Business Continuity Management Plan

Introduction and Policy Statement

The operation of the organisations business depends on a given combination of people, processes & technology, in connection with a given set of current business assets.

SOS Homecare seeks to develop by following a business plan, the achievement of which is dependent on effective business operations. **Business Continuity** is therefore seen as the activities maintaining and recovering business operational effectiveness against **'threats'**, which if realised may materialise as incidents and could ultimately escalate into a full-scale crisis or situation.

Threats to the survival and growth of the business can come in many different forms and the purpose of this document is to set out an understanding of those threats and the prescribed responses to them. Each threat is evaluated by means of a Risk Assessment. The goal of the business is for all operations to exist within the acceptable modes of operation for the relevant business critical areas of operations.

The disaster recovery portions of this Business Continuity Plan (BCP) flow from Recovery Time Objectives (RTO's) specified for each key business process in response to any identified threat, materialising as tangible interruptions, incidents or crisis conditions. In each case the RTO specifies the maximum desirable time it should take for the business to return to normal operating conditions in response to any given threat materialising. The RTO is set by SOS Homecare based on the expected overall business impact severity of different interruptions to its normal operating conditions.

The relevant Disaster Recovery Action Plans and Procedures within this document detail how SOS Homecare will respond in the event of so-called 'disasters', while the wider BCP sets out how SOS Homecare seeks to avoid, mitigate against and otherwise minimise the impact of such potential events.

Both these Disaster Recovery Plans and the BCP, of which they form part, depend centrally on key people and effective communication to restore normal operating conditions.

Management action can seek to restore this desired level, subject to other business resource priorities. As well as proactive prevention activities, reactive intervention (or Disaster Recovery), in accordance with this BCP, will be called for.

If given aspects of Operations fall below pre-defined levels, for more than a pre-defined minimum acceptable duration, this constitutes what is commonly referred to as a crisis or disaster. SOS Homecare considers 'disaster' & 'crisis' to be emotive words, the use of which may not be constructive to effective action during such events. Therefore this plan adopts the use of the words **incident** and **situation**, to reflect the differing levels of seriousness of these events.

Disaster Recovery is taken to mean those activities recovering IT, communications and other infrastructure from interruptions, to restore normal operating conditions. In this BCP, an interruption to operations is deemed to be anything which degrades, or halts altogether those activities and services necessary to maintain normal operating conditions, whether that is in technical operations, sales operations or infrastructure operations. Technical, sales and infrastructure are the high level logical divisions of the business, referred to generically hereinafter as **Functional Areas**. SOS Homecare **Business Continuity Policy** is to plan to avoid altogether, or mitigate potential threats to the normal operating conditions, to the extent that it is deemed

reasonable, practical and commercially viable by the Board, out of a duty of care to both shareholders and staff alike.

Where threats materialise into inconveniences and then incidents (and possibly into situations), this BCP sets out the steps needed to be taken by management to recover normal operating conditions, possibly through certain identifiable recovery phases. Should incidents escalate into what is deemed a situation; the relevant Situation Management procedures contained within this BCP will be invoked by a member of the Situation Management Team (SMT). The standard of what constitutes normal operating conditions can be amended by the respective **Owners** of the functional areas, namely sales, infrastructure & technical operations. The existence, proper maintenance and adherence to normal operational procedures itself is a suitable defense against the threat to the business of not having Procedures defined, up to date and accessible to the relevant individuals.

Following this introduction and the document control and contact lists, Section 5 covers individual roles with respect to the plan. In Section 6, various threats to people, infrastructure and assets are identified and categorised, along with their associated action plans for response. Each action plan incorporates procedures to follow in response to set triggers. Section 7 lists the detail of each of those procedures.

Summary

Together with the SOS Homecare company handbook and operational procedures, this BCP sets out the major perceived threats to business survival, normal operating conditions and the achievement of the business plan itself. It lists the action plans and procedures to respond to those threats, should they materialise as incidents, or situations to be managed. The BCP document is itself tested with live tests and subsequently reviewed, as part of SOS Homecare's formal Business Continuity Policy. Such testing gives SOS Homecare the best opportunity to continue to survive and thrive in the face of all perceived potential threat types and scenarios that it faces.

Distribution

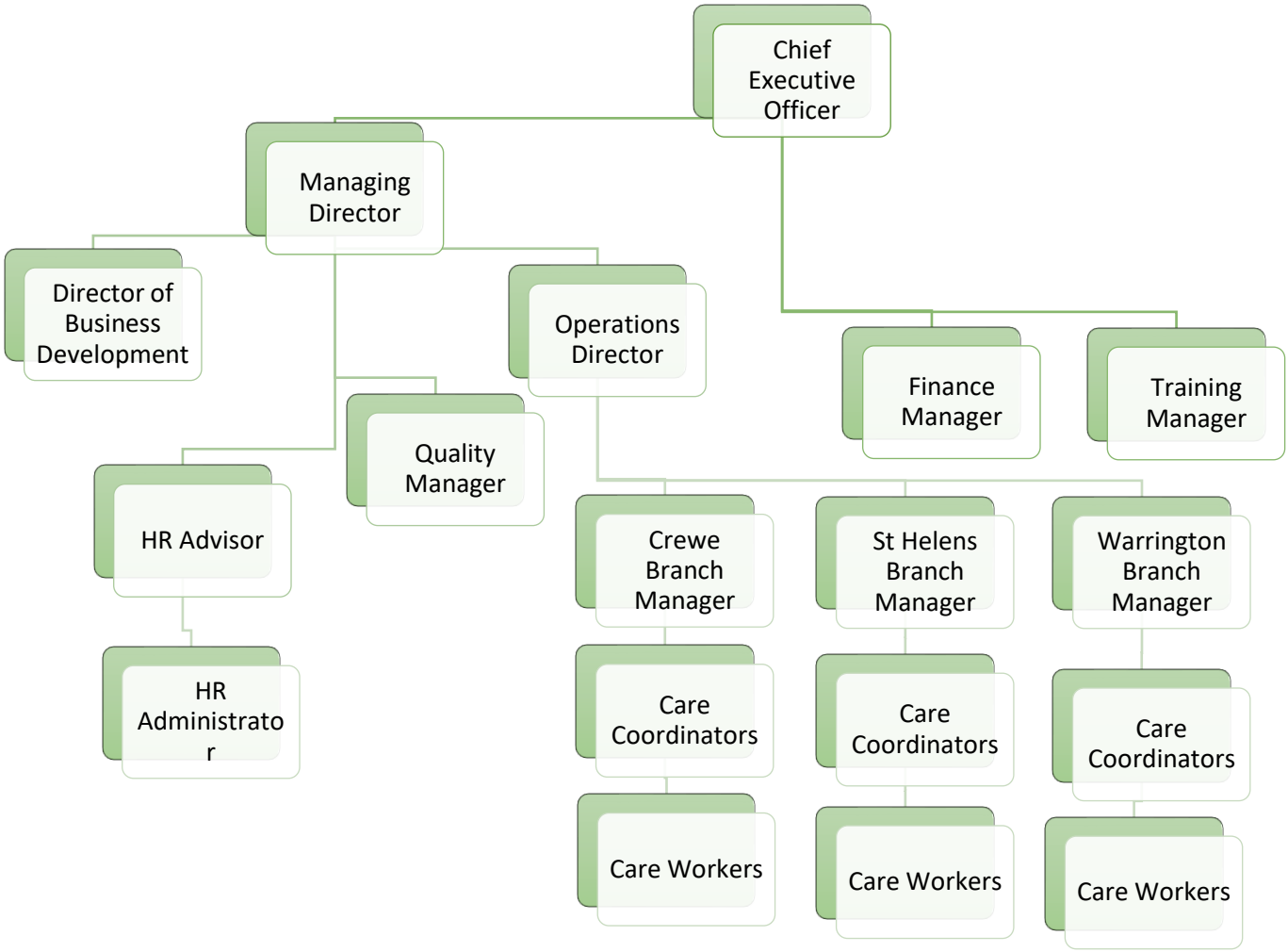
This document is intended for the recipients listed below only and is intended for the sole purpose of informing relevant staff and third parties of the necessary actions and procedures to be adhered to if a given incident, or situation occurs, such that the business, its employees and the public may be adequately safeguarded and normal operating conditions can be rapidly restored.

