Business Continuity Management Plan for Company Limited

[LOGO]

Company Limited
[Address]
UK

T: 0870 [Number]
F: 0870 [Number]
Web Site: http://www.Company.co.uk
Email: info@Company.co.uk

Version: 1.0
Date: [Date]
Plan Owner: [Name]
Next Review: [Date]

1. INTRODUCTION AND POLICY STATEMENT

[Search & Replace the word Company throughout, using your own business/organization name]

The Operation of the Company business depends on a given combination of People, Processes & Technology, in connection with a given set of current Business Assets. Company 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 materialize as Incidents and could ultimately escalate into a full scale Crisis, or "Situation".

This Business Continuity Plan adheres to the Good Practice Guidelines issued by the **Business Continuity Institute** (www.thebci.org) , an electronic "pocket" version of which can be obtained at: http://www.thebci.org/PocketsizeGPGIC.pdf . This Plan and the Company programme of which it forms an integral part, both seek to intercept the emerging British Standard for such activities BS25999, a Draft copy of which can be downloaded by filling out the necessary form at: http://www.bsi-global.com/Risk/dpc.xalter . The Review Process within Company's Business Continuity Management Programme includes making use of prevailing good practice review Checklists, such as those available via www.londonprepared.gov.uk , tailored to be relevant respective to business sizes. Company use the "Ten Minute Assessment" and the check list resource at: http://www.londonprepared.gov.uk/business/businesscont/index.htm for businesses of [Up to 10 Staff] [10-50] [50-250] [Over 250 Staff].

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 (refer to Risk Assessment Table in Appendix 2, considering the potential scenarios [for generic Excel spreadsheet version of Risk Assessment & Business Impact Analysis, email request to jonathan.stuart@criticall.co.uk].

The Scale of each perceived potential impact on the business can be worked out as part of a Business Impact Assessment (BIA), given such parameters as degree and duration of the given disruption and the financial consequences per unit of measurement (eg minutes, days). The goal of the business is for all Operations to exist within the acceptable zone of Normal Mode of Operation (NMO), ie between Optimum Mode of Operations (OMO) and Minimum Mode of Operations (MMO) as defined in the Operations Procedures Manual (OPM) for the relevant Business Critical areas of Operations.

The Disaster Recovery portions of this Business Continuity Plan flow from Recovery Time Objectives (RTOs) specified for each key business process in response to any identified threat, materializing as tangible Interruptions, Incidents or Crisis conditions. These key business processes and their respective RTOs are listed in Appendix 3 of this Document. In each case, the RTO specifies the maximum desirable time it should take for the business to return to NMO in response to any given threat materializing. The RTO is set by Company based on the expected overall business impact severity of different interruptions to its NMO, as detailed in the Business Impact Assessment for identified Threats shown in Appendix 2. The relevant Disaster Recovery Action Plans and Procedures within this Document detail how Company will respond in the event of so-called "disasters", while the wider BC Plan sets out how Company seeks to avoid, mitigate against and otherwise minimize the impact of such potential events.

Both these Disaster Recovery plans and the Business Continuity Plan of which they form part, depend centrally on key people and effective communication to restore NMO.

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

Operations fall below pre-defined MMO levels, for more than a pre-defined minimum acceptable duration, this constitutes what is commonly referred to as a Crisis, or Disaster. Company 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** & **Situation**, to reflect the differing levels of seriousness of these events.

Disaster Recovery is taken to mean those activities recovering IT and other infrastructure from interruptions, to restore NMO. In this BC Plan, an Interruption to Operations is deemed to be anything which degrades, or halts altogether those activities and services necessary to maintain NMO, whether that is in Technical Operations (including Product Development), Sales Operations, or Infrastructure Operations. Technical, Sales & Infrastructure are the high level logical divisions of the business, referred to generically hereinafter as **Functional Areas**. Company's **BC Policy** is to Plan to avoid altogether, or mitigate potential Threats to the NMO defined in the OPM, 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 materialize into inconveniences, Interruptions and then Incidents (and possibly into Situations), the OPM and this BC Plan together set out the steps needed to be taken by Management to recover NMO, possibly through certain identifiable Recovery Phases. Should incidents escalate into what is deemed a Situation, the relevant Situation Management procedures contained within this BC Plan will be invoked by a Member of the Situation Management Team (SMT). The OPM sets out the way the Operations of the Business should operate, the methods of monitoring those operations and the thresholds of acceptability, or NMO. The standard of what constitutes NMO can be amended by the respective **Owners** of the Functional Areas, namely Sales, Infrastructure & Technical Operations. The OPM is a related document and its existence and use are key considerations within this Business Continuity Plan. The existence, proper maintenance of and adherence to the OPM itself is a suitable defence 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 categorized, along with their associated Action Plans for response. Each Action Plan incorporates Procedures to follow in response to identifiable Triggers. Section 7 lists the detail of each of those Procedures.

