Adaptive Web Ltd
Disaster Recovery & Business Continuity

August 2019

AD-01

1.0 Overview

1.1 Policy Statement

It is the policy of Adaptive Web Limited to maintain a Disaster Recovery and Business Continuity Plan and associated controls, for all critical functions, to minimize downtime and data loss in the event that all or part of its operations and/or computer services are rendered unusable. The goal of these processes is to minimize any negative impact on company operations and the services provided to our clients.

The MD is responsible for ensuring compliance with this policy and that it is tested and reviewed annually. Adaptive Web Limited's disaster recovery efforts exercise reasonable measures to protect employees, safeguard assets, and client accounts.

1.2 Introduction

The purpose of this Disaster Recovery and Continuity Plan is to ensure that Adaptive can still accomplish its mission and it would not lose the ability to process, retrieve and protect information maintained in the event of an interruption or disaster.

At the onset of an emergency condition, Adaptive employees and resources will respond quickly to any condition, which could impact Adaptive's ability to perform its critical functions.

The primary business location of Adaptive - referred to in this document - is The Mill, Lodge Lane, Derby DE1 3HB

2.0 Defined Scenario

A disaster is defined as a disruption of normal organisation functions where the expected time for returning to normal operations would seriously impact Adaptive's ability to maintain customer commitments and business continuity. A disaster could be caused by a natural or man-made event.

Scenarios which could impact the operational continuity of Adaptive's primary business location are:

- Power failure which results in all pc's, servers, lighting, heating being offline
- Infrastructure failure such as, server/switch or broadband outage
- Fire in the Adaptive or adjacent buildings
- Flood
- Terrorist Attack
- Burglary
- Staff absences due to pandemic

3.0 Recovery Objectives

The plan was written with the following objectives:

- To ensure the life/safety of all Adaptive employees throughout the emergency condition, disaster declaration, and recovery process.
- To re-establish the essential organisation-related services provided by Adaptive as quickly as possible, reducing service downtime.
- To mitigate the impact to Adaptive's customers through the rapid implementation of effective recovery strategies.
- To provide instructions about how and when the plan will be activated, including outage timeframes, who declares a disaster and who should be contacted.

4.0 Plan Assumptions

Adaptive's Disaster Recovery Plan was developed under certain assumptions. These assumptions are:

- Adaptive's recovery efforts are based on the premise that Cloud Computing allows all Adaptive staff to operate from any location with Internet access including from home.
- All records, emails and documentation can be retrieved from virtual storage via Cloud storage without delay. Zero data loss is anticipated even if the primary business location was destroyed.
- Adaptive staff currently have the option to work from home in many circumstances which can reduce risks of illnesses being spread or exposure to a number of risks that might impact the primary business location. In some emergency/disaster scenarios this would be extended on the MD's authority.
- Staff, developers in particular, are quickly able to set up and work from home due to the availability of Git Repo which contains a recent image of a developer's machine.
- This document and all vital records are stored in a secure cloud location which is accessible by all staff.

5.0 Disaster Definition

A disaster is defined as any loss of utility service (power, water), connectivity (systems/sites), or catastrophic event (weather, natural disaster, vandalism) that causes an interruption in the service provided by Adaptive to its customers. The plan identifies vulnerabilities and recommends measures to prevent extended service outages.

6.0 Recovery Strategies

All working documents, contracts etc are held in secure virtual storage meaning that even if the Adaptive premises were totally destroyed – all documents would be safe and could be accessed remotely.

Websites and applications are hosted and backed-up at multiple UK locations to do everything humanly possible to maintain availability 24/7 under any circumstances. Two main companies are used – www.memset.com and Amazon AWS ensuring the highest levels of security. These companies have been selected by Adaptive because of their dedicated resilient server set-up, back-up power generators, pro-active monitoring, alarms and security.

Memset holds certification under ISO 9001:2008 Quality Management System; ISO 14001:2004 Environmental Management System and ISO 27001:2005 Information Security Management System.

Amazon AWS delivers its services in accordance with the industry's highest and strictest security best practices. AWS conducts regular and thorough audits to demonstrate the security of its infrastructure. AWS holds the following certification; SAS 70 Type II, PCI DSS Level 1, HIPAA, FISMA Moderate and ISO 27001. AWS also conducts regular audits to ensure its infrastructure security.