Holder	Signature	Date
Richard Jackson		
Gareth Rogerson		
Charlotte Taylor		
Jayne Voss		

KEY CONTACT DETAILS

Category	Name	Telephone	Email
SMT	Richard Jackson	07908 83355	RichardJackson@soshomecare.co.uk
	Gareth Rogerson	07939 548500	GarethRogerson@soshomecare.co.uk
	Charlotte Taylor	07388 944622	CharlotteTaylor@soshomecare.co.uk
	Jayne Voss	07939 547500	JayneVoss@soshomecare.co.uk
Operational Managers	Gareth Rogerson	As above	As Above
	Charlotte Taylor	As Above	As Above
	Jayne Voss	As Above	As Above
Response Team(s)	Richard Jackson Gareth Rogerson Charlotte Taylor Jayne Voss	As above	As Above
	Cheryl Ockerby	0161 8725716	CherylOckerby@soshomecare.co.uk
	Kristen Edwards	01618725716	finance@soshomecare.co.uk
Staff	Vivien Pudney	01744 757564	VivienPudney@soshomecare.co.uk
	Paula Wilkinson	01925 597891	PaulaWilkinson@soshomecare.co.uk
	Jodie Swift	01270 509124	JodieSwift@soshomecare.co.uk
Suppliers	Alexandra Uniforms	01454 875741	N/a
	Focus	0330 024 2000	support@focusgroup.co.uk
	BT	0800 400 400	N/a
	British Gas	0845 608 0227	N/a
	United Utilities	0845 746 2255	N/a
	MB Digital	01539 731681	mal.bland@mbdigital.co.uk
Other 3rd Parties	CQC GPW Recruitment Citi Base Regis John Spittle	03000 616161 01744 452049 01925 396800 01270 917841 01606 84777	www.cqc.org.uk will.fairhurst@gpw.com thomasmckenzie@citibase.co.uk rachel.roberts@regis.com johnspittle@susanhowarthsolicitors.co.uk
St Helens Borough Council	Contact Cares	01744 676767	contactcares@sthelens.gov.uk
Warrington Borough Council	Vicky Taylor	01925 444057	Vicky.taylor@warrington.gov.uk
Cheshire East Council	Emma Bibby	07385 002342	Emma.Bibby@cheshireeast.gov.uk

Organisation Chart



Document Control Sheet

	Version	Last Updated
Introduction and Policy Statement	2	Feb 25
Distribution	2	Feb 25
Key Contact Details List	2	Feb 25
Ownership & Contact Groups Control Sheet		
BCP – Roles	2	Feb 25
Plan Owner	2	Feb 25
Infrastructure Operations	2	Feb 25
Technical Operations	2	Feb 25
Sales & Marketing Operations	2	Feb 25
Functional Area Owner	2	Feb 25
ICT	2	Feb 25
Customer Communications	2	Feb 25
Supplier Communications	2	Feb 25
Finance	2	Feb 25
Plan Holders	2	Feb 25
Action Plan Control Sheet		
Action Plans Summary	2	Feb 25
AP 1 Loss of Key Personnel Resources	2	Feb 25
AP 2 Telecoms Infrastructure Failure	2	Feb 25
AP 3 Denial of Workplace Access – Short	2	Feb 25
AP 4 Denial of Workplace Access – Long	2	Feb 25
AP 5 Key Systems Infrastructure Failure	2	Feb 25
AP 6 Loss of Data	2	Feb 25
AP 7 Threat to Wellbeing of Staff	2	Feb 25
Procedure Control Sheet		
1.1 Faulty Workstation Evaluation	2	Feb 25
1.2 Replace Hardware Device	2	Feb 25
1.3 Physical recovery	2	Feb 25
1.4 Invocation of Emergency Call Routing	2	Feb 25
1.5 Disable Key Application Server	2	Feb 25

1.6 Communications Service Fault Resolution	2		Feb 25
1.7 Internal Telephone System Fault Resolution	2		Feb 25
1.8 Peripheral & Routing Hardware Fault Resolution		2	Feb 25
1.9 Supplier Communications	2		Feb 25
1.10 Applications Recovery to Server	2		Feb 25
1.11 Data Recovery to Server	2		Feb 25
1.12 Data Access Validation	2		Feb 25
2.1 Change of Account Manager Letter	2		Feb 25
2.2 Interim Customer Order Process	2		Feb 25
2.3 Customer Communications	2		Feb 25
2.4 Key Account Review	2		Feb 25
2.5 Workload & Delivery Assessment	2		Feb 25
3.1 Staff Communications	2		Feb 25
3.2 Press Communications	2		Feb 25
3.3 Fire and Evacuation	2		Feb 25
3.4 Situation Management Team Comms.	2		Feb 25
3.5 Damage Assessment and Salvage	2		Feb 25
3.6 Situation Management Team Meetings	2		Feb 25
3.7 Invocation of Situation Management Centre	2		Feb 25
3.8 Diversion of Telephone & Fax	2		Feb 25
3.9 Interim Recruitment	2		Feb 25
3.10 Recruitment	2		Feb 25
3.11 Reallocation of Resource Letter	2		Feb 25
3.12 New Employee Induction Procedure	2		Feb 25
3.13 Staff Protection Procedure	2		Feb 25
4.1 Identify Alternate for Workload	2		Feb 25
4.2 Assess & Prioritise Current Workload	2		Feb 25

Business Continuity Plan - Role

This section identifies the groups, or individuals having specific roles with respect to this BCP.

Plan Owner

They are responsible for controlling input to, review and circulation of the BCP in a timely manner, to meet the requirements of the business and its stakeholders.