SUMMARY

Together with the Company OPM, this Business Continuity Plan sets out the major perceived threats to Business Survival, Normal Mode of Operations and the achievement of the Business Plan itself. It lists the Action Plans and Procedures to respond to those Threats, should they materialize as Incidents, or Situations to be managed. The BC Plan document is itself tested with live tests and subsequently reviewed, as part of Company's formal BC Policy and holistic BC Programme. Such testing gives Company the best opportunity to continue to survive and thrive in the face of all perceived potential threat types & scenarios that it faces.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

2. 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 NMO can be rapidly restored.

HOLDER	SIGNATURE	DATE

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

3. KEY CONTACT DETAILS

CATEGORY	NAME	TELEPHONE	EMAIL
SMT	JOHN SMITH	M: 0777 1234567 O: 020 7654 321 H: 020 7123 456 F: 020 9999 999 P: 0866 66666 (Pager)	john.smith@company.com ; john@home.co.uk (private) john@blackberry.com (instant) john@msn.com (Instant Messenger)
	JOHN DOE		
FUNCTION MANAGERS	MATTHEW		
	MARK		
	LUKE		
	JOHN		
RESPONSE TEAM(S)			
STAFF			
SUPPLIERS			
KEY CUSTOMERS			
OTHER THIRD PARTIES			

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

4. DOCUMENT CONTROL SHEET

	VERSION	LAST UPDATED
Introduction and Policy Statement	1.0	[Date]
Distribution	1.0	[Date]
Key Contact Details List	1.0	[Date]
Ownership & Contact Groups Control Sheet	1.0	[Date]
Business Continuity Plan – Roles	1.0	[Date]
Plan Owner	1.0	[Date]
Infrastucture Operations	1.0	[Date]
Technical Operations	1.0	[Date]
Sales & Marketing Operations	1.0	[Date]
Functional Area Owner (FAO)	1.0	[Date]
Product Development	1.0	[Date]
ICT	1.0	[Date]
Human Resources	1.0	[Date]
Customer Communications	1.0	[Date]
Supplier Communications	1.0	[Date]
Finance	1.0	[Date]
Media Handling	1.0	[Date]
Third Parties	1.0	[Date]
Plan Holders	1.0	[Date]
Action Plans Control Sheet		
Action Plans Summary	1.0	[Date]
AP001 Loss of Key Personnel Resources	1.0	[Date]
AP002 Telecomms Infrastructure Failure	1.0	[Date]
AP003 Denial of Workplace Access – Short	1.0	[Date]
AP004 Denial of Workplace Access – Long	1.0	[Date]
AP005 Key Systems Infrastructure Failure	1.0	[Date]
AP006 Loss of Data	1.0	[Date]
AP007 Threat to Wellbeing of Staff	1.0	[Date]
Procedures Control Sheet		
1.1 Faulty Workstation Evaluation	1.0	[Date]
1.2 Replace Hardware Device	1.0	[Date]
1.3 Physical recovery	1.0	[Date]
1.4 Invocation of Emergency Call Routing	1.0	[Date]
1.5 Disable Key Application Server	1.0	[Date]
1.6 Data Communications Service Fault Fix	1.0	[Date]
1.7 Internal Telephone System Fault Fix	1.0	[Date]
1.8 Peripheral & Routing Hardware Fault Fix	1.0	[Date]
1.9 Supplier Communications	1.0	[Date]
1.10 Applications Recovery to Server	1.0	[Date]
1.11 Data Recovery to Server	1.0	[Date]
2.1 Change of Account Manager Letter	1.0	[Date]
2.2 Interim Customer Order Process	1.0	[Date]
2.3 Customer Communications	1.0	[Date]
2.4 Key Account Review	1.0	[Date]
2.5 Workload & Delivery Assessment	1.0	[Date]
3.1 Staff Communications	1.0	[Date]
3.2 Press Communications	1.0	[Date]
3.3 Fire and Evacuation	1.0	[Date]

