Gi GROUP UK POLICY

Business Continuity Plan

OBJECTIVE

The objective of the Gi Group's Business Continuity Plan is to ensure that in the event of a major failure to our key systems or processes caused by a man made event or natural disaster our critical business activities continue to operate as effectively as possible until normality can be re-established.

PLAN GENERATION PROCESS

The plan has been created by completing the following stages:

1. Conducting a Business Process Analysis by:
   - Determining the critical services or assets needed to run the business
   - Identifying the most serious threats to these critical items
   - Assessing the probability of these risks and the resultant business impact
   - Defining the maximum tolerable disruption to the critical services or assets

2. Defining the key actions points that, when implemented within a given timescale, will result in the minimum level of disruption. The plan has been designed to apply to both our high street locations within the branch network and our SMS locations that are based on a client's premises. All SMS locations are required to liaise with the client to ensure that the plan dovetails with the companies own policy/plan. The key actions have been categorised as follows:

   - Emergency actions that focus on the immediate steps required to report the incident to all relevant parties and if possible immediately restore damaged facilities and equipment
   - Contingency actions that focus on the steps required to find alternative solutions if facilities, equipment and assets cannot be immediately restored
   - Continuity actions focus on managing relationships with clients and suppliers and identifying how service levels will be maintained
   - Crisis actions focus on protecting the company's reputation and legal standing and where necessary dealing with press or public reaction to events

3. Identifying the individuals who will form the following response teams that will take on board the responsibility for executing the relevant action:

   - Emergency Response Team (ERT)
   - Business Continuity Team (BCT)
   - Crisis Management Team (CRT)
   - Pandemic Response Team (PRT)

CRITICAL BUSINESS PROCESSES

The analysis determined that in the event of an incident priority should be given to maintaining the following processes and the essential services/assets that support them:

- Maintaining existing client relationships
- Payment of temporary workers and permanent employees
- The recruitment and supply of temporary workers and permanent candidates
- New business generation

Essential facilities and assets:

- Suitable premises
- Competent members of staff
- Communication equipment
- Accurate live data
- Secure archived data
- Suppliers
- Cash flow

Group
YOUR JOB, OUR WORK

The key risks to the functionality of our critical business processes have been identified as being:

- Fire
- Flooding
- Theft
- Vandalism
- Civil Disorder
- Power loss
- Viruses
- Accidents
- Pandemics
- Serious breach of company policy – non IT related.

The following tables take each key risk in turn, clarifies the response team members and confirms the action required at each stage to ensure that the minimum level of disruption is experienced by all those directly affected.

The actions identified within each table will be supported by the specific post-incident processes that are detailed within the supporting company policies. Each policy also details the pre-incident activity that lies within our realm of control in order to prevent a set of circumstances that leads to the need for the Business Continuity Plan to be brought into play.

Each response team will consist of the following appointed personnel who will all have received a full briefing on their individual responsibility for implementing the various stages of the overall business continuity plan. The briefing will have been supported by any training deemed to be required to enable each team member to carry out their role effectively.

Response Team Members:

Location Manager – LM
Senior Manager – SM
Divisional Director – DD
IT Manager – ITM
HR Manager – HRM
Health and Safety Manager – HSM
Training and Compliance Manager – TCM
Chief Executive Officer – CEO

FIRE AT SUITABLE PREMISES	
Response teams	ERT - LM, SM, HSM BCT - LM, SM, HSM, TCM, ITM CMT - DD, HRM, CEO
Emergency action ERT	• Evacuate the building, as per the company fire prevention policy • Notify the emergency services • Ensure all staff are safe • Assess the damage to the property, office equipment and records • Inform property agents • Establish temporary communication links • Provide a full evaluation of the situation • Escalate the next stage of the plan to the BCT
Contingency action BCT	• Locate alternative temporary premises • Source and install communications and general office equipment • Generate new paper records. • Inform all relevant parties of new contact details • Escalate the need for any crisis action to the CMT
Continuity action BCT	• Assess the damage to the current premises, inform insurers. • Establish a refurbishment programme or, if applicable, identify new premises
Crisis action CMT	• In the case of serious injury or fatality notify all relevant parties
Supporting company policy	• Fire Prevention Policy

