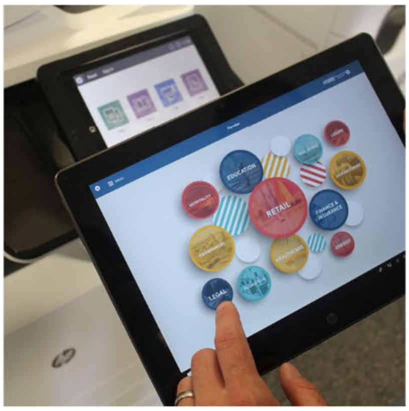
APOGEE
An HP Company

Apogee Business Continuity Plan



March 2020

Speak to us today
0345 300 9955
info@apogeecorp.com

More information at
www.apogeecorp.com

Introduction

Apogee is committed to ensuring we adequately assess business continuity risk on an ongoing basis. This document establishes our approach to identified risk and our mitigation approach, the specific actions taken should such an event occur and the hierarchy of responsibility for action.

The term *disaster* is used to represent natural disaster, human-made disaster, and any other event leading to significant business disruption.

Business Recovery Team

The recovery team consists of the following personnel;

Mark Smyth	Operations
Gary Downey	Marketing & Communications
Steve Shaw	HR
Simon Green	Information Technology

Authority for this Plan

This plan has been approved by the following personnel;

- ➢ Board of Directors

Objectives of this Plan

The objective of the plan is to ensure any disruption to the business is reduced to a minimum by performing the immediate action drills contained herein

Scope of Disasters and Failures covered by this Plan

All threats share a common impact in that they have the potential to damage our organisational infrastructure, operations and services to clients;

- Earthquake
- Fire or Flood
- Disease, Infection and Pandemic
- Cyber Attack or IT systems failure
- Theft, Sabotage
- Utility Outage
- Terrorism

Business Continuity Planning

The following outlines the key areas of the business that may be affected by a disaster with the levels of continuity planning in place.

Computer Systems & IT Services

Local servers are located at Apogee Maidstone & Lincoln offices. All servers are backed up locally to ensure minimum loss of data. All data centres are provided with UPS power and backup power generation to ensure that there is continuity of service in the event of loss of mains power.

Data Backups

Back-ups are instantiated to a backup environment hosted at both Lincoln & Maidstone offices. All servers operate in virtualised environments with VM snapshot backups performed at intervals to meet organizationally agreed RPO/RTO targets. Automated replication of VM data is performed on completion of snapshot creation. Tape backups are taken on a daily basis and operate on a grandfather, father, son rotation scheme with monthly backups retained on a permanent basis. All backup tapes are removed from site on a daily basis and stored in an off-site location with 24x7x365 secure access.

Disaster Recovery Location

The disaster recovery locations are based in Leeds (3rd Party), Maidstone & Lincoln.

All VM images are replicated on an automated basis to the above locations in a ready state such that they can be invoked on demand based on pre-defined failover plans.

Loss of Power

Maidstone – Managed Service Operations Centre

Essential services covered by the UPS are:

- Data Centre
- Telephone system
- Wireless connectivity across the site

Lincoln – National Logistics Centre

Essential services covered by the UPS and backup power generation are:

- Data Centre
- Telephone system
- Wireless connectivity across the site

Loss of Telecommunications

In the event of the loss of the telephone services into the Managed Services Operations Centre, a procedure is in place for inbound calls to be diverted to alternative locations. The primary failover site for customer service calls is the Lincoln office with Anasacom (3rd party) configured to provide interim continuity whilst service migration occurs.

Fire

The Maidstone and Lincoln sites are protected by a fire alarm system throughout all office areas. The alarm systems is monitored by a third party provider and manned 24x7x365. The Maidstone office is also equipped with fire extinguishers and trained fire marshals are on duty during normal working hours. The site is manned during normal working hours. Lincoln main data centre is protected with a fire suppression system.

Health and Safety

Health and Safety training is carried out as part of the induction program for new staff and all necessary training is provided to staff working in the organisation. Risk Assessments are continually carried out via our Health and Safety Manager as part of our business-as-usual activities.

Access to sites

Apogee liaises with local authorities in order to minimise any disruption caused by road, gas or electricity works which could possibly cause problems with access to site premises.

Building Redundancy

In cases of restrictions to access to our physical sites we have contingency plans to ensure continuity of service;

Maidstone – Managed Service Operations Centre

IT systems and SIP based telecoms services are available from all Apogee locations and via established remote access protocols. Staff will be redirected to appropriate Apogee office locations or requested to work from alternate locations (home) during the interruption.

Lincoln – National Logistics Centre

IT systems and SIP based telecoms services are available from all Apogee locations and via established remote access protocols. Staff will be redirected to appropriate Apogee office locations or requested to work from alternate locations (home) during the interruption.

Stock distribution will be dispatched from key supply chain partner facilities. PDI activities will be transferred to one of two key supply chain partner facilities.

Nationwide - Branch Offices

IT systems and SIP based telecoms services are available from all Apogee locations and via established remote access protocols. Staff will be redirected to appropriate Apogee office locations or requested to work from alternate locations (home) during the interruption.

Site Security

The Maidstone operations centre is monitored by security systems including closed-circuit television 24 hours per day. Site security is provided by a third party Centre Management function with access to the site controlled via a pin environment.

The Lincoln site is monitored 24 hours per day with third party response to site in the event of an alarm condition.