3.4 Situation Management Team Comms	1.0	[Date]
3.5 Damage Assessment and Salvage	1.0	[Date]
3.6 Situation Management Team Meetings	1.0	[Date]
3.7 Invocation of Situation Management Centre	1.0	[Date]
3.8 Diversion of Telephony & Fax	1.0	[Date]
3.9 Interim Recruitment	1.0	[Date]
3.10 Recruitment	1.0	[Date]
3.11 Reallocation of resource letter	1.0	[Date]
3.12 New Employee Induction Procedure	1.0	[Date]
4.1 Identify Alternate for Workload	1.0	[Date]
4.2 Assess & Prioritise Current Workload	1.0	[Date]

Appendices Control Sheet

Appendix 1: Customer Contact List	1.0	[Date]
Appendix 2: Risk Assessments	1.0	[Date]
Appendix 3: Ts & Cs of Employment	1.0	[Date]
Appendix 4: Ts & Cs of Sale	1.0	[Date]
Appendix 5: Internal IT Configuration Diagram	1.0	[Date]
Appendix 6: Company Key Details Sheet	1.0	[Date]
Appendix 7: Insurance Certificates Copies	1.0	[Date]
Appendix X: [Other relevant documents]	1.0	[Date]

5. BUSINESS CONTINUITY PLAN – ROLES

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

Plan Owner

Responsible for controlling input to, review and circulation of the BC Plan 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 Business Continuity Planning to combat Threats to Infrastructure Operations, so as to reduce, or remove the impact and/or duration of such Threats. Also responsible for defining and executing policy 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 NMO 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. 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 minimize the likelihood of a Threat to the business, through loss, or underperformance of a Supplier to Technical Operations. 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 minimize 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 conducting adequate Risk Assessments to the Sales & Marketing Operations of the business and establishing effective Business Continuity Planning to combat Threats to these Operations, so as to reduce, or remove the impact and/or duration of such Threats.

Responsible for ensuring the People, Processes and Technology required are in place to maintain NMO 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 (FAO)

Overall ownership and co-ordination of crisis management and business operational recovery for the relevant Functional Area, howsoever defined by the business. Responsible for Plan maintenance, policy, review and testing activities relevant to the Functional Area. 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. Company's designated sub-level Functional Area Owners are as follows:

Product Development Owner

Overall responsibility for defining, communicating and implementing policy to ensure resilience of Product Development activities against potential Threats to NMO. Responsible for defining the operational response to an Incident/Situation in this area. Overall responsibility for minimizing 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 NMO following all anticipated business disruptions.

ICT Owner

Overall responsibility for defining, communicating and implementing policy to ensure resilience of Information and Communications Technology (ICT) activities against potential Threats to NMO. Responsible for defining the operational response to an Incident/Situation in this area. Overall responsibility for minimizing 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 NMO following all anticipated business disruptions.

Human Resources Owner

Overall responsibility for defining, communicating and implementing policy to ensure resilience of Human Resources activities against potential Threats to NMO. Responsible for defining the operational response to an Incident/Situation in this area. Overall responsibility for minimizing 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 NMO following all anticipated business disruptions. Ensuring the welfare needs of staff are met during a Situation. Sourcing interim, or replacement staff as appropriate to the Situation.

Customer Communications Owner

Responsible for ensuring Customers are informed of Situations, as directed by the Situation Management Team (SMT). Responsible for scripting corporate messages for Customers. Notifying Customers when NMO will be/has been restored and what (if anything) will be done to avoid the same scenario happening in the future.

Supplier Communications Owner

Responsible for ensuring that relevant suppliers are informed of a Situation, to the extent required, as directed by the SMT. 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

Overall responsibility for defining, communicating and implementing policy to ensure resilience of Finance activities against potential Threats to NMO. Responsible for defining the operational response to an Incident/Situation in this area. Overall responsibility for minimizing 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 NMO following all anticipated business disruptions. 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 minimize the effects of the Situation on the business. Managing all exceptional financial transactions during a situation, including all insurance and banking matters arising.

Media Handling Owner

Responsible for nominating spokespersons and approving press releases, statements and stories to be used in media handling.