Infrastructure Operations Owner

Responsible for conducting adequate risk assessments to the infrastructure operations of the business and establishing effective plans to combat threats, so as to reduce, or remove the impact and/or duration of such threats. They are also responsible for defining and executing policies regarding crisis management of incidents and situations impacting infrastructure operations.

Technical Operations Owner

Ownership of all policy, plans & activities to ensure the staff can follow required processes using suitable technology & infrastructure to maintain and recover normal operating conditions for the business. Minimise potential threats and impact of those threats to the business through technical operations, including those arising from infrastructure, staff and suppliers, as well as other external threats. They are responsible for providing all necessary enabling technical facilities to allow staff to be productively employed as soon as possible, in the event of an incident, or situation. Responsible for ensuring all reasonable precautions are in place to protect the staff in technical operations, in accordance with prevailing Health & Safety legislation and published best practice. Responsible for ensuring all necessary plans, processes and technology are in place to minimise the likelihood of a threat to the business, through loss, or underperformance of a supplier to technical operations. They are responsible for ensuring effective and timely communications with key suppliers before, during and after incidents & situations. Engage necessary support from suppliers before, during and after incidents and situations to minimise their impact and duration.

Sales & Marketing Operations Owner

Overall ownership and responsibility for ensuring that revenue-generating and cash collection activities are maintained at the normal level in the face of threats. Responsible for ensuring the people, processes and technology required are in place to maintain normal operating conditions for revenue and cash generation. Responsible for defining and executing policy of managed communication with customers and prospects, in the event of a threat, incident, or situation deemed to require it.

Functional Area Owner

Have overall ownership and co-ordination of crisis management and business operational recovery for the relevant functional area. They are responsible for plan maintenance, policy, review and testing activities relevant to the functional area. They are also responsible for activating the relevant portions of the plan in response to threats to, or incidents & situations affecting the functional area. Responsible for ensuring all relevant actionees within the functional area are able to discharge their individual responsibilities to normal target levels. SOS Homecare designated sub-level functional area owners are as follows:

ICT Owner

Have overall responsibility for defining, communicating and implementing policy to ensure resilience of Information and Communications Technology (ICT) activities against potential threats to normal operating

conditions. They are responsible for defining the operational response to an incident or situation in this area. They also have overall responsibility for minimising impact & duration of an incident or situation affecting this functional area. Responsible for ensuring effective operational practices are in place and well-rehearsed to ensure swift restoration of normal operating conditions following all anticipated business disruptions.

Customer Communications Owner

Responsible for ensuring customers are informed of situations, as directed by the Situation Management Team (SMT). They are also responsible for scripting corporate messages for customers. Notifying customers when normal operating conditions will be or has been restored and what (if anything) will be done to avoid the same scenario happening in the future.

Supplier Communications Owner

They are responsible for ensuring that relevant suppliers are informed of a situation, to the extent required, as directed by the SMT. They are also responsible for defining key messages for suppliers and sourcing alternative suppliers where supply issues are contributing to the severity, or duration of the situation.

Finance Owner

They have overall responsibility for defining, communicating and implementing policy to ensure resilience of finance activities against potential threats to normal operating conditions. They are also responsible for defining the operational response to an incident or situation in this area. And have overall responsibility for minimising the impact & duration of an incident situation affecting this functional area. Responsible for ensuring effective operational practices are in place and well-rehearsed to ensure swift restoration of normal operating conditions following all anticipated business disruptions. They are responsible for establishing and maintaining necessary arrangements to enable financial commitments to be met in a situation. Renegotiating financial facilities and arrangements as necessary to minimise the effects of the situation on the business. Managing all exceptional financial transactions during a situation, including all insurance and banking matters arising.

Plan Holders

Defines the list of people authorised to hold and maintain printed copies of the versions of the BCP and its constituent sections when they are updated and published, as listed in Section 2 of this Plan.

5. Ownership and Contact Groups

Plan Owner

Owner: Richard Jackson

Infrastructure Operations
Owner: Gareth Rogerson
Members: Charlotte Taylor
Jayne Voss

Technical Operations
Owner: Richard Jackson

Sales & Marketing Operations
Owner: Gareth Rogerson
Members: Charlotte Taylor
Jayne Voss

Functional Areas
Owner: Gareth Rogerson

ICT
Owner: Richard Jackson

Customer Communications
Owner: Richard Jackson
Members: Vivien Pudney, Paula Wilkinson & Jodie Swift

Supplier Communications
Owner: Cheryl Ockerby
Members: Kristen Edwards

Finance
Owner: Cheryl Ockerby
Members: Kristen Edwards

Plan Holders
Owner: Richard Jackson

6. Action Plans Summary

The following action plans have been developed in response to known or possible potential threats to the SOS Homecare business and the risk assessments made in connection with those identified threats. Each action plan is designed to achieve SOS Homecare' intended Recovery Time Objective.

AP 1 Loss of Key Personnel Resources

This action plan identifies procedures to be followed, or steps to be taken in the event of key individuals, or a critical percentage of staff being absent long term, or permanently.

AP 2 Telecommunications Infrastructure Failure

This action plan defines the Procedures to be followed, or steps to be taken in the event of critical degradation, or outright loss of telecommunications services, affecting voice (telephone & fax), or data (email, web browsing & remote access), such that normal operating conditions are threatened, or actually interrupted.

AP 3 Denial of Workplace Access - Short Term

This action plan defines the procedures to be followed, or the steps to be taken in the event of a threat, or actual loss of access to the workplace for up to 4 hours during office hours.

AP 4 Denial of Workplace Access - Long Term

This action plan defines the procedures to be followed, or the steps to be taken in the event of a threat, or actual loss of access to the workplace for more than a 4 hour period during office hours.

AP 5 Key Systems Infrastructure Failure

This action plan defines the steps to be taken and procedures to be followed, in the event of a threat, or actual Incident of loss of key computer systems and services.

AP 6 Loss of Data

This action plan defines the steps to be taken and the procedures to follow in the event of a lack of access to correct data usually accessible to a user under normal operating conditions.

AP 7 Threat to Wellbeing of Staff

This action plan defines the steps to be taken and the procedures to follow in the event of tangible threats to the wellbeing of staff, through scenarios including, but not limited to: fire, flood, explosions and violence.

AP 1 Loss of Key Personnel Resources

This action plan identifies procedures to be followed or steps to be taken in the event of key individuals, or a critical percentage of staff being absent long term, or permanently.

