1ST STEP solutions limited

Business Continuity Plan

IMMEDIATE ACTIONS

Manager/Supervisor

1. Ensure emergency services contacted
2. Ensure safety of personnel
3. Co-ordinate with the emergency services
4. Contact Senior members of the company
5. Assess situation/ damage and formulate response together with Deputy
6. Allocate tasks

Deputy Manager

1. Assess damage and formulate response together with the Manager
2. Notify heads of department and instruct them to contact their staff members
3. Issue press release if appropriate

Admin Support

1. Restoration of services to premises
2. Source accommodation and business equipment to enable business to continue
3. Set up emergency telephone and fax lines

IT Support

1. Source replacement computer equipment
2. Source replacement telephone/communications equipment

ONGOING ACTIONS

Manager/Supervisor

1. Continuous co-ordination of Disaster Recovery Plan
2. Manage recovery and salvage operations

Deputy Manager

1. Update situation reports from emergency services
2. Liaise with Insurance Manager for provision of Loss Adjuster
3. Liaise with H & S Director for HSE issues
4. Liaise with Accountant for financial controls and measures

Admin Support

1. Source temporary storage for undamaged contents
2. Organise salvage contractors
3. Manage telephone calls from clients, staff, and press
4. Divert post to emergency centre or alternative office
5. Issue details of temporary numbers/press adverts

IT Support

Restore computer from back-up at designated emergency centre or other pre-arranged ‘hot start site’

INTRODUCTION

All organisations should prepare themselves to withstand a disaster and ensure that procedures and resources are in place to ensure that the business can continue. A successful Business Continuity Plan (BCP) depends on the implementation of a set of procedures by those in authority based on a clear understanding of their roles and responsibilities during a crisis.

A BCP is an integral part of the company's risk management programme based on continuous risk assessment that aims to:

- cope with the immediate impact of a disaster if one occurs
- minimise the severity of the disaster to the business in the short term

The BCP will:

- Give a clear definition of what constitutes a 'disaster' for the company with examples
- Identify and prioritise the company's core activities which if disrupted, even for a short period, would have serious consequences for the company's future
- Prioritise the company's activities by considering the consequences of being unable to carry them out
- Identify key resources needed to reinstate each critical activity in terms of personnel, accommodation, information and equipment
- Identify and document the actions required to overcome a disaster, in the immediate aftermath and the short term thereafter
- Identify, document and inform individuals of their roles and responsibilities after an incident occurs
- Highlight the dependencies between the different company offices and external suppliers and clients
- Provide a structured basis for testing the plan and evaluating the results
- Identify the training needs

Disaster recovery begins at the time of the event, but it is concerned with the future, and the resumption of normal operations with the minimum of delay. The back-up resources needed for recovery shall be identified at the next SMT meeting and documented here.

There are some critical factors necessary for a successful recovery operation. These are:

1. Establish an emergency centre for each location
2. Establish clear lines of communication
3. Have a clear and tested BCP in place with up to date contact details of key staff, details of vital records and readily available back-up facilities

RISK ASSESSMENT ANALYSIS

It is unrealistic for the BCP to address every risk or threat facing the company's business. It is therefore necessary to utilise a risk-based approach to ensure that this BCP addresses the threats which pose the greatest risk to our company. This section identifies the critical business processes, the impact on the business from failures of these processes and the current controls in place to prevent or mitigate such failures.

General and specific risks

The immediate threats to the business are those which are physical, e.g. fire, flood, theft, other damage, computer breakdown resulting in loss of documents etc. Also in this day and age, loss of systems and communications poses a serious risk. Likewise a long term loss of power resulting in loss of or loss of use of company premises, plus the loss of plant/vehicles and equipment and their fuel supply. There is also a location risk in itself, for example by proximity to dangerous areas e.g. railway; gasometers and the like.

Other physical threats can be similar but external to the business, e.g. long term loss of power in the area; loss of access due to illness or incident e.g. murder in the vicinity; fire at a nearby premises; industrial sabotage e.g. to systems or premises.