Third Parties Owner

Responsible for defining the Member list of third party contacts within organizations on which this BC Plan has some dependency for execution.

Plan Holders

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

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

5. OWNERSHIP AND CONTACT GROUPS

PLAN OWNER

[Plan Owner]

INFRASTRUCTURE OPERATIONS

Owner: [Owner]

TECHNICAL OPERATIONS

Owner: [Owner]
Members:

SALES & MARKETING OPERATIONS

Owner: [Owner]
Members:

FUNCTIONAL AREAS

Owner: [Owner]

PRODUCT DEVELOPMENT

Owner: [Owner]

ICT

Owner: [Owner]

HUMAN RESOURCES

Owner: [Owner]

CUSTOMER COMMUNICATIONS

Owner: [Owner]
Members:

SUPPLIER COMMUNICATIONS

Owner: [Owner]
Members:

FINANCE

Owner: [Owner]

MEDIA HANDLING

Owner: [Owner]
Members:

THIRD PARTIES

Owner: [Owner]

PLAN HOLDERS

Owner: [Owner]

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

6. ACTION PLANS SUMMARY

The following action plans have been developed in response to identified potential Threats to the Company business and the Risk Assessments made in connection with those identified Threats. Each Action Plan is designed to achieve Company's intended Recovery Time Objective, arising from the Company Business Impact Analysis.

AP001 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. Refer to the Risk Assessment/Loss of Personnel entry in Appendix 2.

AP002 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 Mode of Operations are threatened, or actually interrupted. Refer to the Risk Assessment for Loss of Infrastructure in Appendix 2.

AP003 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. Refer to the Risk Assessment for Loss of Infrastructure in Appendix 2.

AP004 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. Refer to the Risk Assessment for Loss of Infrastructure in Appendix 2.

AP005 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. Refer to the Risk Assessment for Loss of Infrastructure in Appendix 2.

AP006 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 NMO conditions. Refer to the Risk Assessment for Loss of Data in Appendix 2.

AP007 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. Refer to the Risk Assessment/Threat to Wellbeing of Staff in Appendix 2.

AP 001 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 Account Handler: Long Term	1. Identify Alternates to take on Workload 2. Advise clients of interim and/or permanent changes 3. Consider re-assignment of specific account responsibilities to other account handlers 4. Assess current/imminent activity and projects 5. Consider re-assignment of specific account responsibilities to Senior Managers 6. Advise Staff	4.1 Identify Alternate for Workload 2.1 Change of Account Manager Letter 5.4 Key Account Review 2.4 Key Account Review 2.4 Key Account Review 3.1 Staff Communications
Key Account Handler: Permanent	1. Advise Clients of interim, or permanent changes 2. Assess current/imminent activity and projects 3. Consider re-assignment of specific account responsibilities to other account handlers 4. Consider re-assignment of specific account 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 5. Advise suppliers as appropriate 6. Advise Staff	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
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	1. Assess & prioritise current Workload 2. Decide whether clients will be materially affected and advise as appropriate	4.2 Assess/Prioritise Current Workload 3.11 Reallocation of Resource Letter

Term	3. Review cause and recruit replacement staff as appropriate 4. Engage additional resources from suppliers	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 002 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 Operations are threatened, or actually interrupted. Refer to the Risk Assessment for Loss of Infrastructure in Appendix 2.

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 NMO 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

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

AP 003 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. Refer to the Risk Assessment for Loss of Infrastructure in Appendix 2.

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 company 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 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 004 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. Refer to the Risk Assessment for Loss of Infrastructure in Appendix 2.

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 company facilities within the Premises are unaffected 2. Ensure SMT leaders are aware	3.6 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	2.4 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	1.4 Physical Recovery 3.2 Staff Communications 2.4 Customer Communications 1.9 Supplier Communications

AP 005 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. Refer to the Risk Assessment for Loss of Infrastructure in Appendix 2.

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

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

AP 006 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 NMO conditions. Refer to the Risk Assessment for Loss of Infrastructure in Appendix 2.

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

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

AP 007 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. Refer to the Risk Assessment for Loss of Infrastructure in Appendix 2.

