SPILL DEFENCE

MANUFACTURERS OF SPILL CONTROL PRODUCTS

Business Continuity Plan

BUSINESS CONTINUITY PLANNING PROCESS

1. Purpose of this document

Spill Defence Ltd has a duty to ensure that it continues to function in the event of an incident or damage affecting its operations. Business Continuity Planning is a planned process aimed at managing the many and varied operational risks inherent in the day-to-day activities involved in service delivery.

The main purpose of the process is to ensure continuity of delivery following an unexpected disruption to normal working. It is the Business Continuity Plan that provides the primary means of ensuring an organised and effective 'return to normality'.

Any major incident can cause significant disruption to the essential business of an organisation such as Spill Defence Ltd over weeks and months. There is a need for a robust system to ensure that essential work can be undertaken even in the most adverse of circumstances, hence the need for a Business Continuity Plan.

The Business Continuity Plan is concerned with the general operational systems and physical facilities of Spill Defence Ltd. The plan ensures that contingency arrangements are in place so that service provision can continue.

1.1 Objectives

The objectives of this plan are:
- To ensure that maximum possible service levels are maintained
- To ensure that we recover from interruptions as quickly as possible
- To minimise the likelihood and impact (risk) of interruptions

1.2 Principles

The principles behind this plan are:
- Disaster Recovery is just part of Business Continuity
- Risks are assessed for both probability and business impact
- The Business continuity plan must be reasonable, practical and achievable, in other words, we are not planning for every possibility. Diminishing returns affect the benefits of planning for extreme cases.

1.3 Functions vs Causes

We have developed this plan by analysing what is being interrupted, rather than why. For example, our office building may be unavailable for many reasons – but in terms of its impact on the operations and services of Spill Defence Ltd, it does not matter whether the cause is a failed boiler unit, or a major

external incident. Obviously, Spill Defence Ltd will manage each incident differently, depending in some cases on the cause, but for our more specific purposes, the building is simply unavailable.

2. Guide to Managers: production / use of the plan

The advantages of a planned response include:
• Identifying critical systems and information in advance of an event, so that an informed decision can be taken on the extent to which such systems should be protected.
• Defining the roles of individuals – both in terms of responding to and recovery from a disruption.
• Determining the resources required to maintain a minimum acceptable locality to the community.

The Business Continuity Plan must take account of all other relevant Spill Defence Ltd policies.
If there is any disruption to business continuity, the plan will need to be implemented. The plan deals with all aspects of business continuity and the following section outlines a six-stage process to produce a plan.

The Guide examines two potential scenarios: -
• The disruption to business continuity is relatively minor and can be handled within an individual locality and would be left to the individual manager to establish arrangements based on the plan.
• The disruption to business continuity would be significant enough to affect the whole of Spill Defence Ltd and it would be necessary to convene an emergency Management meeting.

Arrangements should be made for the annual review and updating of the Business Continuity Plan and appropriate information will be provided to the Company Directors. The Spill Defence Ltd Directors will be advised that a system is in place for Business Continuity.

3. Activating and using the Plan in the event of disruption

Reaction management will be invoked whether there is an unscheduled interruption to the provision of core or service delivery, or business processes and a decision will be taken whether to use Business Continuity Plans. An incident arises whenever an unanticipated situation occurs which causes an interruption to essential core or localities systems or business processes.

3.1 Triggers for the Plan

The key to success is the flexible use of staff and other resources. The following table lists example events, which may serve to trigger business continuity arrangements:

Interruption Service availability impaired

Threat	Likely impact
Staff shortage due to sickness	Service availability impaired
Theft or wilful damage	Confidentiality and Service availability impaired
Fire / explosion	Service availability impaired
Power failure	Service availability impaired
Water damage	Service availability impaired
Communications failure	Service availability impaired
Introduction of virus or disruptive software	Service availability impaired

Network management failure	Service availability impaired
National Emergency	Service availability impaired

3.2 Issues to ensure effective implementation of the Plan

3.2.1 Emergency Action

Ensure emergency action, where necessary, to ensure the safety of life, implementing normal Fire and Health and Safety procedures.