There is a risk to a business from unexpected Personnel changes, e.g. accident to or death of key personnel. This could be as a result of a disaster scenario or a separate incident like a car crash. In most businesses, a mass resignation for example due to a departmental lottery syndicate win would cause huge problems. There are also potential industrial disputes which could lead to mass loss of staff.

Non-tangible risks must be considered, e.g. loss of reputation which might occur due to a major business incident being reported either locally or nationally. The loss of or non-renewal of a contract, either anticipated or unexpected would lead to serious problems for the division concerned as well as the business as a whole. The possibility of non-delivery on a contract as a result of another incident, for example the loss of key sub-contractors/s and/or suppliers of any kind should also be considered.

EMERGENCY RESPONSE SCENARIOS AND REQUIREMENTS

In the event of any disaster, the designated team leader would take control and assess the scenario in the first instance. He/ She would start the communication process to team, clients etc. The key team members should be pre determined within each division or location, and as mentioned in part 1, have list of specified personnel and clients to call. It is vital that key team members each have a designated 'deputy' and vice versa, in case of absence when the disaster occurs, for example they are absent on holiday, so that the procedures do not fall at the first hurdle.

In the event of a physical disaster such as a fire, it is essential to have the emergency response contact numbers available (including our alarm company and maintenance company numbers) and evacuation procedures clearly marked in case the building is occupied at the time. Contact should be made with the local fire station and police station and preferably the name of a specific officer noted within the emergency procedures contacts. Invitations should be extended to the relevant personnel to visit the premises to assess risk and give advice where possible.

Emergency response services include not only the fire service and the like, but the contact lists must extend to include details for the provision of temporary materials, vehicles, emergency plant, and emergency equipment to minimise loss such as provision of dehumidifiers and the like, glaziers, boarding up companies, and if course loss adjusters and insurance details if not obtainable directly through liaison with the insurance department.

Consideration should be given to the purchase of a mobile telephone which is solely activated in the event of a disaster scenario for contact purposes so that there is one specific overall contact number.

In the event of loss of accommodation and facilities e.g. communication, the response will be formulated subject to the numbers of personnel affected.

Consideration should be given as to whether some or all of them could work at home with mobile telephones? If so, how long would be reasonable for this to continue?

Can some be moved to alternative local offices or other divisional offices?

Can some be moved to a client's premises, or even another local business with which we might formulate a mutual arrangement if they had a disaster scenario?

In the event that a disaster causes a long term loss of accommodation, then a knowledge is required to source local alternative premises with addresses of local agents, details of the approximate time scales to source alternative premises; the likely costs which would be immediately incurred for example if a deposit is required, plus the exploration of minimum rental times.

In the event of a loss of power or other main service, we need to establish the set up times to restore the service. A list of emergency numbers and vital information and equipment should be complied which should be kept either easily accessible but safe at each main premises, or held off premises in case of emergency. Things to be included in the items should include contract details; computer backups; spare laptop & mobile telephone; contract's personnel list and other contact details including sub-contractor and client details. These information folders could also hold duplicates of keys as well as documentation.

In the event of the loss of IT systems at head office there would need to be a designated co-ordinator within the disaster team, as per the procedure above. The procedure for bringing in the backups of information would need to be established, and the current security of backup information checked. The location of backups would need to be ascertained and checked. A test restoration from backup exercise should be carried out at regular intervals to test the integrity of the information. Serious consideration should be given to the supply of alternative equipment.

Do we have a 'hot start up' off site backup server available? Do we have spare replacement equipment, and if not should we have a small supply of emergency laptops. Consideration needs to be given to the lead in time required to repair or replace server, e.g. if there is a partial or total loss of this vital equipment. Do we have spare parts on site or at least readily available for repairs if necessary. Equally, what is the lead in time to replace PCs, printers etc. Do we have or could we acquire a 'special' client status with our computer suppliers to guarantee swift response in an emergency?