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

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

7. PROCEDURES SUMMARY

NAME	VERS.	DATE	NUM.
TECHNICAL OPERATIONS			
Faulty Workstation Evaluation	1.0	[Date]	**1.1**
Replace Hardware Device	1.0	[Date]	**1.2**
Physical Recovery	1.0	[Date]	**1.3**
Invocation of Emergency Call Routing Procedures	1.0	[Date]	**1.4**
Disable Key Application Server	1.0	[Date]	**1.5**
Data Communications Service Fault Resolution	1.0	[Date]	**1.6**
Internal Telephone System Fault Resolution	1.0	[Date]	**1.7**
Peripheral & Routing Hardware Fault Resolution	1.0	[Date]	**1.8**
Supplier Communications	1.0	[Date]	**1.9**
Applications Recovery to Server	1.0	[Date]	**1.10**
Data Recovery to Server	1.0	[Date]	**1.11**
[Other Technical Procedures]	1.0	[Date]	**1.12**
SALES & MARKETING OPERATIONS			
Change of Account Manager Letter	1.0	[Date]	**2.1**
Interim Customer Order Process	1.0	[Date]	**2.2**
Customer Communications	1.0	[Date]	**2.3**
Key Account Review	1.0	[Date]	**2.4**
Workload & Delivery Assessment	1.0	[Date]	**2.5**
[Other Sales & Marketing Procedures]	1.0	[Date]	**2.6**
INFRASTRUCTURE OPERATIONS			
Staff Communications	1.0	[Date]	**3.1**
Press Communications	1.0	[Date]	**3.2**
Fire & Evacuation	1.0	[Date]	**3.3**
Situation Management Team Communications	1.0	[Date]	**3.4**
Damage Assessment & Salvage	1.0	[Date]	**3.5**
Situation Management Team Meetings	1.0	[Date]	**3.6**
Invocation of Situation Management Centre	1.0	[Date]	**3.7**
Diversion of Telephony & Fax	1.0	[Date]	**3.8**
Interim Recruitment	1.0	[Date]	**3.9**
Recruitment	1.0	[Date]	**3.10**
Reallocation of Resource Letter	1.0	[Date]	**3.11**
New Employee Induction Procedure	1.0	[Date]	**3.12**
Staff Protection Procedure	1.0	[Date]	**3.13**
[Other Infrastructure Operations Procedures]	1.0	[Date]	**3.14**
GENERAL			
Identify Alternate for Workload	1.0	[Date]	**4.1**
Assess & Prioritise Current Workload	1.0	[Date]	**4.2**
[Other General Procedures]	1.0	[Date]	**4.3**

NOTE: THESE PROCEDURES *MUST* BE ADAPTED TO SUIT YOUR BUSINESS!

8. PROCEDURES

P1.1 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 OPM
4. Identify if fault is a known software problem that can be remedied by applying patch, or upgrade. If so, apply the patch/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.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P1.2 TECHNICAL OPERATIONS – REPLACE HARDWARE DEVICE

1. Assess if faulty device can be fixed by replacing/repairing faulty component (eg 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/benefit of sourcing replacements from remote locations, versus local purchase from local sources, factoring in lead time considerations.
4. Reroute user Services to Secondary platforms, subject to cost/benefit assessment in terms of time estimated to recover NMO for User.
5. Purchase replacement device as necessary.
6. Purchase additional replacement devices as necessary, as contingency, if considered beneficial to shorten future recovery to NMO by Functional Area Owner, out of discretionary budget.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P1.3 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:** If physical damage occurs to the [Location] address, [Regus] are accountable for effecting such repairs and providing alternative temporary Premises in the local area in the interim.
5. **Manufacturing & Related Facilities:** [The only such operational premises occupied by the company are the responsibility of outsourced service providers, with their activities governed by the relevant contractual conditions covering such circumstances].

