Business Continuity Plan

Gi Group understands the critical importance of maintaining uninterrupted service delivery. As such, we recognise the importance of having robust plans in place to ensure we can minimise disruption and maintain continuity of service for all stakeholders, including our valued workforce and clients.
The purpose of this Business Continuity Plan is to document the action steps that we would put in place in the event of an emergency. The plan considers the following emergencies, taking each one by turn and clarifying the actions required at each stage in order to minimise disruption:

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

PLAN

Critical Documents

As part of our plan, we will require all locations to upload critical documents that would allow them to perform essential services to an Offline Secure Backup System, which staff will be able to access in an emergency situation. It is also proposed that each location should hold written instructions, which should include:

- Names and contact details for who to contact in a situation where we are unable to operate normally
- A 'How to Guide' detailing how to ensure essential services are maintained

Responsibilities

The plan includes the following Response Teams:

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

The Response Teams will be made up of the following Personnel:

- Location Manager – LM
- Senior Manager – SM
- Divisional Director – DD
- IT Director – ITD
- Group Head of People – GHP
- Health and Safety Manager – HSM
- Head of Compliance – HC
- Chief Executive Officer – CEO
- Head of Payroll Services – HP

Risks

Fire

Emergency Action (ERT made up of LM, SM, HSM)

- 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 made up of LM, SM, HSM, HC, ITD)

- 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 made up of LM, SM, HSM, HC, ITD)

- Assess the damage to the current premises, inform insurers.
- Establish a refurbishment programme or, if applicable, identify new premises

Crisis Action (CMT made up of DD, GHP, CEO)

- In the case of serious injury or fatality notify all relevant parties

Flooding

Emergency Action (ERT made up of LM, SM, HSM)

- 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 Made up of LM, SM, HSM, HC, ITD)

- 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 Made up of LM, SM, HSM, HC, ITD)

- Assess the damage to the current premises notify insurers and establish a refurb programme or, if applicable, identify new premises.

Crisis Action (CMT made up of DD, GHP, CEO)

- In the case of serious injury or fatality notify all relevant parties.

Theft of Office Equipment, Sensitive Data or Vandalism (inclusive of Civil Disorder)

Emergency Action (ERT made up of LM, SM, ITD)

- 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 made up of LM, SM, ITD)

- In the case of serious vandalism locate alternative temporary premises BCT
- Source and install communications and general office equipment
- Generate new paper records
- Inform all relevant parties of new the contact details

Continuity Action (BCT made up of LM, SM, ITD)

- 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 made up of LM, SM, DD, CEO, ITD)

- 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.

Power Loss

Emergency Action (ERT made up of LM, SM, ITD)

- 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 made up of LM, SM, ITD)

- 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 made up of LM, SM, ITD)

- 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 made up of LM, SM, ITD, DD)

- In situations where essential services will not be provided for a sustained period of time notify all relevant parties with immediate effect.

Viruses to Equipment

Emergency Action (ERT made up of LM, SM, ITD)

- 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 made up of ITD, DD, HC)

- 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 made up of ITD, DD, HC)

- 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 made up of ITD, LM, SM, DD, GHP, HSM, HC, CEO)

- 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.

Serious Accidents Involving Internal Employees and Temporary Workers

Emergency Action (ERT made up of HSM, GHP, DD)

- 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 made up of LM, SM, GHP, DD, CEO) and CMT made up of GHP, DD, CEO)

- Source alternative members of staff to provide temporary cover for those directly affected by the accident.

Continuity Action (BCT made up of LM, SM, GHP, DD, CEO) and CMT made up of GHP, DD, CEO)

- 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 made up of GHP, DD, CEO)

- 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.

Pandemics

Emergency Action (PRT made up of GHP, DD, CEO)

- 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.

Serious Breach of Company Policy by Internal Employees

Emergency Action (ERT made up of SM, GHP, HC, DD)

- 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 made up of SM, GHP, DD, CEO, HSM, HC and CMT made up of GHP, DD, CEO)

- 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 affected by the breach
- Notify the relevant emergency services
- Notify the relevant governing bodies or trade association

Continuity Action (BCT made up of SM, GHP, DD, CEO, HSM, HC and CMT made up of GHP, DD, CEO)

- 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 made up of GHO, DD, CEO)

- Coordinate 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.