Local offices are securely locked when unmanned and access is available to key holders only. Access to the sites is provided only when the sites are manned to allow access and egress of delivery vehicles.

The larger local offices are provided with security systems including closed circuit television which monitors sites 24 hours per day.

All local offices have security intruder alarms installed with links to BT Redcare alarm services.

Insurance

Apogee is comprehensively covered by all required insurance and buildings insurance on all its sites.

Stock is insured according to agreements concluded with individual clients. In some cases clients insure their own stock under third party all risk insurance.

In other cases, Apogee insures clients stock through our own insurers. These agreements are concluded as part of the original negotiations with clients when concluding the contract between Apogee and the client and form an integral part of the client’s contract with Apogee.

Delivery/Engineer Vehicles

Delivery vehicles are provided by two outsourced vehicle services providers. In the event of a delivery vehicle failure, break down or being involved in an accident, the service replacement vehicle is dispatched as soon as possible to collect the freight and deliver it to its destination. A pool of engineer vehicles are maintained for emergency use with this supplemented with hire vehicles as necessary.

Staff Unavailability

Staff, including both office based teams and field based support resources e.g. Engineers, Professional Services may be unavailable for a number of reasons, including:

- Significant loss of life (e.g. through fire, explosion)
- Widespread failure of public transport (e.g. industrial action or major incident)
- Adverse weather conditions
- Widespread illness (e.g. pandemic)
- Mass resignation or other form of industrial action

With regard to administrative staff we support multi-disciplinary training and therefore have resilience to staff shortage. In this event key business processes would be transferred to the appropriate staff in an alternative location. We have established relationships with external temporary staff agencies and may choose to supplement permanent staff as appropriate with temporary workers.

With regard to our field service team our engineer coverage overlaps extensively. In the event of staff shortage, engineering activities would be reallocated to the appropriate resources. We further have access to a pool of engineering resource via our recruitment department and established relationships with external temporary staff agencies and may choose to supplement permanent staff as appropriate with temporary workers.

General Plan of Action

The following steps must be followed at all times:

1. Alert Stage – notification received of a disaster or failure

2. Invocation Stage – enable an assessment of the situation

3. Immediate Action Drill – appropriate action taken

4. Restoration Stage – once the disaster or failure has been satisfactorily resolved business functions to be restored to normal.

Alert Stage

This encompasses the notifications and raising of the alarm in the event of a disaster or failure and contacting key personnel. In the event of a disaster or failure outside of normal business hours, on-site security guards will contact the business recovery team immediately. An action task list for the Alert Stage will commence as detailed below;

Action Task	Title	Responsible
Co-ordination Alert 1	Receive notification of a disaster or failure	Simon Green (Steve Shaw)
Co-ordination Alert 2	Request Zoom conference call with BCP response team	Simon Green (Steve Shaw)

Invocation Stage

The objectives of the invocation phase are to enable an assessment of the situation to be made in order to:

- Decide whether to declare a disaster or failure
- Declare the type and degree of the disaster or failure
- In the event of a serious disaster or failure, to activate the relevant Immediate Action Drills.

Action Task	Title	Responsible
Co-ordination Invocation 1	Assess and categorise	BCP Response Team
Co-ordination Invocation 2	Agree appropriate response	BCP Response Team
Co-ordination Invocation 3	Instruct relevant Immediate Action Drills	BCP Response Team

Immediate Action Drills

Once the degree of the disaster or failure has been assessed, the business recovery team will take appropriate actions to secure and reintroduce key business functions and supporting services.

Action Task	Title	Responsible
Co-ordination IM Drill 1	Relocate physical operations due to site failure	Mark Smyth (Simon Green)
Co-ordination IM Drill 2	Invoke IT Services Failover to alternate data centre	Simon Green (Mark Smyth)
Co-ordination IM Drill 3	Reallocate Business Processes to alternate location	Mark Smyth (Steve Shaw)
Co-ordination IM Drill 4	Reallocate staff to alternate location	Steve Shaw (Mark Smyth)
Co-ordination IM Drill 4	Deploy/recruit additional staff	Steve Shaw (Mark Smyth)

Restoration Stage

After the disaster or failure has been satisfactorily resolved, the BCP Response Team will meet and direct that:

- Business functions must be restored to normal
- All IT Services fail back to original data centre
- All equipment specifically allocated to contingency for a disaster or failure is recalled.

Action Task	Title	Responsible
Co-ordination Restoration 1	Relocate physical operations back to original site	Mark Smyth (Simon Green)
Co-ordination Restoration 2	Failback IT Services	Simon Green (Mark Smyth)
Co-ordination Restoration 3	Reallocate Business Processes to original location	Mark Smyth (Steve Shaw)
Co-ordination Restoration 4	Reallocate staff to original location	Steve Shaw (Mark Smyth)
Co-ordination Restoration 5	Assess staff requirement and right-size	Steve Shaw (Mark Smyth)

Document History

Issue	Date	History
Rev 1	May 08	Initial release
Rev 2	Dec 11	Addition of staff unavailability
Rev 3	Sept 15	Updated to Maidstone MSOC
Rev 4	June 16	Updated to reflect Maidstone infrastructure changes
Rev 5		Updated IT DR
Rev 6	Sept 17	Updated to reflect retirement of Dunstable National Logistics Centre and introduction of Lincoln.
Rev 7	Mar 20	Updated to reflect SIP telecoms and mobile working arrangements.