3.2.2 Assess the potential impact of the occurrence

If a Team Member becomes aware of information which may precipitate an incident, or is informed of an incident, they should inform the Officer or Deputy Officer. They will decide if the Business Continuity Plan needs to be activated. If the plan is activated the Directors should be informed at the earliest opportunity. Initial assessments will inform whether it is safe to continue to work and the length of time the interruptions are expected to continue.

3.2.3 Identify the options for corrective measures

These will have previously been identified and will be contained within the Business Continuity Plan, although it must be accepted that all eventualities cannot be anticipated.

3.2.4 Recovery

Timescales for full recovery should be determined by the business and/or legal requirements.
Steps should be taken to ensure that the restoration of full services considers any changed circumstances.

3.2.5 Return to Normal Working

The decision to return to normal working will be based on information received and will be made by the Management Team and or the Directors. It is the responsibility of The Management Team to ensure that the information is cascaded to the staff involved.

3.2.6 Debrief and Review

It will be the responsibility of the Management Team to conduct an evaluation following an incident, which will obtain the views of all staff involved, in relation to the following issues:
- The reasons for the incident
- The effectiveness of the Business Continuity Planning arrangements
- The management of the recovery
- Lessons learned from the events and reassessment to identify any new threats or hazards.

The outcome of the evaluation will be shared, and lessons learned will be reflected in subsequent training and revisions to the plan.

Reports will be prepared for and by the management team and circulated to the Spill Defence Ltd Directors.

4. Roles and responsibilities of the Spill Defence Ltd, Managers and Staff

This section sets out the roles of the various Spill Defence Ltd teams and individuals and lists the actions needed to ensure that the plan will work in practice. It focuses on the need for testing, training, audit and review.

4.1 Responsibilities in relation to the Business Continuity Plan

• Officer
or their deputy have overall responsibility for business continuity arrangements.
• Directors
will need to be assured that the business continuity arrangements are robust and effective.
• Management Team
will have overall responsibility to support the Officer and to oversee the implementation and effectiveness of plans within their areas of control. They will be responsible for the management of incidents which impact on their area of work. They will be involved in initial evaluation, be responsible for assessing the status of the incident and be able to escalate to senior level. The task of developing, maintaining and reviewing business continuity plans is undertaken by the management team.
• All Staff
will potentially be involved in the implementation of business continuity plans and must therefore be aware of the process and the arrangements within their area of work.

4.2 Action to ensure effective implementation

4.2.1 Testing the Plan

The plan should be easily accessible and available its contents and procedures must be made known to all key staff.
The contingency element of the Plan should be tested at least annually. Regular reviews should be undertaken to ensure the plan is up to date and effective; and, to ensure all staff are aware of the plans. Testing should be scheduled and conducted in a way that does not put essential business functions of the organisation at risk. The testing methods should be practical, cost effective and appropriate and designed to promote confidence.

4.2.2 Training

Training should be undertaken to ensure that staff have the right skills and knowledge to undertake the roles expected of them in the event of a failure.

4.2.3 Review

Business Continuity Plans should be reviewed annually by the management team and by the Directors at least every three years to ensure that they remain current and viable and take account of any organisational changes.

5. Business continuity charts

The table below indicates the charts completed for the plan.

	Chart section	Instruction
1	Risk Assessment	Conduct a Risk Assessment in accordance with instructions in risk management policy.
2	Essential Functions	Define essential functions for each team and the minimum necessary staff.
3	Essential accommodation	Detail accommodation, office equipment and telephones required as essential for teams.
4	Essential IT and Manual Records	Detail the IT facilities and manual records required for the essential function of teams.

The items below form a part of the plan but are maintained on the server		
-	Staff Contact Details. Includes Directors and applicable personnel	Ensure that there is a register of all staff, giving details of how they may be contacted. This is maintained on the server.
-	Key contacts – External	Ensure that a key contacts list is maintained for external people and their role in an emergency. This is maintained on the server.

Chart 1 is a risk assessment of a broad range of possible scenarios which could affect business continuity. For information the three-part guide for calculating risk rating(s) from the risk management policy is included here.