FLOODING AT SUITABLE PREMISES

Response teams	ERT - LM, SM, HSM BCT - LM, SM, HSM, TCM, ITM CMT - DD, HRM, CEO
Emergency action ERT	• If required identify the source of the flood and take any remedial action • Ensure the electricity supply has been switched off • Notify the relevant emergency services of the incident. • Ensure all staff are safe. • Assess the damage to the property, office equipment and records. Inform property agents. • Establish whether we can continue to operate from the location or determine that alternative premises need to be found • Provide a full evaluation of the situation • Escalate the next stage of the plan to the BCT
Contingency action BCT	• Locate alternative temporary premises • Source and install communications and general equipment • Generate new paper records • Inform all relevant parties of the new contact details • Escalate the need for any crisis action to the CMT.
Continuity action BCT	• Assess the damage to the current premises notify insurers and establish a refurb programme or, if applicable, identify new premises.
Crisis action CMT	• In the case of serious injury or fatality notify all relevant parties.
Supporting company policy	• To be developed

THEFT OF OFFICE EQUIPMENT, SENSITIVE DATA OR VANDALISM (INCLUSIVE OF CIVIL DISORDER) AT SUITABLE PREMISES

Response teams	ERT – LM, SM, ITM BCT – LM,SM,ITM CMT – LM,SM,DD,CEO,ITM
Emergency action ERT	• In the case of loss of equipment or sensitive data due to theft/vandalism, notify the emergency services if they are not already aware of the incident • Ensure that the ITM is provided with a full appraisal of the situation as soon as possible to ensure that the relevant security measures required to protect any sensitive data are taken with immediate effect. • Assess the damage to the infrastructure of the location and inform the property agents • Establish whether we can continue to operate from the location or determine that alternative premises need to be found • If required establish temporary communication links. • Obtain a full evaluation of the situation and depending on the immediate level of disruption to our processes or the level of risk attached to the loss of data, escalate the next level of the plan to the BCT or the CMT • In the case of serious vandalism ensure that the premises are secure when unoccupied.
Contingency action BCT	• In the case of serious vandalism locate alternative temporary premises • Source and install communications and general office equipment • Generate new paper records • Inform all relevant parties of new the contact details
Continuity action BCT	• In the case of data theft; data would be restored from the latest back up. • In the case of equipment theft; if immediately available temporary equipment would be provided whilst permanent replacement equipment is provided.
Crisis action CMT	• Appraise all relevant parties directly affected by the data theft of the current situation and the action being taken to resolve the situation. Also provide the details of any recommended action that they would be advised to take.
Supporting company policy	• Acceptable Use of IT and Computer Systems

POWER LOSS AT SUITABLE PREMISES	
Response teams	ERT – LM, SM, ITM BCT –LM,SM,ITM CMT – LM,SM,ITM,DD
Emergency action ERT	• Establish the nature of the power loss • Notify the relevant authorities and establish the likely duration of the outage • Establish temporary communication links • Provide a full evaluation of the situation • Escalate the next stage of the plan to the BCT
Contingency action BCT	• Establish alternative processes to ensure all key activities continue to take place with the minimal level of disruption to all relevant parties • Establish alternative premises to ensure all key activities continue to take place with the minimal level of disruption to all relevant parties • Inform all relevant parties of any potential delay in the delivery of our essential services
Continuity action BCT	• Once power has been restored review the overall effectiveness of the alternative processes and their ongoing suitability to supporting the business in the event of another loss of power of the same magnitude. • Implement any improvements with immediate effect and support with training where required.
Crisis action CMT	• In situations where essential services will not be provided for a sustained period of time notify all relevant parties with immediate effect.
Supporting company policy	• To be developed

VIRUSES TO EQUIPMENT AT SUITABLE PREMISES	
Response teams	ERT – LM, SM, ITM BCT – ITM,DD,TCM CMT - ITM,LM,SM,DD,HRM,HSM,TCM,CEO.
Emergency action ERT	• Establish the source and the severity of the virus • Where possible remove the virus from the system • Provide a full evaluation of the situation • Escalate the next stage of the plan to the BCT/CMT
Contingency action BCT	• Where a virus cannot be removed immediately the affected hardware / data will be removed from the company network and revert to paper based systems where required
Continuity action BCT	• If the virus cannot be removed the affected hardware / software may be supplied by a stand-a-lone system for data reference and may have to be re-created.
Crisis action CMT	• Where a virus cannot be removed immediately the affected hardware / data will be removed from the company network • Appraise any parties put at high risk due to the virus of the situation and what action we are taking to minimise the risk.Also provide the details of any recommended action that they would be advised to take.
Supporting company policy	• Acceptable Use of IT and Computer Systems

