SAFEDATASTORAGE

Business Continuity Plan – Victoria Works

Specific Adaption of BCP for COVID-19

Document Ref.	BCP_SPECIFIC_COVID-19
Version:	2
Dated:	07 April 2020

SAFEDATASTORAGE

ISO 9001 CERTIFIED
UKAS MANAGEMENT SYSTEMS
British Assessment Bureau

ISO 27001 CERTIFIED
UKAS MANAGEMENT SYSTEMS
British Assessment Bureau

Contents

Introduction

This Business Continuity Plan (BCP) captures the information that describes Safe Data Storage's (SDSL) ability to withstand the potential impact of COVID-19.

All system users at SDSL use a Remote Desktop environment on a daily basis for all of their day to day duties, all vital servers or systems are backed up every hour using StorageCraft ShadowProtect and replicated to a secondary site.

Our telephony system is VOIP based and has a mobile application for IOS and Android. For long term solutions, the desk phones can be taken home or shipped to home addresses where they auto configure and connect to our central system.

Both of our Datacentres have their own Business Continuity Plans.

Definition of a Disaster

For this specific risk (COVID-19), we are defining a disaster as either a Government induced policy which dictates that travel should be minimised, that a City, County or Country lockdown is enforced or that SDSL's Management Team decide that they wish to invoke measures to protect the health of their personnel.

Purpose

The purpose of this BCP document is to outline the method and technology that the business will take should the invocation of the aforementioned disaster be realised.

The primary focus is to protect the staff within the organisation and secondarily to ensure that our service to our clients continues in a manner that is expected.

Objectives

The principal objective of this BCP is to document our well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from the invocation of this specific disaster.

Scope

All of the following areas are considered:

- Telephony System
- Network Infrastructure
- End-user Computers
- Organisational Software Systems
- Database Systems

Communicating the Disaster

Communicating with Employees

The Managing Director will ensure that the entire company has been notified of the disaster.

The best and/or most practical means of contacting all of the employees will be used with preference on the following methods (in order):

- E-mail
- Skype
- Telephone to employee mobile phone number
- Telephone to employee home phone number

Communicating with Clients

In the event that this plan is invoked, it will not affect clients using our service. Notification will be made available on SDSL website and a status email will be sent via Mailchimp to our current clients. Inbound and outbound calls will be made and received through the main business phone number (01689 661030).

Dealing with a Disaster

BCP Activation

When the decision is formally made to invoke this plan, we will communicate to the rest of the organisation by email, phone call and/or verbally.

From this point all or some staff will be sent home or requested to stay at home until such time as the organisation sees it safe to return to the company premises.

Internal Communication during the Disaster

All methods available in "normal" daily operation remain open to all employees during the invocation of this plan and will be used with preference on the following methods (in order):

- VOIP Phone
- E-mail
- Helpdesk Ticket System
- Skype
- Telephone to employee mobile phone number
- Telephone to employee home phone number

External Communication during the Disaster

All methods available in "normal" daily operation remain open to all employees during the invocation of this plan and will be used with preference on the following methods (in order):

- VOIP Phone
- E-mail
- Helpdesk Ticket System
- Skype
- Personal Mobile Phone

Business Continuity Standard Operating Procedure

PC's and Laptops

1. All users have confirmed access to a PC or Laptop and have internet access
2. All users have the correct (tested) configuration file loaded on their allocated machine
3. All users will connect to the same remote desktop solution as they do in the office
4. 2FA is in place in the same way as it is used while in the office
5. All applications are presented in the same way as when in the office.
6. Printer redirection is enabled for those that still require this

Phones

1. IP phones can be taken from the office and plugged in at home, configuration is automatic
2. All internal and external calls are the same as when in the office
3. All hunt groups work the same as in the office
4. All mobile phones are configured with the mobile App (Android and IOS)

Seeding Services

Due to the specific nature of the COVID-19 pandemic and following the advice of the Government, Safe Data Storage has adapted our seeding service to fit in with the recommended measures.

To further protect our staff and our clients, we are ceasing the use and transportation of physical media for backup and restore seeds, this includes sending our staff to the datacentre and a home based service that were implemented as an interim measure. Our service will remain free but will now occur over an SFTP connection opposed to the physical shipment of seed drives for both upload and download services.

Until further notice or until such time as the Government see's fit to significantly relax the lockdown rules, all tickets that are logged for seeding services will be provided with the details from us to connect and upload or download the data to us over SFTP.

The only exception to this would be in the case of the "end client" of SDSL or our wider Reseller Network being in the Education, Charitable, Government or Healthcare sector. If deemed by the Managing Director of Safe Data Storage that a specific scenario or circumstance requires physical media then he, alone has the choice to do so.

Plan Testing and Maintenance

Testing

All users have tested access from home within the last 2 months and most users have worked from home within the last month at some time.

Maintenance

All systems that are in use are BAU systems, these are patched for service packs and hotfixes on a bi-monthly basis and antivirus / malware is updated as it is released.