Trigger	Action	Procedure
Key Consultant: **Long Term**	1. Identify Alternates to take on Workload 2. Advise clients of interim and/or permanent changes 3. Consider re-assignment of specific responsibilities to other members of staff 4. Assess current/imminent activity and projects 5. Consider re-assignment of specific responsibilities to Senior Managers 6. Advise Staff	4.1 Identify Alternate for Workload 2.1 Change of Account Manager Letter 2.4 Key Account Review 2.4 Key Account Review 2.4 Key Account Review 3.1 Staff Communications
Key Consultant: **Permanent**	1. Advise Clients of interim, or permanent changes 2. Assess current/imminent activity and projects 3. Consider re-assignment of specific responsibilities to other members of staff 4. Consider re-assignment of specific responsibilities to Senior Managers 5. Decide whether to restructure the account-handling team, or to recruit replacement(s) 6. Recruit replacement if appropriate 7. Consider competitive threat/loss of clients 8. Advise Staff	2.1 Change of Account Manager Letter 2.4 Key Account Review 2.4 Key Account Review 2.4 Key Account Review 4.1 Identify Alternate for Workload 3.10 Recruitment 2.4 Key Account Review 3.1 Staff Communication
Senior Manager: **Long Term**	1. Assess current/imminent activity and projects 2. Consider responsibilities that can be delegated to other Senior Managers 3. Consider interim management resources 4. Advise clients as appropriate	4.2 Assess & Prioritise Current Workload 4.2 Assess & Prioritise Current Workload 4.1 Identify Alternate for Workload 2.1 Change of Account Manager Letter

	5. Advise suppliers as appropriate 6. Advise Staff	1.9 Supplier Communications 3.1 Staff Communications
Senior Manager: **Permanent**	1. Consider competitive threat 2. Recruit replacement as appropriate 3. Assess forward workload and responsibilities 4. Consider re-assignment of workload and/or responsibilities to other Senior Managers 5. Assess requirement for interim management, pending recruitment of replacement 6. Advise clients as appropriate 7. Advise suppliers as appropriate 8. Advise Staff	2.4 Key Account Review 3.9 Interim Recruitment 4.2 Assess & Prioritise Current Workload 4.2 Assess & Prioritise Current Workload 4.1 Identify Alternate for Workload 2.1 Change of Account Manager Letter 1.9 Supplier Communications 3.1 Staff Communications
Functional Area: **Critical Percentage Reduction – Long Term**	1. Assess & prioritise current Workload 2. Decide whether clients will be materially affected and advise as appropriate 3. Review cause and recruit replacement staff as appropriate 4. Engage additional resources from suppliers	4.2 Assess/Prioritise Current Workload 3.11 Reallocation of Resource Letter 3.10 recruitment 1.9 Supplier Communications
Functional Area: **Critical Percentage Reduction – Permanent**	1. Assess & prioritise current Workload 2. Decide whether clients will be materially affected and advise as appropriate 3. Review cause and recruit replacement staff as appropriate 4. Engage additional resources from suppliers	4.2 Assess/Prioritise Current Workload 3.11 Reallocation of Resource Letter 3.10 Recruitment 1.9 Supplier Communications
Key Worker: Unavailable Long Term	1. Evaluate options for workload 2. Notify any clients materially affected 3. Notify any suppliers materially affected 4. Notify Staff	4.1 Identify Alternate for Workload 2.3 Customer Communications 1.9 Supplier Communications 3.1 Staff Communications

AP 2 Telecommunications Infrastructure Failure

This action plan defines the procedures to be followed, or steps to be taken in the event of critical degradation, or outright loss of telecommunications services, affecting voice (telephone), or data (email, web browsing & remote access), such that normal operations are threatened, or actually interrupted.

Trigger	Action	Procedure
Initial Report of Symptom(s)	1. Send network broadcast to identify extent of fault 2. Investigate fault	1.6 Data Communications Service Fault Resolution 1.6 Data Communications Service Fault Resolution
Failure of External Link Identified	1. Contact service provider for fault resolution	1.6 Data Communications Service Fault Resolution
Failure of Telephone Switch Identified	1. Establish interim function of answering system/service 2. Implement system fault resolution	1.7 Internal Telephone System Fault Resolution 1.7 Internal Telephone System Fault Resolution
Failure of Routing, or own Network Hardware Identified	1. Implement fault resolution	1.7 Internal Telephone System Fault Resolution
Recovery Phase Achieved, or Full NOC Resumed	1. Decide on the extent of the need to inform clients of the situation 2. Inform Staff of incident status	2.3 Customer Communications 3.1 Staff Communications

AP 3 Denial of Workplace Access - Short Term

This action plan defines the procedures to be followed, or steps to be taken in the event of a threat, or actual loss of access to the workplace for up to 4 hours during office hours.

Trigger	Action	Procedure
0830 - 1730 Premises Evacuated	1. Ensure at least one Situation Management Team Member is aware. 2. Establish reason for evacuation and confirm Premises is unaffected. 3. Implement emergency evacuation procedure as appropriate	3.4 Situation Management Team Communications 3.5 Damage Assessment & Salvage 3.3 Fire and Evacuation
1731 – 0829 Call Received Advising Denial of Access	1. Establish that SOS Homecare facilities within the Premises are unaffected 2. Ensure SMT leaders are aware	3.5 Damage Assessment & Salvage 3.4 Situation Management Team Communications
Confirmed that Premises is Unaffected	1. Establish expected duration of denial of access	3.5 Damage Assessment & Salvage
Expected Duration of Denial of Access is Established	1. Decide whether to implement Emergency Workplaces	3.6 SMT Meetings
Decision Not to Implement Emergency Workplaces	1. Instruct all Staff to go home and return to the workplace next working day, or another specified date, or to await further instructions as appropriate	3.1 Staff Communications
Decision to Implement Emergency Workplaces	1. Assess probable impact on customer orders 2. Divert telephones and fax as appropriate 3. Disable key applications server as required 4. Ensure all staff are advised of where to report and operate from	2.5 Workload & Delivery Assessment 3.8 Diversion of Telephony & Fax 1.5 Disable Key Application Server 3.1 Staff Communications
Decision to Implement Emergency Order	1. Implement emergency order fulfillment arrangements 2. Notify customers	2.2 Interim Customer Order Process

Fulfillment Arrangements		
All Reports received – Emergency Operations Stable	1. Advise all affected customers of the Situation 2. Advise all relevant suppliers of the Situation 3. Confirm expected date/time to return to Premises	2.3 Customer Communications 1.9 Supplier Communications 3.1 Staff Communications and 1.9 Supplier Communications
Advised of Date of Return to Premises	1. Develop plan to return all Functional Areas affected to Normal Operations 2. Inform all Staff of planned date of return to work 3. Inform all customers of expected date of return to Normal Operations 4. Inform all suppliers of expected date to return to Normal Operations	1.3 Physical Recovery 3.1 Staff Communications 2.3 Customer Communications 1.9 Supplier Communications

AP 4 Denial of Workplace Access - Long Term

This action plan defines the procedures to be followed, or steps to be taken in the event of a threat, or actual loss of access to the workplace for more than a 4 hour period during office hours.

