BUSINESS CONTINUITY / DISASTER RECOVERY PLAN

PROCEDURES TO BE TAKEN IN THE EVENT OF A DISASTER AFFECTING THE RUNNING OF THE BUSINESS

Contents

V 1 . 3

Failure scenarios

This table represents the effect of certain scenarios

Failure Scenarios	Dependency	Failure Event	Duration	Probability	Criticality
1-A	Infrastructure Supplier	Water Supply Outage	Immediate	2	2
1-B	Infrastructure Supplier	Water Supply Outage	Short-term	2	3
1-C	Infrastructure Supplier	Water Supply Outage	Intermediate	1	4
1-D	Infrastructure Supplier	Water Supply Outage	Long-term	1	5
2-A	Infrastructure Supplier	Power Supply Outage	Immediate	4	4
2-B	Infrastructure Supplier	Power Supply Outage	Short-term	3	5
2-C	Infrastructure Supplier	Power Supply Outage	Intermediate	2	5
2-D	Infrastructure Supplier	Power Supply Outage	Long-term	1	5
3-A	Infrastructure Supplier	Phone Line Outage	Immediate	4	4
3-B	Infrastructure Supplier	Phone Line Outage	Short-term	3	5
3-C	Infrastructure Supplier	Phone Line Outage	Intermediate	2	5
3-D	Infrastructure Supplier	Phone Line Outage	Long-term	1	5
4-A	Infrastructure Supplier	Loss of Internet Connection	Immediate	4	4
4-B	Infrastructure Supplier	Loss of Internet Connection	Short-term	2	4
4-C	Infrastructure Supplier	Loss of Internet Connection	Intermediate	1	5
4-D	Infrastructure Supplier	Loss of Internet Connection	Long-term	1	5
5-A		Building Loss	Immediate	2	4
5-B		Building Loss	Short-term	1	5
5-C		Building Loss	Intermediate	1	5
5-D		Building Loss	Long-term	1	4
6-A	External Supplier	Web Hosting Loss	Immediate	3	5
6-B	External Supplier	Web Hosting Loss	Short-term	2	5
6-C	External Supplier	Web Hosting Loss	Intermediate	1	5
6-D	External Supplier	Web Hosting Loss	Long-term	1	5
7-A	Hardware Stock	Hardware Loss	Immediate	4	1
7-B	Hardware Stock	Hardware Loss	Short-term	3	1
7-C	Hardware Stock	Hardware Loss	Intermediate	2	2
7-D	Hardware Stock	Hardware Loss	Long-term	1	2
8-A	Employee	Employees cannot get to work	Immediate	3	2
8-B	Employee	Employees cannot get to work	Short-term	2	4
8-C	Employee	Employees cannot get to work	Intermediate	1	5
8-D	Employee	Employees cannot get to work	Long-term	1	5

APLHealth™

Continuity Plan Checklist

Incident	Preventative measure in place	Plan in place
Fire	Fire plan available	
Flooding	Risk of flooding from weather/roof only – negligible	
Burst Pipes	Stop tap in kitchen	Notify landlord
Electrical Failure	Phones not available but main system still working. Single phone line available on site	Contact service provider.
Burglary/theft	Security lock on doors. Alarm systems with individual codes and entry log	
IT Issues	All IT issues contact Impactus	
Data Recovery	Data storage and backup managed by Impactus	
Premises denial of access	See burglary / theft	
Illness	Most jobs are able to be covered by other members of staff.	
Loss of Key personnel	Staff aware of each other's duties and kept up to date on workload.	
Adverse Weather	Most staff have the ability to access critical systems from a remote location.	
Breakdown of key equipment	Impactus	
Loss of key supplier	Backup suppliers available	
Professional indemnity claims	Insurance	
Product complaint issues	Eod system	
Terror threat	Negligible	

APL Health™

Plan Locations – electronic	Local copy on server, copy on web server.
Plan Locations – Hard Copy	External hdd or NAS setup held by Company secretary: David Wiles ALT: Max Tebbitts solicitor Local copy held in firesafe.
Date annual review scheduled	1st August
Person responsible for activation decisions	Harry Cramer
Person responsible for review	Harry Cramer
Staff education plan in place	Harry Cramer
Person responsible for training	Harry Cramer
Person responsible for plan contacts update	Harry Cramer
Emergency pack locations	Offsite +onsite locations
Temporary relocation address(es)	Core systems accessible from home, telesales will need relocation.
Fire action plan/role/procedure locations	On site/ with documentation
Person responsible for fire risks assessment	Aimee Hulme
Person responsible for health and safety	Aimee Hulme
Location of fire evacuation point	Front door
Location of assembly point	Car park
Person responsible for building maintenance	Harry Cramer
Location of water mains stop tap	Disabled toilet
Location of mains electricity switch	Outside kitchen
Location of mains gas stop tap	n/a
Location of mains water externally	Outside
Location of nearest hydrant	Outside
Age and condition of plumbing/heating	Heating electric, recently developed last 10 years.
Trained first aider(s)	Nick Baldwin, Gareth Venn, Chloe Hulme
Key-holder(s)	Harry Cramer, Chloe Hulme, Jack Marshall, Gareth Venn
Person responsible for IT backup	Impactus, details covered later in this document
Location of backups	Server room + offsite location
Location of backup critical documentation	Server room + offsite location
Critical IT Systems	Impactus
Critical key equipment	Impactus
Key suppliers	Listed in following table
Key suppliers alternatives	Gradwell backup - Sipgate
Emergency communication methods	Company Mobile/emails. Home phone numbers
Flood risks assessed	Negligible

