery Team.

- Activation of any reciprocal processing arrangements that may have been put in place with other entities hosting similar systems (if needed).

- Implementation of backup plans for operation without computers

II. Recovery

a) Analysis

The first step in recovery after a disaster is to determine the extent of damage to all system components. Selected members of the disaster team will go through the site and make a detailed inventory of all equipment and its condition. The inventory shall include the following:

- Equipment location,

- An item list by equipment type: is it a workstation, printer, switch, etc.,

- Each item’s serial number for an exact identification,

- A damage rating: operational, repairable, or scrap.

Damage to look for will vary by disaster. In both cases of fire and flood, water will be a significant concern, and probably the major cause of damage. **In cases of suspected water damage, the equipment will not be turned on until it has been thoroughly dried.**

b) Replacement & Repair

To place orders and schedule repairs, the vendor contact list will be used *(See Appendices 4 & 6).* A determination may be made to contact a second company to repair equipment.

The main source of funds for restoration will be insurance proceeds (See Appendix 1 for contact information of insurance carriers and FEMA). Depending on the extent of the disaster, insurance may not cover the total cost of damage. In the case of older equipment, it is unlikely replacements will be found. In this case OutSolve will look at upgrading. Even in choosing not to upgrade, more funds may be needed. If a second source of income will be necessary, OutSolve will access its emergency funds.

c) Operability

While restoring the system to operational status, initial effort will be placed on servers. Once they are fully operational then the connection to the Internet, as well as the operability of workstations and other equipment will be addressed.

d) Reboot Backup Procedure

Once the damaged system(s) have been replaced or repaired, the software and files are reinstalled. In reinstalling, the software and files will be loaded from the backup media. By loading off the backup media, the data transferred is a direct copy of what was on the machine before the disaster. Reloading in this fashion also allows us to bring the system on-line in a more organized and faster manner than by reloading the programs and reconfiguring the software. The element this plan relies on is an up to date backup of both programs and data files. Note: We will use the original image to reinstall workstation software and use the backups to restore the data files associated with this software.

e) Reliability

OutSolve and its representatives will make sure restoration solutions are long term and reliable. In the effort to bring the system on-line as quickly as possible, short-term solutions may be used with the intention of replacing them later. When hardware and software solutions such as these are implemented early on, they may be built upon as the system is brought back on-line.

III. Restoration

a) Hardware

The hardware phase of the detection process will encompass the identification and remedy of any physical hardware faults in the damaged system(s). This includes bad connections, mislaid wire, terminals not properly connected, and the like.

b) Software

Software problems are detected and fixed in the software phase. Software detection will likely be the most long term part of the recovery since software problems may continue to appear long after the damaged system is up and running.

c) Post-Recovery Debugging

This covers both hardware and software problems. With the complete start up of a system after a disaster there are bound to be a number of minor problems to be addressed. Detecting and correcting will continue until all problems related to the disaster have been identified and resolved.

Disclosure of Business Continuity and Disaster Recovery Plan

Attached is our written BCDRP disclosure statement we provide clients and during a Request for Proposal (RFP) response. We also provide it to clients upon request.

Updates and Annual Review

Our firm will update this plan whenever we have a material change to our operations, structure, business or location or to those of our alternate location or off-site storage facility. In addition, our firm will perform a Business Impact Analysis (BIA) annually to determine if there are any changes in our operations, structure, business, location or backup facilities that would need to be reflected in our BCDRP. This analysis and review will be performed annually, on or around January 1st.

Plan Approval

I have approved this Business Continuity and Disaster Recovery Plan as reasonably designed to enable our firm to meet its obligations to clients in the event of an SBD.