Trigger	Action	Procedure
0830 - 1730 Premises Evacuated	1. Ensure at least one Situation Management Team Member is aware 2. Establish reason for evacuation and confirm Premises is unaffected. 3. Implement emergency evacuation procedure as appropriate	3.4 Situation Management Team Communications 3.5 Damage Assessment & Salvage 3.3 Fire and Evacuation
1731 – 0829 Call Received Advising Denial of Access	1. Establish that SOS Homecare facilities within the Premises are unaffected 2. Ensure SMT leaders are aware	3.5 Damage Assessment & Salvage 3.4 Situation Management Team Communications
Confirmed that Premises is Unaffected	1. Establish expected duration of denial of access	3.5 Damage Assessment & Salvage
Expected Duration of Denial of Access is Established	1. Decide whether to implement Emergency Workplaces	3.6 SMT Meetings
Decision Not to Implement Emergency Workplaces	1. Instruct all Staff to go home and return to the Workplace next working day, or another specified date, or to await further instructions as appropriate	3.1 Staff Communications
Decision to Implement Emergency Workplaces	1. Invoke situation management centre plans 2. Assess probable impact on customer orders 3. Divert telephones and fax as appropriate 4. Disable key applications server as required 5. Ensure all staff are advised of where to report and operate from	3.7 Invoke SMC 2.6 Workload & Delivery Assessment 3.8 Diversion of Telephony & Fax 1.5 Disable Key Application Server 3.1 Staff Communications
Decision to Implement Emergency Order Fulfillment Arrangements	1. Implement emergency order fulfillment arrangements 2. Notify customers	2.2 Interim Customer Order Process

All Reports received – Emergency Operations Stable	1. Advise all affected customers of the Situation 2. Advise all relevant suppliers of the Situation 3. Confirm expected date/time to return to Premises	2.3 Customer Communications 1.9 Supplier Communications 3.1 Staff Communications and 1.9 Supplier Communications
Advised of Date of Return to Premises	1. Develop plan to return all Functional Areas affected to Normal Operations 2. Inform all Staff of planned date to return to Premises 3. Inform all customers of expected date of return to Normal Operations 4. Inform all suppliers of expected date to return to Normal Operations	1.3 Physical Recovery 3.1 Staff Communications 2.3 Customer Communications 1.9 Supplier Communications

AP 5 Key Systems Infrastructure Failure

This action plan defines the procedures to be followed, or steps to be taken in the event of a threat, or actual incident of loss of key computer systems & services.

Trigger	Action	Procedure
Problem Reported	1. Determine whether the problem is local to a particular workstation, or with the network	1.1 Faulty Workstation Evaluation
Established that a Network Computer has Failed and cannot be used	1. Determine whether the failed item can be replaced under Warranty	1.2 Replace Hardware Device
Established that the Failed Computer is NOT included in the Maintenance Service Agreement	1. Arrange for repair, or replacement of the failed computer as appropriate 2. Assess the impact on the network and consider reviewing hardware covered on the maintenance service agreement	1.2 Replace Hardware Device
Established that the Failed Computer is included in the Maintenance Service Agreement	1. Invoke replacement computer service	1.2 Replace Hardware Device
Replacement Computer Service Invoked	1. Replace failed hardware	1.2 Replace Hardware Device
Failed Hardware Repaired/Replaced & functioning correctly	1. Review age/condition/suitability of all hardware Assets and the extent of the businesses critical dependence upon each item	1.2 Replace Hardware Device

AP 6 Loss of data

This action plan defines the procedures to be followed, or steps to be taken in the event of a lack of access to correct data usually accessible to a user under normal operating conditions.

Trigger	Action	Procedure
User Cannot Access Data	1. Determine whether the lack of access is due to password access failure 2. Check if loss is due to corrupt data 3. Check if loss is due to system configuration change 4. Check if loss is due to faulty workstation 5. Check if loss is due to Key Systems Infrastructure Failure 6. Check if loss is due to network, or peripheral routing hardware failure 7. Check if loss is due to telecommunications infrastructure failure	1.12 Data Access Validation 1.12 Data Access Validation 1.12 Data Access Validation 1.1 Faulty Workstation Evaluation 1.8 Peripheral & Routing Hardware Fault Resolution 1.8 Peripheral & Routing Hardware Fault Resolution 1.6 Data Communications Service Fault Resolution

AP 7 Threat to Wellbeing of Staff

This action plan defines the procedures to be followed, or steps to be taken in the event of tangible threats to the wellbeing of staff, through the likes of fire, flood, explosions & violence.

Trigger	Action	Procedure
Individual, or Group is Identified as Under Threat	1. Alert Staff to take action to remove, or avoid threat 2. Invoke Staff Protection procedures 3. Alert at least one Member of the SMT 4. Inform Staff as appropriate	3.1 Staff Communications 1.13 Staff Protection Procedure 3.3 SMT Communications 3.1 Staff Communications
Individual, or Group is Identified as Suffering Actual Harm	1. Invoke Staff Protection procedures 2. Alert at least one Member of the SMT 3. Inform Staff as appropriate	1.13 Staff Protection Procedure 3.3 SMT Communications 3.1 Staff Communications

7. Procedures Summary

	Version	Date	Number
Technical Operations			
Faulty Workstation Evaluation	2	Feb 25	**1.1**
Replace Hardware Device	2	Feb 25	**1.2**
Physical Recovery	2	Feb 25	**1.3**
Invocation of Emergency Call Routing Procedures	2	Feb 25	**1.4**
Disable Key Application Server	2	Feb 25	**1.5**
Data Communications Service Fault Resolution	2	Feb 25	**1.6**
Internal Telephone System Fault Resolution	2	Feb 25	**1.7**
Peripheral & Routing Hardware Fault Resolution	2	Feb 25	**1.8**
Supplier Communications	2	Feb 25	**1.9**
Applications Recovery to Server	2	Feb 25	**1.10**
Data Recovery to Server	2	Feb 25	**1.11**
Data Access Validation Procedure	2	Feb 25	**1.12**
Sales & Marketing Operations			
Change of Account Manager Letter	2	Feb 25	**2.1**
Interim Customer Order Process	2	Feb 25	**2.2**
Customer Communications	2	Feb 25	**2.3**
Key Account Review	2	Feb 25	**2.4**
Workload & Delivery Assessment	2	Feb 25	**2.5**
Infrastructure Operations			
Staff Communications	2	Feb 25	**3.1**
Press Communications	2	Feb 25	**3.2**
Fire & Evacuation	2	Feb 25	**3.3**
Situation Management Team Communications	2	Feb 25	**3.4**
Damage Assessment & Salvage	2	Feb 25	**3.5**
Situation Management Team Meetings	2	Feb 25	**3.6**
Invocation of Situation Management Centre	2	Feb 25	**3.7**
Diversion of Telephony & Fax	2	Feb 25	**3.8**
Interim Recruitment	2	Feb 25	**3.9**
Recruitment	2	Feb 25	**3.10**
Reallocation of Resource Letter	2	Feb 25	**3.11**
New Employee Induction Procedure	2	Feb 25	**3.12**
Staff Protection Procedure	2	Feb 25	**3.13**
General			
Identify Alternate for Workload	2	Feb 25	**4.1**
Assess & Prioritise Current Workload	2	Feb 25	**4.2**

8. Procedures

P 1.1 Technical Operations – Faulty Workstation Evaluation

1. Confirm whether issue is loss of access to data and if so, follow the set procedure for this issue.
2. Confirm that the fault can be replicated by the user.
3. Carry out system self-test diagnostics in accordance with the relevant section of the instruction booklets.
4. Identify if fault is a known software problem that can be remedied by applying patch, or upgrade. If so, apply the patch or upgrade.
5. Advise user to seek use of alternate workstation for access to necessary services in the interim.
6. Check that replicated fault is isolated to one application for the user. If so, reinstall the application for the user.
7. If reinstallation attempts generate multiple error conditions, schedule the workstation for software rebuild.
8. If the root cause is hardware, schedule the workstation for repair, or replacement accordingly.