1 Likelihood of an incident occurring

Level	Likelihood of Occurrence	Details / Description
1	Rare	Very unlikely this will happen
2	Unlikely	Unlikely to happen again but is possible
3	Possible	May reoccur occasionally
4	Likely	Not persistent but probably will reoccur
5	Almost certain	Persistent and likely to reoccur

2 Consequence of an incident occurring

Level	Consequence	Details / Description
1	Insignificant	No injuries - No treatment /intervention required/given No loss/reduction of capacity to deliver service Low financial loss/cost
2	Minor	First Aid Treatment required/given Reduced capacity to deliver service Medium financial loss/cost
3	Moderate	Medical Treatment required/given. Assistance required to deal with reduced capacity to deliver service Medium financial loss/cost
4	Major	Extensive injuries. Temporary loss of capacity to deliver service Major financial loss/cost
5	Catastrophic / Death.	Long term/permanent loss of capacity to deliver service High financial loss/cost

3 Matrix for calculating the level of risk attaching to an incident

Likelihood	Consequence				
	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5

5	H	H	E	E	E
4	M	H	H	E	E
3	L	M	H	E	E
2	L	L	M	H	E
1	L	L	M	H	H

Risk Rating
Red = Extreme
Orange = High
Yellow = Medium
Green = Low

Chart 1: RISK ASSESSMENT - THREAT TO BUSINESS CONTINUITY

The following table contains the assessment of risk which relate to Spill Defence Ltd, where the Risk is a function of Likelihood and Consequences (R = L x C)

Hazard	Risk	L	C	Risk	Controls currently in place (if any)	Action needed
Unidentified factors effecting delivery of our services	A major unidentified problem could disrupt or stop the delivery of work	1	3	3	Risk assessments are undertaken on activities and risks are managed through various internal processes e.g. management meetings, management review meetings. Spill Defence Ltd have a proactive approach in delivering projects and ensures that robust systems exist to counter problems	Risk and Risk Management is always considered as part of the Management / Governance process
Failure to meet milestones/ outcomes	Failure to deliver would Impact on the financial constraints	1	4	4	All activities are monitored against targets / outcomes and appropriate steps taken if necessary	Spill Defence Ltd Management will monitor progress against targets / outcomes to ensure activities are meeting expectations
Competition	Inability to compete	1	2	4	Spill Defence Ltd is currently a strong organisation that can react to competition. Spill Defence Ltd will continue to maintain high quality Governance, Management and provide a quality service.	Given our industry we work throughout the competition from another organisation is likely. This must be monitored constantly.
Hazard	**Risk**	**L**	**C**	**Risk**	**Controls currently in place (if any)**	**Action needed**
Negative publicity/ coverage	Impact on Clients	1	5	5	All activities (publicity) from internal sources are monitored against required targets / outcomes and appropriate steps taken if necessary. Activities (publicity) from external sources are monitored and appropriate steps taken if necessary	Any complaint that is made must be assigned to the appropriate manager and dealt with at the earliest opportunity.
Damage to Spill Defence Ltd image/ reputation/brand	Impact on Clients	1	5	5	All activities from internal sources are monitored against required targets / outcomes and appropriate steps taken if necessary. External sources are monitored and appropriate steps taken if necessary	