SERIOUS ACCIDENTS INVOLVING INTERNAL EMPLOYEES AND TEMPORARY WORKERS	
Response teams	ERT – HSM, HRM, DD BCT – LM, SM, HRM, DD, CEO CMT – HRM, DD, CEO
Emergency action ERT	• Obtain the full details of the accident and record as per the company accident reporting procedure. • Work with the relevant emergency services to co-ordinate the communication of the accident to the next of kin of all of those involved and provide support and guidance where required • Where the incident occurred at a client's premises, work with the relevant contacts on any subsequent investigation • Depending on the nature of the accident either continue to manage the incident themselves or escalate the next stage to the BCT or CMT.
Contingency action BCT/CMT	• Source alternative members of staff to provide temporary cover for those directly affected by the accident.
Continuity action BCT/CMT	• Review the relevant company policy relating to the cause of the accident and if applicable amend the content re distribute across the network and deliver any training required to support the revised policy content. • Source alternative members of staff to replace those directly affected by the accident that will not be returning to work.
Crisis action CMT	• Co-ordinate the communication of the accident and the action that will take place as a result to all relevant parties such as the operational network, clients, suppliers and the media.
Supporting company policy	• Health and Safety Policy, Driving Policy

PANDEMICS	
Response teams	PRT – HRM, DD, CEO
Emergency action	• The PRT will convene with immediate effect and implement the necessary steps identified in the Pandemic Response Policy until the threat to the business has been contained.
Contingency action	• Detailed in Pandemic Response Policy
Continuity action	• Detailed in Pandemic Response Policy
Crisis action	• Detailed in Pandemic Response Policy
Supporting company policy	• Pandemic Response Policy

SERIOUS BREACH OF COMPANY POLICY BY INTERNAL EMPLOYEES	
Response teams	ERT –SM,HRM,TCM,DD BCT – SM,HRM,DD,CEO,HSM,TCM CMT – HRM, DD, CEO.
Emergency action ERT	• Clarify both the nature of the breach of policy and the level of risked posed both to the business and individuals. • Provide a full evaluation of the situation • Escalate the next stage of the plan to the BCT /CMT
Contingency action BCT/CMT	• Ensure a full investigation has taken place in accordance with the disciplinary and grievance policy • Instigate any relevant disciplinary action against the individual(s) involved • Notify any clients and temporary workers that are effected by the breach • Notify the relevant emergency services • Notify the relevant governing bodies or trade association
Continuity action BCT/CMT	• Review the relevant company policy relating to the cause of the breach and if applicable amend the content re distribute across the network and deliver any training required to support the revised policy content.
Crisis action CMT	• Co ordinate the communication of the incident and the action that will take place as a result to all the relevant parties such as the operational network, clients ,suppliers and the media.
Supporting company policy	• All company policies inclusive of disciplinary and grievance policy.

EXTERNAL SUPPLIERS AND CASH FLOW

The Analysis identified that any major disruption to the following Essential Facilities would pose the biggest risk to our business:

- Communications Equipment and Support.
  All current and potential future suppliers of communications equipment and support will be expected to have their own business continuity plan in place. The plan should satisfy the relevant buyer/relationship holder that in the occurrence of an event which affects the suppliers' ability to provide goods or service's to the level required, the Gi Group experience's the minimal amount of disruption to its day to day activities.

- Financial Support.
  In the event that current funding streams are directly affected by events beyond the providers' control, any potential shortfall will be underwritten by the overall holding company.

- Limitations of the Plan
  Advance planning for a major incident can help to reduce both the likelihood of its occurrence and its impact. It is impossible however to predict future events and developments with accuracy and we can only take an educated guess as to how certain events may unfold and provide a broad brush estimate of possible developments.

- Plan Review
  The content of the plan will be reviewed every 6 months or when:
  There is a major change to premises, processes, equipment or services.
  A new threat emerges that threatens to disrupt our day to day business activities.
  The review of the plan will focus on identifying any single points of failure, further actions that can be taken to reduce the risk to our critical services or assets and the opportunities that we have to speed up our recovery and response processes.