P 1.2 Technical Operations – Replace Hardware Device

1. Assess if faulty device can be fixed by replacing or repairing faulty component (e.g. screen, cartridge, etc). If so, replace component as an expense item.
2. If not, confirm if replacement devices are available from a local supplier, with sufficient similarities in terms of features.
3. If not, assess cost or benefit of sourcing replacements from remote locations, versus local purchase from local sources, factoring in lead time considerations.
4. Reroute user's services to secondary platforms, subject to cost or benefit assessment in terms of time estimated to recover normal operating conditions for the user.
5. Purchase replacement device as necessary.
6. Purchase additional replacement devices as necessary, as contingency, if considered beneficial to shorten future recovery to normal operating conditions by functional area owner, out of discretionary budget.

P 1.3 Technical Operations – Physical Recovery

1. **Physical Recovery is set out in the following sections:** Replacement of IT equipment & Systems; Replacement of Fixtures & Fittings; Repairs & Refurbishment of Buildings, Including Offices & Interiors; and Repair, or Replacement of Manufacturing and Related Facilities.
2. **IT Equipment & Systems:** The IT & telecommunications systems are to be restored to their previous standard, specification & configuration. A schedule of necessary hardware & software purchases, plus services to achieve this, must be drawn up and submitted to the relevant budget holder for approval. Where relevant, a schedule of confirmed damage and losses from the salvage contractor, as agreed by the loss adjuster, must accompany this schedule.
3. **Fixtures & Fittings:** Fixtures & fittings, including furniture, must be reinstated to their pre-incident standard. Approval for all such replacements must be obtained from the loss adjuster. A schedule of all original assets may be obtained from the relevant Finance section.
4. **Buildings & Infrastructure:**

   Head Office - If physical damage occurs to the head office address, Citi-Base is accountable for affecting such repairs and providing alternative temporary Premises in the local area in the interim.

   Warrington - If physical damage occurs to the Warrington office, John Spittle is accountable for affecting such repairs and providing alternative temporary Premises in the local area in the interim.

   Crewe - If physical damage occurs to the Crewe office, Regis is accountable for affecting such repairs and providing alternative temporary Premises in the local area in the interim.

   St Helens - If physical damage occurs to the St Helens office, GPW Recruitment is accountable for affecting such repairs and providing alternative temporary Premises in the local area in the interim.

P 1.4 Technical Operations – Invoke Emergency Call Routing

1. Confirm main workplace and its facilities will not be available for an extended period (over 4 hours).
2. Reroute via focus online website to designated alternate numbers, as specified by any member of the SMT.
3. Revert to original routing number when normal operating conditions are resumed.

P 1.5 Technical Operations – Disable Key Application Server

1. Notify affected users informing them of relevant server shut down at the specified time.
2. Send warning messages to logged on users 30 minutes, 10 minutes and 1 minute prior to shut down.
3. Check that all users are logged off at shut down time.
4. Contact any users still logged on after shut down time & instruct them to log off, or lose work.

5. Issue server shut down command at operating system level.
6. Power system off, if required.
7. If down time is known, include this in the messages to users.
8. Notify user community, or key Contacts within it, that Services have been recovered, with broadcast email, and/or other notification method.

P1.6 Technical Operations – Communications Fault Resolution

1. Identify that there appears to be an external communications service fault into the building, such that the phone service is unusable.
2. Contact Focus and inform them of the fault during office hours.
3. Outside of office hours, notify a member of the management.
4. If necessary, contact BT on 151 from any external callbox, or working line, advising them of the fault.
5. If the service provider can identify a fault on the line, request an estimated time to resolution.
6. Divert via Focus online portal to a designated phone number
7. Report expected duration of function loss to relevant staff, suppliers & customers as necessary.
8. Switch to alternate communications methods as appropriate.

P 1.7 Technical Operations – Internal Telephone System Fault Resolution

1. Assess possibility of using alternate handset hardware within the local office.
2. Request replacement handset from Focus.
3. Check replacement handset works with the underlying phone number.
4. Recheck previous configurations on new handset, such as speed dial.

P 1.8 Technical Operations – Peripheral & Routing Hardware Fault Resolution

1. Conduct diagnosis to locate the faulty component
2. Does a unit of the replacement component exist locally on site? If so, replace and re-order to replenish under warranty, or as a purchased consumable.
3. If component cannot easily be replaced, consider rerouting workload, or traffic, or other similar technical workarounds.
4. Notify any staff, customers, or suppliers likely to be materially affected.
5. Ensure replacement of item & restoration of normal operating conditions after installation.
6. Consider cost-benefit of buying spare units of the failing component, or implementing alternative, more resilient technical solution.

P 1.9 Technical Operations – Supplier Communications

1. Identify list of suppliers materially affected.
2. Determine the nature, frequency & content of the communication, defaulting to email on an 'as needs' basis.
3. Specify clearly the way in which the supplier relationship is likely to be affected.
4. Specify any increased services required, or any changes needed in normal operating conditions procedures between organisations.
5. Keep suppliers informed regarding likely resumption of normal operating conditions and when it is actually achieved.

P 1.10 Technical Operations – Applications Recovery to Server

1. Power server down if necessary.
2. De-install any previous versions of the application as required, to permit clean install.
3. Back up associated data, as required.
4. Install fresh version of application, following installation instructions to achieve desired configuration.
5. Check access to the application across the network & locally
6. Check relevant Users can access both the application & any associated data as appropriate.

P 1.11 Technical Operations – Data Recovery to Server

1. If relevant, back up data files that can be identified.
2. Identify most recent version of stored data required, from various storage media.
3. Deploy data files into correct location, where they can be properly accessed by the user's application.
4. Notify user when the operation is complete.
5. Check with User that they can access both application & data as expected during normal operating conditions.

P 1.12 Technical Operations – Data Access Validation Procedure

1. Confirm if same data can be accessed from another workstation
2. Confirm if same data can be accessed using another valid password access code
3. Check if there are error messages linked to the data source in the relevant system monitoring logs.
4. Check with Managing Director whether there have been any recent configuration changes, since the last time the User recalls having full access.
5. Check what the user recalls doing immediately prior to the loss of access to the data.