Cyber Attack Impacting the Functionality of the Approved Timesheet System

Emergency Action (EMT made up of LM, SM)

- Notify ITD and HC
- ITD identify the level of impact, and report to BCT
- LM, SM notify client (verbally / email) and workforce (via the Payroll System)

Contingency Action (BCT made up of LM, SM, ITD, HC)

- ITD engage service provider to determine steps for resolution
- Provide a full evaluation of the situation
- Escalate the next stage of the plan to the BCT
- Generate new paper records for signing in / out to include Name, Contact Number, Time In/Out , Managers Name and Signatures
- Using the Daily Timesheets establish current week schedule and utilise excel-based schedule tracker
- Inform all relevant parties of new signing in / out procedure
- Escalate the need for any crisis action to the CMT

Continuity Action (BCT made up of LM, SM, ITD, HC)

- Implement new signing in / out procedure
- Maintain excel-based schedule tracker

Continuity Action (Client)

- Co-operation in facilitating and implementing the signing in / out procedure
- Flexible approach to non-technological confirmation of daily hours / week invoiced hours worked (based upon the signing in / out procedure)
- Co-operation in review and adjustment' of hours worked data / invoices once systems are restored
- Be flexible and understanding with worker where attendence issues occur as direct / indirect result of system issues

Crisis Action (CMT made up of LM, SM, ITD, DD, CEO)

- In the event that incorrect number of operatives attend work, inform client to agree variations to work organisation

Cyber Attack Impacting the Functionality of the Approved Payroll System

Emergency Action (ERT made up of HP, ITD)

- Notify LM, SM, HC
- ITD identify the level of impact, and report to BCT
- LM, SM notify client (verbally / email)

Contingency Action (BCT made up of HP, LM, SM, ITD, HC)

- ITD engage service provider to determine steps for resolution
- Provide a full evaluation of the situation
- Escalate the next stage of the plan to the BCT
- Payroll service provider to provide alternative environment
- Establish and recreate missing data
- Inform all relevant parties (provide training where required) of contingent payroll process
- Escalate the need for any crisis action to the CMT

Continuity Action (BCT made up of HP, LM, SM, ITD, HC)

- Utilise alterative environment to process payroll

Continuity Action (Client)

- Co-operation in review and adjustment' of hours worked data / invoices once systems are restored
- Flexibility and co-operation in relation to any increase in pay queries as a direct / in-direct result of system issues

Crisis Action (CMT made up of ITD, HC, DD, GHP, CEO)

- In the event that the alternative payroll environment fails to make on-time payments / raise on-time invoices notify all interested parties

Functions

The Business Process Analysis also highlighted functions within the company that are essential. As part of this Business Continuity Plan, we have, therefore considered these functions alongside the risks and have planned steps that detail how these functions can be delivered in an emergency situation.

The following functions have been identified as essential and have been documented within this plan.

- Marketing and PR Activities
- Payroll
- Credit Control
- Candidate Registrations
- RTW Document Collection
- Client Management
- Information Technology (Including Training Delivery)

Marketing and PR Activities

Identified Issues

- No access to social media scheduling tools
- Inability to update the company website or post job advertisements
- Delayed communication with the public and stakeholders
- Risk of reputational damage due to a lack of updates

Action Plan

- Use mobile applications or international company contacts to post urgent notices and updates on social media
- Prepare pre-approved messaging templates for use in emergencies
- Coordinate with external PR agency if available
- Maintain a manual log of all public communications

Responsibilities

Primary: Marketing Team
Backup: PR Coordinator and Marketing Director
Oversight: Managing Director and Chief Executive Officer

Communication Protocols

- Post updates via mobile access to social media platforms
- Email press releases from personal accounts if needed or from PR contact
- Daily status updates to stakeholders via SMS or WhatsApp
- Escalate reputational risks to Managing Director and Chief Executive Officer

Payroll

Identified Issues

- Inability to access payroll software or timesheet data
- No access to bank payment systems
- Delays in processing wages for temporary workers

Action Plan

- Activate manual payroll process using pre-downloaded spreadsheets
- Source a secure offline system
- Source an alternative BACS system
- Contact bank via phone to initiate manual payment batches
- Notify workers of delays and provide estimated timelines

Tools Required

Paper Timesheets – Signing in/out to include:

- Name
- Contact number
- Time in/out
- Managers Name and signatures

Secure Offline Backup System to include:

- Full Employee/candidate payroll report (inc payrates)
- Bank Details
- Full Client list (based on current invoicing)
- Consider access to an alternative BACs payment system.