6.1 Emergency Phone Numbers

Maintenance & repair

1. Electrical: **01332 574547**
2. Glazier: **01332 756200**
3. Carpentry: **01332 721148**
4. Plumbing: **01332 415293**

IT services

1. **0800 634 9270 (memset.com)**
2. **Online support request via https://aws.amazon.com/contact-us/ (AWS)**

Utilities

1. Electricity: **0800 056 8090**
2. British Gas: **0800 077 4412**
3. Water: **0800 783 4444**

6.2 Threat Profile

Hazard:	Profile of Hazard:	First Response:
Fires	A fire in the vicinity of Adaptive's office could pose a risk to Adaptive's staff and equipment.	Step 1: Follow fire drill procedure Step 2: Evacuate personnel on alarm, as necessary Step 3: Notify fire department Step 4: Shut off utilities Step 5: Account for all personnel Step 6: Assess damage
Fire in the Adaptive Office	A fire in the Adaptive office could destroy servers and staff pc's. The likelihood of this happening is low.	Step 1: Work from home Step 2: A developer sets up a local environment from their home pc Step 3: All client resources are located and accessible from within Google Drive Step 4: Code is submitted to the Git Repo which is backed up to the cloud Step 5: Developer uses a recent image of their machine (via usb) to install all relevant software
Flood	Floods are an extremely remote risk given the location of Adaptive's primary business location (second floor offices).	Step 1: Evacuate offices if flooding threatens to invade the offices. Step 2: Remove equipment at risk and use sandbags to protect offices if appropriate.
Power failure	Power failures can be caused by storms, lightning or construction equipment digging in the wrong location.	Step 1: Call electrical company for assessment of downtime Step 2: Leave office to work remotely from outside the affected area if downtime will be more than an hour. Step 3: Working remotely, use the cloud based document storage and code backups. Step 4: Utilise the latests image of a local environment setup.

Terrorist attacks	A terrorist attack on Derby or in the near vicinity could not only impact on the primary business location but may also impact on the ability or willingness of staff to work normally.	Step 1: Protect the safety of staff by all appropriate means Step 2: Obtain information from emergency services and local/national government as appropriate regarding safe travel of employees on any forthcoming business trips. Step 3: Continue to work remotely (including home working) if the primary business location is affected.
Burglary	A raid on the primary business location could result in theft of equipment and damage. Risks are minimized by security and alarms on premises. Adaptive's main office and management offices are protected by separate alarms behind locked doors.	Step1: MD (or his deputy) responds to the emergency call and assesses whether damage/theft require staff to continue to work from home/remotely. Step 2: Contact insurance company to begin claims process. Step 3: All pc's are password protected with management having access to all login details in LassPass (password details are sealed with AES-256 bit encryption, salted hashing, and PBKDF2 SHA-256).
Pandemic	An officially declared Pandemic would impact on Adaptive personnel. In less serious circumstances even a severe flu outbreak or other contagious illness could impact on Adaptive's ability to complete work	Step 1: Adaptive's MD to monitor absence levels from the first indication of a severe illness and to organize back-up contractors. Step 2: Staff to be advised to work remotely, from home, to reduce chance of contracting a contagious illness.
Nagios Monitoring Service Fails	Nagios monitoring service could fail which would result in no notifications being sent about the status of websites and services being monitored. Nagios is hosted at AWS so the risk is low, however a second instance of nagios(a slave) may be required to monitor the master nagios node.	

Loss of Broadband	There is a 'medium' risk that the company will experience a loss of broadband. Operations resumed after 1hr	1. Connect to a wifi hotspot 2. Alternatively switch over to No 1's routing 3. Work from home if after a reasonable time the services are not available.
Local DNS server 2 fail	There is a risk that the local DNS server at Adaptive goes offline due to power failure, flood, fire. Operations would be resumed after 2hrs. No external client sites would be affected as this local server serves adaptive only.	Switch the Adaptive traffic to the backup Memset VPS or AWS servers which are located off site. Details are located in the secure LastPass vault.
Local Server 1 fail	Should the Git Lab server fail then the facility to deploy code would not be possible for approximately 2-3 days whilst the server is re-built. Rocket Chat, the internal messaging system data would be lost. The impact is minimal as users can switch to use Skype messaging.	Git Lab data is backed up to AWS Inform users that Skype is being used

6.3 Recovery Strategy Overview

Adaptive's Disaster Recovery Plan is based on the organisation surviving the loss of facilities and/or key personnel and systems during a disaster and maintaining business continuity.

Steps:	Instruction:
1: Evacuate the office	If the emergency requires an evacuation of employees, execute evacuation plans contained in the Emergency Procedures section.
2: Determine length of outage	Review written and verbal damage assessment reports from the relevant authorities and then estimate the amount of time the facility will be uninhabitable.
3: Select disaster level	Based on the estimated duration of the outage, declare the disaster event as either a L1 (Less than 48hrs.), L2 (48hrs. to 6 weeks), or L3 (6 weeks or longer).
4: Activate alternative working arrangements	Staff would be able to work from home with minimal set-up times and service levels could return to normal as soon as they were at their home. Some staff already work from home most days anyway.
5: Contact customers	Using the contacts held remotely in Google Drive/JIM System, customers would be informed of alternative working arrangements.

6.4 Plan Participants

The MD of Adaptive is the key person in charge of declaring a disaster and activating the recovery plan.

In his absence the member of staff deputising would be responsible.

Signed by Senior Director of company

Dan Frost
Managing Director