P 2.1 Sales & Marketing Operations – Change of Account Manager Letter

This letter is stored as a Word file on the SOS Homecare shared hard drive.

Dear

I am writing to inform you that your current Account Manager {name} has unfortunately requested some time from work due to {reason}. To minimise any disruption, I have allocated {alternate name} to your account and I know that s/he will be making contact with you in the next few days.

If you would like to discuss this situation personally, please call me on the number below and I will answer any questions you may have.

We hope to count on your support under these unusual circumstances and are confident of maintaining the high standard of service that you expect from us.

Yours Sincerely,

[Person]

[Title]

P 2.2 Sales & Marketing Operations – Interim Customer Order Process

1. Identify all outstanding deliverables for clients and timescales expected.
2. Identify business reasons for timescales and what impact any delays will have
3. Negotiate revised deadlines and any associated commercial implications, including SLA's, credit penalties, cash payments, order cancellations, etc.
4. Qualify all customer responses and assess likely overall business impact of delays indicated by the revised work phasing
5. Make recommendations to the SMT as to which customer orders to prioritise.
6. Communicate decision to customers affected, offering escalation route to management if needed.

P 2.3 Sales & Marketing Operations – Customer Communications

1. The account contact List is held on CarePlanner at;

   St Helens Branch - sossthelens.care-planner.co.uk

   Warrington Branch – soswarrington.care-planner.co.uk

   Crewe Branch – sosbeechmere.care-planner.co.uk

   PASS – passgenius.com

2. The SMT will determine, with the Branch Manager, who should contact which customer and in what way.
3. The SMT will determine the content of the message to be communicated.
4. By way of illustration, the following template should be adapted as required:
5. "Our premises have been affected by a fire, explosion, flood or other type of incident and we cannot use the premises for the time being. Fortunately, the relevant section of our BCP has been invoked and we are in the process of returning to normal operational capacity. As an organisation, we are built to operate effectively as a virtual team and the Situation Management Team is handling matters. We are implementing the necessary arrangements with our suppliers and sub-contractors to meet our outstanding obligations to you. As we have been able to switch your service over to our Secondary Site, we have all our data safely held. If there will be any foreseeable impact upon our committed service provision to you, we will be in touch within 1 day to confirm."

P 2.4 Sales & Marketing Operations – Key Account Review

1. Collate list of all affected clients.
2. Review outstanding requirements and committed requirements, using the latest information on the CarePlanner database.
3. Prioritise immediate actions that need to be addressed.

P 2.5 Sales & Marketing – Workload Delivery Assessment

1. Assessment of anticipated operational capacity to cope with outstanding requirements in expected timescales.
2. Reconcile outstanding requirements with revised estimates of capacity, including prioritisation.
3. Assess staff availability.
4. Formulate plan to best match outstanding assignments with the skills of the available staff.
5. Produce revised outstanding bookings report.
6. Monitor revised schedule to assess need for new iteration of this process, until the normal operating conditions are resumed.

P 3.1 Infrastructure Operations – Staff Communications

1. In each communication, ensure inclusion of relevant elements of whether there is denial of access, duration of any interruption to normal operating conditions, IT, telephony, other service issues, any casualties and wider considerations of feedback, welfare & staff morale.
2. **During office hours**:
    a. Ensure any staff known to be present, or associated with the affected premises, are advised regarding what action they should take.
    b. Initiate emergency call-out or broadcast to notify staff according to agreed, scripted message.
    c. If the incident occurs before 4pm contact all absent staff members to advise them of action to take.
    d. Record whether contact was reached, or whether just a message was left.
    e. After 6pm, consider contacting remaining staff on their mobile phone numbers.
    f. If any affected staff are on holiday or away from their home, contact them by phone if possible, otherwise by email and post as a last resort.
3. **Outside office hours**:
    a. If the incident occurs before 5am, consider waiting until after 6am to notify them at home. Otherwise, always default to primary contact on their mobile phone.
    b. Give guidance on how long incident is likely to continue.
    c. Record whether person has been contacted, or just a message was left.
    d. Advise staff on how they will be kept updated on latest developments regarding the incident.
    e. Confirm when normal operating conditions has been resumed.

P 3.2 Infrastructure Operations – Press Communications

1. Unless specifically authorised by the SMT, no comment should be made to the Press. If approached, staff response should be **"no comment"** and enquiries should be referred to the SMT.
2. The default spokesperson in Situations will be Richard Jackson. When Richard Jackson is unavailable, the SMT shall nominate the most appropriate alternative, which will be Gareth Rogerson or Charlotte Taylor unless otherwise specified.
3. The SMT shall agree on the content of what shall be communicated, via what channels and to whom, in what order. Prior to briefing the press, a decision should be made as to whether to provide an interview, conference, or merely issue a read press statement. The latter is the preferred method for most foreseeable circumstances.
4. Wherever possible, staff should be notified first, customers second, suppliers third and Press last of all. SOS Homecare has no specific obligations with respect to notifying the Public concerning incidents at its locations. Third parties are responsible for the respective premises.
5. Policy is to stick to communicating facts and expressing sorrow at any personal loss, or injury suffered as a consequence of the Situation.

P 3.3 Infrastructure Operations – Fire & Evacuation

1. This procedure is to be used in the event of a fire.
2. If you discover a fire:
    a. Operate the fire alarm immediately by breaking the seal on the nearest relevant unit
    b. Attack the fire if possible with the equipment provided, but do not take any personal risks. Leave immediately if the fire cannot be brought quickly under control.
3. On Hearing the Alarm
    a. The **ALERT** signal is a continuous ring on a bell alarm.
    b. Unless having received prior warning that the Alarm is a planned exercise, staff and visiting personnel should proceed immediately to the nearest muster point, the defaults being in the Car Park at the rear of the building, and the pavement outside the front of the building if nearest the front stairs.
    c. **DO NOT USE LIFTS (EXCEPT WHERE SPECIAL ARRANGEMENTS EXIST FOR THE DISABLED).**
    d. **DO NOT STOP TO COLLECT BELONGINGS.**
    e. **DO NOT RE-ENTER THE BUILDING UNTIL INSTRUCTED TO DO SO BY THE AUTHORISED FACILITIES MANAGEMENT REPRESENTATIVE**
    f. Upon receiving notification of when staff will be able to return to their workspace, the most senior member of staff present in the group should notify a member of the SMT
    g. Upon returning to the workspace, the most senior member of staff present should assess the workspace for damage and inform the SMT of the need to invoke Damage Assessment & Salvage Procedures, if necessary.