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P1.4 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 0870 telephone lines to designated alternate numbers, as specified by any member of the SMT.
3. Revert to original routing number when NMO conditions are resumed.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P1.5 TECHNICAL OPERATIONS – DISABLE KEY APPLICATION SERVER

1. Notify affected users informing them of relevant server shut down at 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.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

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 on-site facilities at [Regus] and inform them of the fault, for escalation to their own service provider, during office hours.
3. Outside of office hours, notify [the on-duty security guard].
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. Request the diverting of the line to an alternate number, such as an SMT-designated mobile phone.
7. Ask BT to place a message on the relevant line advising callers of the fault, if necessary.
8. Report expected duration of function loss to relevant staff, suppliers & customers as necessary.
9. Switch to alternate communications methods as appropriate.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P1.7 TECHNICAL OPERATIONS – INTERNAL PHONE FAULT RESOLUTION

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

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P1.8 T/OPS – 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 NMO after installation.
6. Consider cost-benefit of buying spare units of the failing component, or implementing alternative, more resilient technical solution.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P1.9 TECHNICAL OPERATIONS – SUPPLIER COMMUNICATIONS

1. Identify list of suppliers materially affected.
2. Determine the nature, frequency & content of the communication, [using the Criticall *Emergency*Call notification system, or] 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 NMO procedures between organizations.
5. Keep suppliers informed regarding likely resumption of NMO and when it is actually achieved.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P1.10 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.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P1.11 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 NMO.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P1.12 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 [Operations Manager] 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.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P2.1 SALES & MARKETING OPERATIONS – CHANGE ACCOUNT MANAGER

This letter is stored as a Word file on the Company 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 minimize 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]

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P2.2 SALES & MARKETING OPERATIONS – INTERIM 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 SLAs, 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 [using the Criticall *Emergency*Call notification system] .

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P2.3 SALES & MARKETING OPERATIONS – CUSTOMER COMMUNICATIONS

1. The Account Contact List is held on the [Salesforce online database], at [www.salesforce.com]. Username is [Username] and the password is known by [Persons].
2. The SMT will determine, with the Account Manager(s), who should contact which customer and in what way, for example [using the Criticall *Emergency*Call notification system].
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/other type of incident and we cannot use the premises for the time being. Fortunately, the relevant section of our Business Continuity Plan has been invoked and we are in the process of returning to normal operational capacity. As an organization, we are built to operate effectively as a virtual team and the our 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 your data safely held. If there will be any foreseeable impact upon [our committed deliverables to you], we will be in touch within X hours/days to confirm."

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P2.4 SALES & MARKETING OPERATIONS – KEY ACCOUNT REVIEW

1. Collate list of all affected accounts.
2. Review outstanding sales activities and committed deliverables, using the latest information on the [salesforce.com] database, and/or the latest Sales Progress Report.
3. Prioritise immediate actions that need to be addressed.
4. Reallocate workload to another Account Manager, or Senior Manager as required.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P2.5 SALES & MARKETING OPERATIONS – WORK & DELIVERY ASSESSMENT

1. Assessment of anticipated operational capacity to cope with customer order & deliverables workload in expected timescales.
2. Reconcile open orders with revised estimates of capacity, including prioritisation.
3. Assess supplier production capacity against cost benefits of changing scope of engagement and lead times.
4. Formulate plan to best match operational capacity with expectations & engage plan to notify customers & suppliers.
5. Produce revised order fulfillment schedule.
6. Monitor revised schedule to assess need for new iteration of this process, until the NMO is resumed.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P3.1 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 NMO, 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/broadcast to notify staff according to agreed, scripted message, [using the Criticall *Emergency*Call notification system].
    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 home 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 [5am] to notify them at home [using the Criticall *Emergency*Call notification system]. 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 NMO has been resumed.

P3.2 INFRASTRUCTURE OPERATIONS – PRESS COMMUNICATIONS

1. Unless specifically authorised by the Situation Management Team, no comment should be made to the Press. If approached, staff response should be "no comment" and enquiries should be referred to the Situation Management Team.
2. The default spokesperson in Situations will be Ian Hammond. When Ian is unavailable, the SMT shall nominate the most appropriate alternative, which will be Gary Shepherd, then Colin Hammond, 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. Company has no specific obligations with respect to notifying the Public concerning incidents at its [2] 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.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P3.3 INFRASTRUCTURE OPERATIONS – FIRE & EVACUATION

1. This procedure is to be used in the event of a fire at [Locations]
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 to 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.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P3.4 INFRASTRUCTURE OPERATIONS – SMT COMMUNICATIONS

1. The following should be used for contact between members of the Situation Management Team in connection with Business Continuity Incidents & Situations.
2. Regardless of time, [using the Criticall *Emergency*Call notification system], contact SMT members by the following means, in order, until successful Mobile telephone
    a. Home 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 SM Team and their contact details appear in the Contacts section of this BC Plan.
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)

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P3.5 INFRASTRUCTURE OPERATIONS – DAMAGE ASSESSMENT & SALVAGE

1. In the event of a physical incident where losses and/or damage are likely, [Salvage Contractor], who have been pre-appointed as salvage contractor provide a 24 hour response services.
2. Call [Salvage Contractor's] 24 hour response service on [Number] - quote contract No. [654321].
3. Provide information requested – [Contractor] will attend site within 4 hours to begin salvage operations, liaise with insurers & loss adjuster, and expedite the recovery process.
4. Given the small amount of material involved, any damaged items should be transported by hired vehicles as necessary, to [Person's] garage, at [Address].