Pressure group protest	Impact on Clients and the local community	1	1	1	Spill Defence Ltd has good systems in place for working with its clients and it is highly unlikely that this situation could occur. Action from a group not associated with Spill Defence Ltd would be handled by a member of the management team in a manner which reflects the actual situation. Clients shall be informed	
Key Management staff leave	Loss of continuity in delivering core services / project management	2	4	8	Spill Defence Ltd has good internal support mechanisms for staff and a fairly low staff turnover for key positions.	Ensure that management staff are valued and continue to receive the support needed to deliver the project
Key Management staff are ill / absent (Short Term)	Loss of continuity in delivering core services / project management			6	Spill Defence Ltd has good internal support mechanisms for staff and a low staff turnover	Ensure that staff are valued and continue to receive the support needed for project / service delivery
Hazard	**Risk**	**L**	**C**	**Risk**	**Controls currently in place (if any)**	**Action needed**
Key Management staff are ill / absent (Long Term)	Loss of continuity in delivering core services / project management	2	3	6	Spill Defence Ltd has good internal support mechanisms for staff and a low staff turnover. Key members can also support the role of Key management.	Ensure that staff are valued and continue to receive the support needed for project / service delivery
Key staff leave	Loss of continuity in delivering services	2	3	6	Spill Defence Ltd has good internal support mechanisms for staff and a low staff turnover. Employ and train multi skilled personnel.	Ensure that staff are valued and continue to receive the support needed for project / service delivery
Key Staff are ill / absent (Short Term)	Loss of continuity in delivering project	3	1	3	Spill Defence Ltd has good internal support mechanisms for staff and a low staff sickness absence rate. Employ and train multi skilled personnel.	Ensure that staff are valued and continue to receive the support needed for project / service delivery
Key Staff are ill / absent (Long Term)	Loss of continuity in delivering project	2	3	6	Spill Defence Ltd has good internal support mechanisms for staff and a low staff sickness absence rate. Employ and train multi skilled personnel.	Ensure that staff are valued and continue to receive the support needed for project / service delivery
Industrial action	Loss of continuity in delivering project	1	1	1	Spill Defence Ltd has good internal support mechanisms for staff and a high loyalty rate. Employ and train multi skilled personnel.	
Employee health and safety	Health and Safety Incident	2	3	6	Active Spill Defence Ltd Health and safety policy procedures and associated investigation.	See also Health and Safety Policy and records of checks etc,
Client health safety issue/incident	Health and Safety Incident	1	2	2	Active Spill Defence Ltd Health and safety policy as above.	See also Health and Safety Policy and records of checks etc,
Loss of Electric (Internal)	No lights, sockets, IT, heating	3	4	12	Ensuring electrical power equipment is safe. Get competent advice to avoid overload situations. Five yearly periodic inspection and test completed as per the requirements of BS 7671. Pat Testing	See also Health and Safety Policy and records of checks etc,
Hazard	**Risk**	**L**	**C**	**Risk**	**Controls currently in place (if any)**	**Action needed**

Loss of Electric (External)	No lights, sockets, IT, heating	2	4	8	None Unplanned outages do occur but overall are rare, supply is on average available for 99.9% of the time.	Given our location it is likely that a widespread fault would be resolved quickly (1 hour).
Loss of Telecommunications (Internal / External)	No telephone services (including Broadband connectivity)	2	2	4	Contact our IT support team and telephone provider. Key personnel. Key contacts backed up to cloud and also suppliers/clients available via sage which is installed on the account's employee PC at their place of residence.	Key personnel are issued company mobile phones.
Loss of Broadband	No broadband Connectivity.	2	2	4	In the first instance our broadband supplier should be contacted. Key personnel may access via VPN and using tethering.	
Loss of Heating	No Heating	2	3	6	Would only be a problem for part of the year.	Regular Maintenance of boiler unit and associated equipment by the landlord. Available supplementary heating. An extended outage would require additional supplementary heating which may need to be a mix of gas/electric units, otherwise overload may well occur of the existing electric circuits.
Loss of Water (Internal)	No water for ablutions, general cleaning or refreshments	1	2	2	Regular maintenance of plumbing system.	Bottled water is available.
Loss of Water (External)	No water for ablutions, general cleaning or refreshments	1	2	2	None	
Hazard	**Risk**	**L**	**C**	**Risk**	**Controls currently in place (if any)**	**Action needed**
Sewage ingress	Contamination of workspace, equipment and materials	1	3	3	Regular cleaning maintenance of internal system.	
Vermin	The external areas and workshop can be used by rats and vermin	3	2	6	Good hygiene practices in food preparation areas. Ensure that waste bags are secured and stored in a secure container.	Prompt disposal of food wrappers etc Contact a vermin control officer is any vermin is seen or suspected.
Fire		3	5	15	Fire inspections / drills, periodic checks in accordance with health and safety policy	See also Health and Safety Policy and records of checks etc
Theft	Personal belongings or property may also include vandalism	2	2	4	All staff to be responsible for their own personal belongings and aware of any unknown person(s) in the building. All locks to be used on all doors occupied by Spill Defence Ltd whenever a room is unoccupied. Windows to be closed when a room is unoccupied.	
Loss of premises E.G Extreme weather / flood / high winds	Loss of premises from any cause. The loss of equipment data etc is covered elsewhere	1	4	4	Reserves to cover possibility of moving to temporary new accommodation. Contingency plans for new premises. During project work being undertaken, cease work, contact appointed manager for advice.	
Hazard	**Risk**	**L**	**C**	**Risk**	**Controls currently in place (if any)**	**Action needed**