APLHealth™

Company Details

Office Address(s)
APL Health

9 Brunel Court

Gadbrook Park

Northwich

CW9 8QB

Personnel Contact Information

Name	Work / personal Mobile	Email address
Harry Cramer	07973416768	harry.c@aplhealth.com
Judy Topping	07511996700	Judy.t@aplhealth.com
Aimee Hulme	07772404544	Aimee.h@absenceprotection.co.uk
Chloe Hulme	07881097790	Chloe.h@absenceprotection.co.uk
Daniel Condren	07432603350	Daniel.c@absenceprotection.co.uk

Services

Facility	Firm (Customer No. /Reference No.)	Contact Number
Computer Systems	Impactus	01565 760 050
Telephone Line Redirect	Impactus	01565 760 050
Telephone	BT Business	0800 783 3749
Broadband	BT Business	0800 783 3749
Leased Line	BTnet	0800 707 6315
Data Protection	See data policy	0303 123 1113
PI Insurance	Hiscox	020 744 86000
Office Insurance	Hiscox	020 744 86000
Accountants	Helliwell Handscomb	

Electric		
Fire Extinguisher Maintenance	Walker Fire (Ref:35575)	01772 693777
Council Rates	Cheshire West	
Landlord	NA	01565 757970
Stationary	TechnoType	01565 653354
Mobiles	Vodafone	07953 966 250
Domains	Heart Internet	0845 644 7750
Alarm Company	ViewSecure	C032

Systems Requiring Login information

High Priority	Medium Priority	Low Priority
Gradwell	Gmail	Amazon
BT – leased line	COM 100 live chat visitor monitor	Ebuyer Site
Heart internet	HSBC	Aria Site
FTP Site	BT Site	Wireless Setup
TAL Site; Claims, reports, user etc	Cheshire East Council	Facebook
Domain Server	FCA Site	Twitter
Google apps	3 Mobile	
Elastix	EON Site	
EOD	Orange	
Clearbooks	Calendar	
External Backup data (password protected)	EE	
Routers/Switches		
Moneysoft Payroll		

APLHealth™

Allocation of Responsibilities

Area	Person 1	Person 2
IT Hardware	Chris Grocott	
IT Software	Chris Grocott	
Website	Chris Grocott / Harry Cramer	
Communications	Chris Grocott	
Premises	Harry Cramer	Chloe Hulme
Information	Harry Cramer	Chloe Hulme

Priorities

Below is a ranked list of systems and services and the RTO (Recovery Time Objective) for each system.

Priority Rank		RTO (Work Hours)	RTO (out of hours)
1	Main website accessible by clients	1 hour	9am next working day
2	Database and business critical systems available	1 hour	9am next working day
3	Work building accessible	24 hours	24 hours
4	Phone systems working	1 hour	Start of next working day.
5	Payroll system	By 27th of month	By 27th of month
6	Accounts	1 hour	Start of next working day
7	Banking	1 hour	Start of next working day

APLHealth™

Procedures

Loss of key personnel

Sickness/short-term

Over a short term period a member of staff's duties can be carried out by other staff in the office. Task lists can be managed by a senior member of staff and work delegated. Emails will be redirected to the appropriate person.

Permanent

Business critical data must be retrieved from the user's computer if any is stored there. Accounts to systems disabled.

Succession planning

Key roles	Criticality for cover	Criticality for replacement	Number of available staff	Replacement Source	Cover Source
Owner/Manager	1	1	0	External	Internal
Accounting	1	3	0	External	Internal
HR	3	3	0	External	Internal
Telesales leader	2	2	1	Internal/External	Internal
Claims Management	1	2	1	Internal/External	Internal/External
Telesales	4	3	0	External	NA
Claims Handler	3	2	0	External	NA
Criticality: 1: Must be ready to start immediately and take over all key responsibilities 2: Must be able to start immediately and be fully functional within 6 months. 3: Must be competent within 6 months. 4: Not essential					

All temporary cover can be handled in-house and will not need outsourced candidates.