P 3.4 Infrastructure Operations – SMT Communications

1. The following should be used for contact between members of the SMT in connection with Business Continuity Incidents & Situations.
2. Regardless of time, contact SMT members by the following means, in order, until successful:
    a. Mobile Telephone
    b. Work email, instant-mail, home e-mail
    c. Travel to home address (unless it is known that the contact is away from home)
3. Members of the SMT and their contact details appear in the Contacts section of this BCP.
4. The primary purpose of initially contacting all members of the SMT is to arrange the first SMT meeting (see procedure: Situation Management Team Meetings)

P 3.5 Infrastructure Operations – Damage Assessment & Salvage

1. In the event of a physical incident where losses and/or damage are likely, a salvage contractor needs to be instructed whom provide a 24 hour response services.
2. Call the contractors who have a 24 hour response service.
3. Provide information requested – a contractor should attend site within 4 hours to begin salvage operations, liaise with insurers & loss adjuster, and expedite the recovery process.

P 3.6 Infrastructure Operations – SMT Meetings

1. The first SMT meeting will be held at the nominated location agreed by the SMT, depending on the scale of the emergency. Choices shall include, but not be limited to:
    a. One of the groups location
    b. Virtual Office
    c. Use of Sister Company's premises
2. The objectives for Day 1 of this type of incident would be:

    The standing agenda for the meetings will be:

    a. Casualties, injuries and fatalities, to be recorded
    b. Nature & duration of denial of access - likelihood of regaining access to premises - implementation of emergency workplaces
    c. Losses, damage & salvage
    d. Customer communications
    e. Impact on customers' orders or deliveries
    f. Supplier communications
    g. Stakeholders
    h. Insurance and finance
    i. Prioritise workload & roles within SMT
    j. Date, time & venue of next meeting
    k. AOB

P 3.7 Infrastructure Operations – Invoke Situation Management Centre

1. SMT to discuss options from list of SM Centre locations.
2. SMT to select one location and notify staff from contact list.
3. SMT to arrange purchase of emergency equipment and facilities at the SMC.
4. Quantify impact of Situation and likely duration of need for the SMC.
5. Notify staff, suppliers and customers affected and procedure for obtaining latest information.
6. Advise all of likely resumption of normal operating conditions.

P 3.8 Infrastructure Operations – Diversion of Telephone & Fax

1. SOS Homecare utilises Focus online portal, which allows the office phone to be diverted to a designated phone number
2. The main SOS Homecare phone number for St Helens is 01744757564, Crewe is 01270 509124 and Warrington is 01925 597891
3. The main support number is 07939547000.
4. Once normal operating conditions is restored, remove the divert off the phone line

P 3.9 Infrastructure Operations – Interim Recruitment

1. For recruiting senior or key members of staff, obtain authority from the Managing Director for new position or interim position and determine length of contract.
2. Approach a temporary recruitment agency to discuss job specification.
3. Obtain approval for and agree contract with the temporary recruitment agency.
4. Interview candidates.
5. Make job offer to selected candidate in accordance with standard terms & conditions of employment.
6. Take new employee through induction, as part of their probationary period with SOS Homecare.

P 3.10 Infrastructure Operations - Recruitment

1. Obtain authority from the Managing Director for new position, including detailed job specification and business case.
2. Approach recruitment agencies to discuss job specification.
3. Obtain approval for and agree terms with recruitment agencies.
4. Interview and shortlist candidates.
5. Make offer to selected candidate.
6. Take candidate through induction procedure.

P 3.11 Infrastructure Operations – Reallocate Resource Letter

This letter is held as a Word file on the SOS Homecare shared drive.

The text is as follows:

Dear

Due to the unforeseen consequences of {reason for problem} we are allocating you different members of the {name} department to work with you. {Contact name} will be in contact in the very near future to arrange a mutually convenient time and location for a review meeting.

If you would like to discuss this situation personally, please call me on [number] and I will answer any questions you may have. We hope to count on your support in these unusual circumstances and are very confident of continuing to deliver the high standard of service that you expect from us.

Sincerely,

[Person]

[Title]

P 3.12 Infrastructure Operations – New Employee Induction

1. Ensure employee's details are registered in SOS Homecare HR files, including signed contract of employment
2. Notify Payroll of employee's details, having obtained employee's last P45 if relevant.
3. Set up person with own e-mail account.
4. Obtain access to necessary systems to enable the employee to perform their tasks.
5. Allocate supervisor responsible for guiding them through the early weeks.
6. Set review dates with senior manager as a mentor, to ensure any issues are raised with a mentor.
7. Cover the relevant items on the Technical, Sales, or Infrastructure Induction Syllabus.

P 3.13 Infrastructure Operations – Staff Protection Procedure

1. Confirm details of threat of, or actual harm, to which individual member, or group of staff.
2. Identify if the individual or group is aware of the potential harm.
3. Seek to communicate with the individual or group to direct them away from the threat, and towards safety, with respect to their location.
4. Seek to educate the individual or group concerning the nature of the threat, to avoid, or minimise it in future.
5. Where relevant, notify the authorities: police, fire, ambulance, coast guard.
6. Direct staff towards counseling services relevant to the nature of harm they may have suffered.
7. Notify wider staff community regarding the nature of action taken and any changes to procedure required within normal operating conditions, where appropriate.

P 4.1 General – Identify Alternate for Workload

1. Assess the nature, quantity and expected timescales of the workload and the skills necessary to perform it, by referring to available paperwork, electronic files and co-workers of the person(s) not available.
2. Represent the workload as a set of deliverables with target dates and associated status summaries, or starting positions.
3. Prioritise the workload in terms of the value of the deliverables to the business unit concerned.
4. Evaluate the relative cost or benefits of achieving the deliverables with existing in-house labour with spare capacity, versus subcontracted resources.
5. Formulate a plan identifying all deliverables identified, new deliverable owners, timescales agreed and method of updating progress against the plan.
6. Circulate the plan to all new actionees.
7. Actionees are responsible for notifying their own management and colleagues, and managing their workload to incorporate the newly allocated deliverables, as required.

P 4.2 General – Assess & Prioritise Current Workload

1. Procedure for reviewing the activities of owners of the Functional Areas: Technical Operations, Sales & Marketing Operations & Infrastructure Operations (including HQ and Situation Management Team activities).
2. Coordinator (defaults to most senior team member, unless otherwise agreed) to initiate contact with all relevant representatives of the affected work areas and collate prioritised, bullet-point list of all activities of relevant staff and key third parties.
3. Invite contributions and discuss key perceived issues or activities by project, with all relevant contributors meeting together, or conference in.
4. Coordinator to summarise consolidated view of contributors to assess collective impact of various courses of action and resource prioritisation on business as a whole.
5. Gain agreement and commitment to proposed consolidated course of action, with action owners identified and completion timescales agreed.
6. Invite any final comments from contributors & integrate comments, or deal with the issues before proceeding.
7. Agree time or manner to review progress against agreed action plan.
8. Document & distribute agreed action plan, by e-mail, or other agreed mechanism, if e-mail cannot be relied upon.
9. Review progress at the set time/manner, unless rescheduled in the intervening time.
10. Repeat processes until workload issues are resolved and normal mode of operations is resumed.