Loss of Data (IT)	Most Spill Defence Ltd data is currently held on IT systems.	1	2	2	Regular (daily) backing-up onto separate drive from server, remove from the office daily. Utilise third party backup and control / Opus IT.	—
Loss of Data (Hard Copy)	Most Spill Defence Ltd data is currently held on IT systems. Files such as personnel files and agreements are substantially hard copy			4	Efficient record keeping. Authorisations established for change control. Ensure filing systems are understandable to others. Where documents are sensitive, they should be kept in a secure locked location. Backups to cloud facility from third party (Opus IT).	Personnel hard copy is retained in one cabinet. There is a steady move towards retaining all documents as a primary or secondary document on the IT system.
Loss of access to site	E.G. Police incident restricting access. This could affect not only the actual main entrance but inadvertently if the exit routes are unavailable for emergency purposes closure may be necessary.	1	2	2	None	An assessment will need to be made at the time of any incident in conjunction with incident controller as to whether safe working and access / egress can continue

Chart 2(b): ESSENTIAL FUNCTIONS - Finance Team (Excluding Accommodation and IT)

No	Question	Answer
1	What is the essential critical/ priority function?	• To provide a financial /payroll facility for internal use • To provide a financial / payroll facility for external (Chargeable) users
2	How many staff are required, and which staff are needed for the essential service provision?	1 (variable) dependent on workload at time of incident and nature of any loss
3	Which other departments of the Spill Defence Ltd (if any) are dependent on the services provided?	All
4	Which external contractors (if any) do the essential services depend upon?	Possible IT if an IT fault None, although online access to Bank & HMRC is important and at times critical
5	Which utilities (if any) do the essential services depend upon?	• Electric • Gas (Heating) seasonal. • Water for refreshment comfort breaks • Telecoms • Sewage See also Chart 1, risk assessments, regarding these utilities. All have a high connectivity

Chart 2(c): ESSENTIAL FUNCTIONS - Site Teams (Excluding Accommodation and IT)

No	Question	Answer

1	What is the essential critical/ priority function?	The restoration of service provision
2	How many staff are required, and which staff are needed for the essential service provision?	This may vary dependent on the type of incident
3	Which other departments of Spill Defence Ltd (if any) are dependent on the services you provide?	None
4	Which external contractors (if any) do the essential services depend upon?	Possible IT (None) if an IT fault
5	Which utilities (if any) do the essential services depend upon?	• Electric. • Gas. • Water • Telecoms • Sewage See also Chart 1, risk assessments, regarding these utilities. All have a high connectivity

Chart 2(d): ESSENTIAL FUNCTIONS - Other areas (Excluding Accommodation and IT)

No	Question	Answer
1	What is the essential critical/ priority function?	None
2	How many staff are required, and which staff are needed for the essential service provision?	None
3	Which other departments of the Spill Defence Ltd (if any) are dependent on the services you provide?	None
4	Which external contractors (if any) do the essential services depend upon?	This would be dependent on the Client.
5	Which utilities (if any) do the essential services depend upon?	All utilities when undertaking operational duties. This will be discussed with the Client prior to any work being undertaken and appropriate response plans agreed.

