Business Continuity Policy & Procedure (incorporating IT contingency plans)

Compass Disability Services

Units 11 – 12 Belvedere Trading Estate
Taunton, TA1 1BH
August 2015
Review Date: August 2020

Introduction

Compass Disability Services' Business Continuity Policy and Procedure sets out how the organisation would continue operating in the event of an emergency or disaster such as an office fire, explosion, robbery, terrorist attack, extreme weather conditions or other event beyond the control of Compass Disability Services or its employees. In the event of an emergency or disaster it is imperative that Compass Disability Services is able to maintain its contractual responsibilities.

Policy Statement

Compass Disability Services takes business continuity planning extremely seriously and is committed to dedicating an appropriate level of time to planning for instances that may be beyond our control. We aim to ensure that the responsibilities of the organisation are able to be maintained within the minimum amount of time, with minimal disruption and at minimal cost. It is expected that the organisation would resume usual service within 36 hours of any major disruption to our IT systems and/or premises.

The core functions and contractual responsibilities of the organisation and safety of our staff will take priority, these are:

- The whereabouts of our lone workers and ability to maintain contact with them if they are lone working
- Informing office based staff about the disruption to usual practices and guidance on procedures to follow
- Provision of Support Services
- Payroll and Managed Accounts Services
- Meeting room– For example contacting people that have meetings already booked
- Consultation meetings – For example informing people about changes to meetings already organised

Insurance

Compass Disability Services' Employers Liability Insurance will always include indemnity in the event of business interruption. Currently the policy covers the organisation for the increased cost of working in such an event, and makes provision for a claim up to £5,000,000 in an emergency situation.

Responsible Personnel

The CEO maintains overall responsibility for all the resources used within the organisation, however all managers and staff have individual responsibilities outlined below.

The Operations Manager will pass on instructions when this plan should be initialised. In the absence of the Operations Manager, the Service Manager will pass on any instruction.

Line Managers will also have responsibilities under this plan to ensure that staff are kept up to date with instructions.

Staff are expected to remain professional in their conduct and communications with external contacts.

Scope

Building Emergency (flood, fire, or other damage that makes the offices/buildings unsafe or unusable for any period of time)

In the event our current buildings were no longer suitable for use, a decision would be made by the CEO as appropriate, to utilise:

- Either Unit 11/12 or Unit 2 as preference. With the option to utilise Units 4 and 7, subject to phone and data lines being transferred as it has no external lines
- The Mendip meeting room, subject to phone and data lines being transferred as it has no external lines
- The Chief Executive Officer's residential address

Either of these sites could be used as a temporary office for any interim period. The CEO would contact our telecommunications supplier and arrange for the office phone to be diverted and temporary IT equipment could be sourced from our IT service provider on a permanent or temporary basis as required.
Should an alternative office space be required on a more permanent basis, we would seek to rent a suitable office rather than continue to operate from an unsuitable premise; however this would need to be reviewed depending on the nature of the emergency.

Should a home workers office become unusable, the line manager would allocate their work until such times that their offices become usable. Replacement equipment would be available within 72 hours.

Computer / IT emergency

Possible reasons for failure:

- Power loss (partial/total – long/short term)
- Server/Office 365 Email failure
- Theft
- Broadband failure
- Fire/flood
- National/local disaster

- Software malfunction

Warning Indicators:

- Serious/Intermittent computer faults
- Lack of power to any or all areas of the building or home office
- Telephone line failure
- Weather forecast

Areas that may be affected:

- Main offices
- Meeting Rooms
- Contact with service users/customers
- Remote worker home offices
- Electronic communications (internal/external)
- Fax facilities
- Payroll
- General office work (printing, copying, data entry etc)
- Report/project work
- Alarm systems
- Scheduled internal meetings
- Workstations

Backup Resources

Compass Disability Services operates a Windows Small Business Server, which is backed up onto a NAS drive connected to the network and is located in West Wing; with the main server housed in Unit 11 12. These backups are saved daily, with the oldest weekly backup only over written once the drive becomes full.

The following will be checked and monitored by IT Support Company to ensure availability and suitability of resources that maybe required in the event of serious IT failure

- Server
- Back-up Nas drive
- IT equipment (computers, routers, etc)

All faxes are sent via the photocopier located in Unit 11 12 which will remain on site (to enable documents to be faxed to remote staff to assist with their work). All incoming faxes are automatically diverted to finance@compassdisability.org.uk. A spare traditional fax machine is stored in West Wing for use in an emergency. All company email addresses are accessible via the internet, using the following www.mail.office365.com. An Office 365 password (4 letters 4 numbers) is required to access; which are stored securely on the server.
Assisted by our IT Support we would expect normal service to be resumed within 36 hours where possible.
Remote staff have a responsibility to maintain a printed stock of the latest version of frequently used forms.

Pre-failure Actions

If staff become aware of possible information and communication technology failure, they should inform one of the following CEO, Operations Manager, Service Manager or Development Manager.

Depending on the type and severity of failure office staff may be advised to save current and predicted work to an additional source e.g. to memory stick. Remote staff will be advised to copy and paste current documents and current versions of any document templates that they may need to their desktop. When normal service has been resumed remote staff must copy and paste any documents back to their server folders and delete desktop documents. All due consideration must be given to the protection of sensitive data when saving to alternative media.

Recovery Time

Depending on what is the cause and level of failure – once the impact on the ability to operate has been established the recovery time will be estimated by the senior member of staff present in the following order –

- CEO Office Manager
- Operations Manager
- Service Manager
- Development Manager
- Project Coordinators

Notification

If the CEO is not present, senior staff must notify the CEO of the current situation as soon as details of impact/severity are known.

All staff on site and those expected on site will be informed of the current situation; responsibility for this is with the office support staff. If remote staff are not at their home office, messages will be left on their answer phones. The Service Manager will liaise with remote staff regarding non-affected tasks and workload management.

If business is not expected to be operational within 24 hours, the CEO will instruct further communications with staff.

To enable staff to be informed regarding information and communication technology failure/interruption the staff contact and service provider contact details can be viewed by logging into Chorus.

Initial Response

Monitoring tasks

If the recovery time is expected to be less than 36 hours, resources should be monitored and staff kept informed. Staff should be encouraged if possible to carry out non-affected tasks. Office Support staff will be available by telephone to help remote staff with documents that are held in paper format in the office.

Ongoing failure tasks

If normal functionality is not expected to be possible for more than 36 hours, the CEO, Operations Manager, Development Manager and Service Manager will advise staff according to role, tasks and period of time until normal service can be resumed.

Our remote workers would be able to continue to work using their telephones and once our IT systems were recovered (within the 36 hour period) usual work for them would resume. If a problem were to arise with one of our remote workers' offices or IT equipment, any items of their urgent workload would be temporarily diverted to a colleague, and all other work would be resumed within 36 hours or as soon as possible thereafter (depending on the nature of the disruption).

If any of our IT equipment were to fail for whatever reason, we would call upon our IT support company with whom we have a service contract. We would expect that any failings or loss (i.e. theft) of IT equipment would not disrupt the work of Compass Disability Services for any more than an absolute maximum of 36 hours.

If normal service is expected to resume within 36 -72 hours, the CEO will advise staff on duties/tasks to be undertaken during this time.

Policy Revision

This policy will be reviewed every five years and amended as necessary, or earlier if changes to the operations of Compass Disability Services occur for example the successful acquisition of a new contract or in accordance with any forthcoming legislation.

All employees should pass suggestions or recommendations for the revision of any aspect of this policy through normal channels to the Chief Executive.