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P3.6 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. [Alternative Site 1]
    b. [Holiday Inn, J4 of M4]
    c. [Holiday Inn, J4 of M40]
2. The objectives for Day 1 of this type of incident would be:
    a. The standing agenda for the meetings will be:
    b. Casualties, injuries and fatalities, to be recorded
    c. Nature/duration of denial of access - Likelihood of regaining access to premises - Implementation of emergency workplaces
    d. Losses, damage & salvage
    e. Customer communications
    f. Impact on customers' orders/deliveries
    g. Supplier communications
    h. Stakeholders
    i. Insurance and finance
    j. Prioritise Workload & Roles within SMT
    k. Staff Communications
    l. Date/time/venue of next meeting
    m. AOB

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P3.7 INFRASTRUCTURE OPS – 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 NMO.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P3.8 INFRASTRUCTURE OPERATIONS – DIVERT TELEPHONE & FAX

1. Company operates 0870 smart numbers that can be diverted to any underlying number by BT's smart network.
2. The main company phone number is 0870 [Number].
3. The main fax number is 0870 [Number].
4. The main support number is 0870[Number].
5. Once NMO is restored, divert the relevant smart number back to their defaults.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P3.9 INFRASTRUCTURE OPERATIONS – INTERIM RECRUITMENT

1. For recruiting senior or key account managers, obtain authority from [Authority] for new position or interim position and determine length of contract.
2. Approach [selected recruitment agency] to discuss job spec
3. Obtain approval for and agree contract with [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 probation period in the company

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P3.10 INFRASTRUCTURE OPERATIONS – RECRUITMENT

1. Obtain authority from CEO for new position, including detailed job specification and business case.
2. Approach [agencies] to discuss job specification
3. Obtain approval for and agree commercials with [agency]
4. Interview and shortlist candidates
5. Make offer to selected candidate
6. Take candidate through induction procedure.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P3.11 INFRASTRUCTURE OPERATIONS – REALLOCATE RESOURCE LETTER

This letter is held as a Word file on the Company 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 and your people. {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 [the usual 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.

Yours Sincerely,

[Person]
[Title]

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P3.12 INFRASTRUCTURE OPERATIONS – NEW EMPLOYEE INDUCTION

1. Ensure employee's details are registered in company 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 date 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.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P3.13 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/group is aware of the potential harm.
3. Seek to communicate with the individual/group to direct them away from the Threat, and towards safety, with respect to their location.
4. Seek to educate the individual/group concerning the nature of the Threat, to avoid, or minimize 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 NMO, where appropriate.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P4.1 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/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.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

P4.2 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. Co-ordinator (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 conferenced in
4. Co-ordinator 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/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 process until Workload issues are resolved, and Normal Mode of Operations is resumed.

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

9. APPENDICES

	VERSION	LAST UPDATED
Appendix 1: Full Customer Contact List	1.0	[Date]
Appendix 2: Risk Assessments	1.0	[Date]
Appendix 3: Recovery Time Objectives	1.0	[Date]
Appendix 4: Ts & Cs of Employment	1.0	[Date]
Appendix 5: Software Ts & Cs of Sale	1.0	[Date]
Appendix 6: Internal IT Configuration Diagram	1.0	[Date]
Appendix 7: Company Key Details Sheet	1.0	[Date]
Appendix 8: Insurance Certificate Copy	1.0	[Date]
Appendix X: [Other Relevant Documents[	1.0	[Date]

Version: 1.0
Last Reviewed/Updated: [Date]
Next Review Scheduled: [Date]

[For electronic copy of generic Risk **Assessment & Business Impact Analysis** spreadsheet in Excel, email request to jonathan.stuart@criticall.co.uk]