Responsibilities

Primary: Payroll, Finance and IT

Oversight: Finance Director, IT Director, Head of Compliance, Managing Director and Chief Executive Officer
Backup: Head of Payroll, Finance Director, Payroll, IT Team and IT Director

Communication Protocols

- Use SMS and personal email accounts to notify temporary workers
- Provide daily updates to Head of Compliance, Managing Director and Chief Executive Officer
- Notify bank relationship manager via phone

Credit Control

Identified Issues

- No access to aged debt reports or invoicing systems
- Inability to send reminders or reconcile payments
- Risk of cash flow disruption

Action Plan

- Use secure offline backups of timesheet data
- Use printed or exported aged debt reports from last backup
- Contact clients via phone to confirm outstanding balances
- Log payments manually and reconcile once systems are restored
- Activate contingency fund if cash flow is impacted

Responsibilities

Primary: Credit Control Team
Oversight: Finance Director, IT Director and Managing Director

Backup: Finance Director and IT Director

Communication Protocols

- Phone calls to key clients with overdue invoices
- Credit Control to provide daily cash flow update to Finance Director
- Weekly summary to Managing Director and Chief Executive Officer

Candidate Registrations

Identified Issues

- No access to online registration forms or CRM
- Inability to track candidate progress or availability
- Risk of losing new candidate leads

Action Plan

- Use paper-based registration forms stored in offline back system
- Set up temporary registration via secure Google Forms or Microsoft Forms
- Assign staff to manually enter data once systems are restored
- Maintain a spreadsheet log of new registrations

Tools Required

Candidate registrations will need to take place face to face in branch, on-site or at a location close to the site of work. An offline or hard copy of a full registration pack will include:

- RTW – Physical check, photo, onsite or in branch
- Application Form, Industrial, Driving, Commercial, Permanent
- Candidate Assignment Information forms, Candidate & Hirer
- KID's Key Information Documents
- CFS Contract for Services
- All bespoke forms and tests relevant to the client

Responsibilities

Primary: Branch/Onsite operation teams
Oversight: Operation Directors, Managing Director and Head of Compliance
Back up: Operation Managers and Operation Directors

Communication Protocols

- Notify candidates via social media (Marketing only) and SMS/Phone calls about alternative registration process
- Maintain daily registration log to be shared with Team Leads
- Provide daily/weekly updates to respective Directors and Head of Compliance

Right to Work Document Collection

Identified Issues

- No access to stored RTW documents or verification tools
- Inability to verify documents online
- Risk of non-compliance with legal requirements

Action Plan

- Use printed RTW checklists and manual verification
- Request physical copies of documents from candidates
- Use Home Office phone support for urgent checks

- Store documents securely in locked cabinets until systems are restored

Responsibilities

Primary: Branch/Onsite operation teams
Backup: Regional Managers, Area Managers and Operation Managers
Oversight: Operations Director and Head of Compliance

Communication Protocols

- Call candidates to confirm RTW status and request documents
- Escalate any compliance risks to the Compliance Team immediately

Client Management

Identified Issues

- No access to client contact details or job orders
- Inability to update clients on candidate progress
- Risk of losing client trust or contracts

Action Plan

- Use printed client contact lists from last backup
- Assign Account Managers to call clients with updates
- Document all communications manually for later CRM entry
- Provide regular updates on recovery progress

Responsibilities

Primary: Regional, Area, Business and Account Managers
Backup: Operation Managers
Oversight: Operation Directors

Communication Protocols

- Daily phone updates to key clients
- Weekly summary email to key clients from personal accounts
- Escalate client concerns to Operation Directors or Managing Director

Information Technology – IT Recovery Procedures

Identified Issues

- Complete loss of access to internal systems and data
- Inability to support remote work or system recovery
- Delayed incident response and troubleshooting
- Risk of data loss or breach
- Inability to deliver training online both internal and to clients

Recovery Actions

- Initiate IT disaster recovery protocol and notify service providers
- Switch to backup servers or local systems if available
- Restore critical data from secure offline backups
- Verify integrity of restored data and systems
- Document all recovery steps and maintain an incident log
- Conduct post-recovery audit and implement improvements
- Consider using other on-line tools to deliver training where necessary or delivering on site if appropriate

Communication Protocols

- Immediate notification to senior management and department heads
- Daily recovery status updates via SMS or alternative channels
- Coordinate with external IT vendors for support
- Escalate unresolved issues to Managing Director and Chief Executive Officer
- Notify staff in line with Marketing when systems are restored and operational

IT Backup Responsibilities

Primary: IT Project and Support Team
Backup: IT Director
External Support: Third-party IT service provider

IT Security Measures and Restoration Steps
Security Measures During Outage

- Restrict access to physical systems and backup drives
- Ensure all manual data handling follows GDPR and internal data protection policies
- Use encrypted storage devices for any temporary data handling
- Monitor for unauthorized access attempts and report incidents immediately
- Disable remote access until systems are verified secure

System Restoration Steps

- Verify integrity of backup data before initiating restoration
- Restore systems in priority order: payroll, CRM, RTW verification, client database
- Test restored systems for functionality and security compliance
- Re-enable remote access with updated credentials
- Notify all staff of system availability and provide updated access instructions
- Conduct post-restoration review and document lessons learned