Business Continuity Policy

The purpose of this policy, is to outline our commitment to ensuring operational resilience and continuity of service for all stakeholders, including our valued clients and workforce.

The policy demonstrates how we can safeguard the integrity of our operations by proactively identifying potential risks and implementing robust contingency measures. In the face of unexpected events, we aim to minimise disruption by identifying essential services and diligently planning how we can deliver these services, in the face of unexpected events.

This policy is an overview of our business continuity plan considering high-level strategies for maintaining essential services and communicating with staff, clients, suppliers and stakeholders in the event of emergency until normality can be resumed.

Scope

This policy applies to all staff in the company. The Compliance Team will maintain and review the Business Continuity Policy and Business Continuity Plan with input from stakeholders from Operations and IT. The Business Continuity Plan will further detail services that are deemed as essential and those with responsibilities for enacting the plan and delivering those services in event of emergency.

Definitions

- Company: means all Gi Group companies, including Gi Group, INTOO, Marks Sattin, Encore Personnel Services, TACK TMI and Gi Group Staffing

- Business Continuity Plan: A documented plan outlining the steps that should be taken to deliver essential services in event of an emergency.

POLICY

Business Continuity Strategy

The strategy that the company will employ in an emergency is fully documented in the Business Continuity Plan, which has been developed by completing the following process:

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 our high street locations within the branch network and our on-site locations that are based on a client's premises, as well as for our remote employees delivering services on behalf our legal entities. It is essential that our on-site locations liaise with the client to ensure that the plan dovetails with the company's 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 (CMT)
   - Pandemic Response Team (PRT)

The Response Teams 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:

- 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

<u>Threats</u>

Through the Business Process Analysis, the company has identified the following as the most serious threats to us being able to deliver our service:

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

The Business Continuity Plan considers each risk and details the action that should be taken by the Response Teams to minimise the level of disruption to our workers, clients and key-stakeholders. Through our Business Continuity Planning activities, the following functions have been identified as essential:

- Marketing and PR Activities
- Payroll
- Credit Control
- Candidate Registrations
- Right To Work in the UK Document Collection
- Client Management
- Information Technology

Steps that should be taken to ensure we can maintain these essential functions are detailed in the Business Continuity Plan.

In an emergency, it is likely that staff won't have access to online documents. Therefore, the critical documents that would allow locations to perform essential services will be uploaded to an Offline Secure Backup System, so that staff will be able to access these. 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 functions are maintained

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 12 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

Testing

If the plan is activated at any point, a full de-brief process will take place to analyse the strengths and weaknesses. If any weaknesses are identified, the plan will be reviewed and updated. Where the plan hasn't been activated, a table-top exercise to test the effectiveness will be completed on an annual basis.

Disclaimer: This policy is meant to provide general guidelines and should be used as a reference. It may not take into account all laws and is therefore not a legal document. The Company will not assume any legal liability that may arise from the use of this policy.

Signed: Paulo Canoa - Regional Head UK, Ireland and Netherlands, Country Manager UK & Ireland
Date: November 2025