In the event of a loss of communications at head office (or any other major site), we need to have details of alternative sources for fax/telephone systems. What is the lead in time with BT or another communications provider to provide temporary number/s, and to instigate a recorded information message on the normal line to alert callers of the circumstances and the alternative number. We need to consider the availability and cost of advertising space/radio advertising both locally and nationally to alert our clients and personnel etc of events.

In the event of loss of documents at head office (or any other major site), we need to check whether the documents can be reinstated from clients or subcontractors, insurers, computer records. However, it is to be noted that the archived documentation, unless very recent, probably cannot be restored by any means.

In the event of loss of documents such as invoices along with the computer system, this could be catastrophic. We have a high reliance on regular cash flow and thus the whole company's survival could be at risk if an efficient alternative accounts processing facility is not set up quickly (see IT requirements above). At the very least the Bank overdraft facility should be at a minimum sufficient to be able to cope with emergency payments e.g. wages. Consideration should be made to the setting up of a 'Fighting Fund' to call upon for emergency expenses. Or an amount of cash should be readily available if required.

In the event of loss of personnel, if this were a single key figure such as a company director, then a designated pre-selected deputy should be agreed upon to handle the situation. Perhaps recourse would be needed to a PR company if there is prolonged or severe media interest, to advise on strategy, statements etc.

In the event of loss of a number of staff at once, there needs to be information as to the availability of replacement personnel via local agencies, with possible time scales and costs. Personnel should have available if possible a list of job seekers or current CVs for various occupations, from agencies, or via 'on spec' applications.

In the event of loss of staff due to death, or long term illness which causes working difficulties, e.g. over 1 month, then consideration should be made to setting up 'Job Shadows'. That is, where there is a pre-selected temporary replacement should a key member of staff be absent for a long time. Other remedies include the secondment of staff from other departments/offices to cover. This could include the consideration of permanent redeployment of staff from other offices/departments as well. We should also have noted alternative sources of information, e.g. brokers, insurers, clients, suppliers etc who may be able to supply staff.

Salvage & Restoration

The final stage of the Business Continuity Plan is to determine the actions to be taken in the area of salvage and restoration. There will be a requirement within the assembled disaster team to determine the extent of the incident. This team will address both physical loss and intangible losses such as loss of reputation, future business etc. as seen in the short term aftermath. Immediately after the incident as we have seen, the team will:

- Identify the immediate loss mitigation and salvage requirements
- Prepare a plan for site safety, security and stabilisation
- Identify methods of protecting on site assets including equipment, premises, data and documentation
- Establish liaison with the company's customers, press and external agencies such as Loss Adjustors, Accident Investigators etc

After stabilising of the incident, and the establishment of an alternative work location, communications etc, attention can be turned to salvage and restoration. A degree of this can be carried out at the affected premises, e.g. storage of undamaged goods and materials, and disposal of debris etc.

The 1st Step Business Continuity Plan

In the event of fire or disaster occurring to the offices, all operations and office staff will be immediately transferred to their respective homes where the staff have their own computer access. Most of our rail consultants have their own transport and can work from the various client site offices using their own laptops. Wherever practical our other branches will manage our assignees.

The offices will be locked down and any salvageable material will be transferred to storage until re-building or refurbishment has been completed. All our existing and new clients will be informed of the new arrangements through letter or e-mail and or face to face discussions. Mail will be diverted. The majority of telephone conversations with clients are already through the mobile telephones held by all our staff and this will continue until alternate office telephone lines are installed.

In the event of temporary or permanent loss of personnel, we already have deputy arrangements in place which will continue until new staff, if necessary are appointed.

The 1st Step server is backed up externally through an external provider who also provide an emergency package that would immediately provide software as appropriate to enable continuity of access to electronic records and IT support.

Mr. Matthew Jones, and Mr Les Fillery the joint Managing Director are the persons nominated to respond to any media involvement and will co-ordinate all the transfer arrangements.

This plan will be reviewed at least annually or sooner if fire drills require it.

This policy will be reviewed annually.

Signed

Matthew Jones, Managing Director,   Les Fillery, Managing Director

April 2017