Signed: _____

Title: _____

Date: _____

OUTSOLVE
BUSINESS CONTINUITY AND
DISASTER RECOVERY PLAN

Appendix 1
Emergency Contact List

** disaster recovery team leader
* members of disaster recovery team

**Name	Jeremy Mancheski
(Home#)	(504) 454-1955
(Work#)	(504) 486-2410
(Cell#)	(504) 458-5568
e-mail	jmancheski@outsolve.com

* Name	Baldwin Read
(Home#)	(985) 705-3304
(Work#)	(504) 486-2410
e-mail	bread@outsolve.com

* Name	Patrick Savoy
(Home#)	(985) 727-4928
(Work#)	(504) 486-2410
e-mail	psavoy@outsolve.com

* Name	Steve Claverie
(Work#)	(504) 486-2410
(Cell#)	(504) 606-8885
e-mail	sclaverie@outsolve.com

Internet Provider	Cogent
Email:	support@cogentco.com

ResTech
220 Phlox Ave.
Metairie, LA 70001
(504) 733-5633
www.restech.net
help@restech.net

FEMA region VI
Regional Director
940-898-5399

Jefferson Parish Emergency Management Office
Col. David Dysart, Director
910 3rd Street
Gretna, LA 70053
P: 504.349.5360
F: 504.227.1315
Email: JPEOC@JeffParish.net

OUTSOLVE
BUSINESS CONTINUITY AND
DISASTER RECOVERY PLAN

Appendix 2

NON-STANDARD EQUIPMENT LIST
& POTENTIAL VENDORS

Equipment	**Department**	**Vendor/Mfg**
All non standard equipment	IT	ResTech

Appendix 3
Business Continuity and Disaster Recovery Plan Disclosure

OutSolve's Business Continuity and Disaster Recovery Planning

OutSolve has developed a Business Continuity and Disaster Recovery Plan on how we will respond to events that significantly disrupt our business. Since the timing and impact of disasters and disruptions is unpredictable, we will have to be flexible in responding to actual events as they occur. With that in mind, we are providing you with this information on our business continuity and disaster recovery plan.

Contacting Us – If after a significant business disruption you cannot contact us as you usually do at (504) 486-2410 or info@outsolve.com, you should call our alternative number (888) 414-2410 or go to our website at https://outsolve.com.

Our Business Continuity and Disaster Recovery Plan – We plan to quickly recover and resume business operations after a significant business disruption and respond by safeguarding our employees and property, making a financial and operational assessment, protecting the firm's information assets, and allowing our clients to access their AAPs. In short, our plan is designed to permit our firm to resume operations as quickly as possible, given the scope and severity of the significant business disruption, usually within 48 hours of a disruption.

Our business continuity and disaster recovery plan addresses: data backup; assessment after a disaster and recovery; alternative communications with clients and employees; alternate physical location of employees; critical suppliers; and assuring our customers prompt access to their AAPs and reports if we are unable to continue our business.

Our firm backs up our data records in a geographically separate area. While every emergency situation poses unique problems based on external factors, such as time of day and the severity of the disruption, we have been advised by our off-site backup provider that while they will make every attempt to restore our data as quickly as possible, there may be slight delays as we download all of our restore data. Any requests for AAPs or other reports could be delayed during this period.

Varying Disruptions – Significant business disruptions can vary in their scope, such as only our firm, a single building housing our firm, the business district where our firm is located, the city where we are located, or the whole region. Within each of these areas, the severity of the disruption can also vary from minimal to severe. In a disruption to only our firm or a building housing our firm, we will transfer our operations to a local site when needed and expect to recover and resume business within 24 to 48 hours. In a disruption affecting our business

district, city, or region, we will transfer our operations to a site outside of the affected area, and recover and resume business within four business days. In either situation, we plan to continue in business, transfer operations to our alternate location if necessary, and notify you through our website https://outsolve.com or our customer emergency number, (888) 414-2410 how to contact us. If the significant business disruption is so severe that it prevents us from remaining in business, we will assure our customer's prompt access to their AAPs and reports.

For more information – If you have questions about our business continuity and disaster recovery planning, you can contact us at (888) 414-2410 or info@outsolve.com.