Chart 3: ESSENTIAL ACCOMMODATION (Assumed Total loss of existing system)

Requirement	Comments	0 - 48 Hours	3 - 7 Days	Over 7 Days
Number of:				
Desks (13)	This number is based on existing usage, the actual operational requirements may vary dependent on the nature of the incident.	✔		

Chairs (13)	This number is based on existing usage, the actual operational requirements may vary dependent on the nature of the incident.	✔		
Filing Cabinets (13 * 2 drawer)	This number is based on existing usage, the actual operational requirements may vary dependent on the nature of the incident.		✔	
Filing Cupboards Large (4)	This number is based on existing usage, the actual operational requirements may vary dependent on the nature of the incident.		✔	
Filing Cupboards Medium (4)	This number is based on existing usage, the actual operational requirements may vary dependent on the nature of the incident.		✔	
		Availability required within:		
Requirement	**Comments**	**0 - 48 Hours**	**3 - 7 Days**	**Over 7 Days**
Number of:				
Additional Office Equipment (eg Photocopier)				
• **Photocopier**	The actual provision made may vary and is dependent on the actual incident		✔	
• **Printer Scanner**	The actual provision made may vary and is dependent on the actual incident	✔		
Storage Space (sq metres)				
• Minimum of 15sq meters (see comments)	This would be dependent on material / equipment salvaged and needing to be stored, it may also be dependent on need for storage of damaged items until insurance claims have been considered		✔	
• Minimum of 34000sq ft (warehouse)	All items stored in the workshop can be replaced or hired. Items that have been saved will need to be located in a safe location / storage area to prevent theft.	✔	✔	
Public Facilities (eg toilets, disabled access)				
• Toilets (3 Male 3 Female 1 Unisex)	The provision and number of facilities will very much depend on the type of accommodation secured for temporary / permanent accommodation	✔		
• Toilets (1 disabled)	The provision and number of facilities will very much depend on the type of accommodation secured for temporary / permanent accommodation		✔	

Chart 4: ESSENTIAL IT and MANUAL RECORDS
(Assumed Total loss of existing systems)

		Availability required within:		
Requirement	**Comments**	**0 - 48 Hours**	**3 - 7 Days**	**Over 7 Days**

Access to Document areas	This would be basic access one computer operating Microsoft Office 2010 and able to access backup system and internet for e-mail communications. Two – Three laptops may be 'off-site' at any time, these could be utilised for this purpose. System backup daily with external storage tapes taken off site. The system is also backed up via third party IT support (Opus IT)	✔		
Access to Document areas on the server (Management Team)	This would be basic access one computer operating Microsoft Office 2010 and able to access backup system and internet for e-mail communications. Two – Three laptops may be 'off-site' at any time, these could be utilised for this purpose. Authorisations established to prevent changes being made to key documents.	✔		
Access to Document areas on the server (Management Team)	A server would be in place and backups from the external IT support (Opus IT)		✔	
Access to Document areas on the server (Financial Team)	A server would be in place and backups from the external IT support (Opus IT)		✔	
Access to Document areas on the server (External Team)	A server would be in place and backups from the external IT support (Opus IT)		✔	
Access to Document areas on the server (All others)	A server would be in place and backups from the external IT support (Opus IT)			✔
Hardware and Networking requirements:				
PC and peripherals	Standard hardware may be purchased from local suppliers	✔		
Server fault	Company server is backed up to cloud facility via IT support. Server replace will be undertaken via out IT specialists (Opus IT).	✔	✔	
		Availability required within:		
Requirement	**Comments**	**0 - 48 Hours**	**3 - 7 Days**	**Over 7 Days**
Number of:				
Public Facilities (eg toilets, disabled access)		✔	✔	✔

Key Contacts in an Emergency			
COMPANY			
Name	**Title**	**Contact in case of**	**Number**
Mark Sanderson	Director	All emergencies	07584 685302
Mark Hutchinson	Director	All Emergencies	07584 685301
Steven Howden	Operations Manager	All Emergencies	07779 771901
Jane North	Accounts Manager	Site Emergencies	07970 843122
Joanne Sanderson	Office Manager	Site Emergencies	07584 685304
Martin Lovatt	Warehouse Manager	Site Emergencies	07584 685306