The selection of candidates for replacement roles will be conducted through interviews. The positions will be available to current members of staff and depending on the role new people may need to be interviewed. The Telesales leader and Claims management roles will be offered to members of the respective teams if they are deemed suitable due to their knowledge of the systems and work involved. Currently, the other roles have no staff available to cover the position on a full time basis without having to recruit.

Loss of Power to building

If there is no power supply to the building calls can still be taken through a standard phone line. Website and other services are based at another location with fail safes on power supply and can be accessed from elsewhere or using mobile devices or a temporary power supply.

IT Failures

The majority of IT related hardware, software and services are managed by Impactus. The following procedures describe the actions to be taken by them on our behalf.

Backups

Backups are taken of all key systems and data relating to them on a regular basis. Key systems are backed up at the end of each working day and whenever any changes are made to the system.

Full database backups are taken every night and stored both onsite and on the dedicated server based at Heart Internet. Hourly incremental backups are also taken during working hours to ensure minimum data loss in the case of any problems. This means that the maximum amount of data lost will be up to 1 hour and in this case we have other means to track where this data would have come from and other possible sources to reconstruct from.

Complete Database loss

In the event of loss of data it can be restored from one of the backups created. This will result in up to 1 hours' worth of collected data being lost which should be easily replicated by other records kept. The backed up data must be restored to the database by being uploaded to the host using the SQL management console.

Partial Data loss

Partial data loss can be recovered through use of backups and reconstruction through data collection.

Software loss

Lost software can be replaced as the keys for all software used has been inventoried. This is all stored in a separate document.

Hardware loss
Single user workstation

Loss of a single workstation will only result in the cost of replacing the machine. No valuable data is stored on local workstations.

Mobile devices

Devices such as phones and tablets are all locked requiring a key code to enter. If one of these devices are lost the device can be remotely disabled. All of the users passwords will be changed to stop access to any emails/ systems that may have the users details saved in the device.

Laptop

All laptops are password protected. If a laptop is lost outside of the office the users accounts will be suspended and then passwords changed.

Peripherals

If a printer is made unavailable printing jobs can be sent to one of the other available printers in the office. All of the workstations are ready to use any printer.

APLHealth™

If all printers are unavailable logs of print jobs will be kept in emails and can be printed when a printer becomes available.

Routers and networking hardware will need replacing with similar products and to be configured. This involves purchase of new 'off the shelf' hardware and minimal configuration.

Phones
Server
Ready configured backup server available to be plugged in immediately. Hard drive from old server can be checked for retrievable data if functioning/available. All settings on backup updated once a month to ensure latest settings and add and changes made.

Line
Phones system runs through a BT leased line with 24/7 support available in the event of failure BT must be contacted to resolve issues. Phone server gateway can be transferred to backup broadband service and limit maximum calls to 3 at any one time to reserve bandwidth and preserve phone line quality. Log into service provider (Gradwell) to change the IP to backup broadband.

Services
If the Gradwell service becomes unavailable switch to alternate trunk using SIPgate and redirect all incoming calls to the normal phone line. Instruct all operators to inform any incoming callers that the calls are not being recorded at this time.

Hardware
Phones work through headsets attached to the users workstation or an IP phone. Each are cheap and easy to replace. Main phone line router is a CISCO unit provided by BT and if it stops working contact BT and follow same steps involved with line failure.

CISCO router gets NAT capabilities through an ASUS router a backup device is available to replace this if needed. If both are unavailable a similar device can be obtained from most IT hardware retailers.

If switch or other networking devices stop functioning preconfigured backup devices are ready or are easy to obtain.

Software
Software used on each workstation is Zoiper. This can be reinstalled easily on any new machine with little setup required.

Internet connection
Connection provided by BT Business. Excluding internal hardware faults BT must be contacted to resolve issues.

Backup broadband line available.

Hosting
Website hosting provided by Heart Internet using a dedicated server if this service becomes unavailable a secondary account is available to switch straight to. A redirect will be placed on the domain through hearts control panel.

If all hosting services become unavailable a redirect can be placed and the website hosted in-house or using another hosting company.

System hacked

If data has been lost/tampered with it can be replaced using a backup. Look into causes and step up security measures where required.

FTP Compromised

Check all available logs (system/user) If needed call security contractor. Change all passwords and check system stability and data.

Web server

Check all available logs (system/user) If needed call security contractor. Change all passwords and check system stability and data.

System password

Change password and educate users on the importance of security.

Brute force attack

Web server has protection against this that blacklists the IPs any attempt made to brute force the system.

DDos

Web server has protection against this that blacklists the IPs of any attempt made to DDos the system.

Email address compromised

Lock email account from administration panel and change passwords following security checks.

Payroll system

Backups kept on server and external media backups taken and kept off site. Backups are taken whenever data has been changed and can easily be restored from one of the backups taken.

Accounting /Banking

The majority of accounting/banking systems are handled offsite and will need internet connection to access.

APLHealth™