BUSINESS CONTINUITY PLAN

XXXX

Business Continuity Plan

VERSION CONTROL

This Business Continuity plan document is to be reviewed and updated annually or sooner where there is a legislative, regulatory, or organisational requirement. Minor changes such as grammar correction will not be recorded as a version change. Instead, such minor changes will be recorded as revisions.

Version	Date	Update	By Whom
1.01	June 2021	Initial Draft	
1.02			

Table of Contents

1. INTRODUCTION

A business continuity plan (BCP) is a well-defined and documented procedure implemented in a business continuity emergency, event, incident, or crisis. Typically, a plan will cover all key personnel, resources, services, and actions required to manage the Business Continuity Management. XXXX is an IT(Information technology) recruitment company that assists clients in finding and secure IT, specialists for specific projects. The objectives of the company include: -

  (a) To find exciting new clients and projects to offer services,

  (b) To find suitable and skilled IT staff for our clients,

  (c) To add value to our clients by advising them on current market services,

  (d) Add value to our candidates by providing a wide range of opportunities, and

  (e) Expand territories and countries that we cover.

This document highlights vital critical incidents identified at XXXX and the level of risk exposure within hiring IT specialists for specific projects. The company has put forward mitigations for such incidents when one consultant leaves the client projects case due to illness or separation.

The Business Impact analysis was carried out in June 2021 under ISO 22301:2019 Business Continuity Management systems standard. The objective of the assessment was to ensure timely identification, analysis, and prevention of disruptive risks/events which could negatively affect the organisation in the achievement of its goals and objectives. The outcome was a business continuity plan.

The most significant critical incidents to operations identified and discussed with management, their recommendations on further steps to improve the processes. Requesting more resources to implement the identified mitigations and documented risk mitigation measures will address key disruptive critical incidents and create contingency plans.

1.1 OBJECTIVES

The Business Continuity Plan aims to coordinate the recovery of essential firm functions to manage and support the business's recovery in recruiting IT specialists. This can encompass both short- and long-term instances of recruited IT specialists leaving the client projects mid-ways and instances where the recruited personnel fall ill during the project implementation phase, especially during this pandemic.

Disruption is defined as any event that renders the provision of business services dysfunctional or unusable, impairing the organisation's capacity to provide critical business services.

In a crisis event, the following priorities must be met:

1 Ensure minimal disruptions of operations.
2 Avoid or limit the damage that disruptions can inflict.
3 Make advanced measures to assure the continuation of essential company functions.
4 Have established plans and procedures to guarantee that recovery methods for essential business functions are implemented quickly and effectively.

The Business Continuity Plan for XXXX comprises procedures for all recovery phases outlined in this document's recovery procedures.

1.2 SCOPE

The Business Continuity Plan is limited in scope to recovery and business continuance from a severe disruption of activities due to the non-availability of the recruited talents to deliver client projects due to instances of illness or desertion of client projects. Unless otherwise modified, this plan does not address temporary interruptions of duration less than the time frames determined to be critical to business operations.

The scope of this plan is based on two critical incidents that affect our core objective of providing clients to secure Information technology specialists for specific projects. These incidents are analysed to give various mitigations that can protect organisational value.

The aim of having a business continuity plan is to: -

• Have a contingency plan in times of a business process disruption.

- Estimate the cost of implementing recovery strategies.

- Establish the foundation for investment in recovery, prevention, and mitigation strategies.

1.3 ASSUMPTIONS

This Business Continuity Plan's viability is predicated on the following assumptions

1. A feasible and tested disaster recovery plan is in place and will be implemented within achievable timelines to restore operations of the organisation at the earliest time possible.

2. The plan has been kept up to date and maintained.

3. The tasks indicated in this plan do not have to exist within the organisation previously; they can be assigned to one or more persons as new duties or delegated to an external third party if money for such services can be established and allocated.

1.4 CHANGES TO THE PLAN /MAINTENANCE RESPONSIBILITIES

The recruiting section is responsible for the maintenance of this business continuity plan.

1.5 PLAN TESTING PROCEDURES AND RESPONSIBILITIES

The management of BlockiworkIT is accountable for ensuring the viability of their Business Continuity Plan. This should be confirmed periodically through active or passive testing.

2. CRITICAL INCIDENTS

This section of the Business Continuity Plan for the XXXX details the approach developed to ensure business continuity following critical incidents that can affect the recruitment process through employee illness and separation from the company. Below are critical incidents identified through impact analysis that can adversely affect the recruitment process, which is the company's core objective, thus affecting the organisation's goals.

1 IT consultants want to leave the project, which could have potential impacts on the delivery of the project.

2 Consultant unavailability since most jobs might be remote.

3   Pandemic: - pandemic could substantially affect staff availability through illness.

4   Cyberattack on internal database and document repository.

2.1 BUSINESS FUNCTION RECOVERY PRIORITIES

The strategy is to re-establish critical services of the consultant projects within the next two hours after the occurrence of the incident. The first procedure is to activate the succession planning and replacement policy of the organisation.

2.3 RECOVERY PLAN PHASES

Fast recovery is key to a successful business, so XXXX must have an emergency plan in place. One way of recovering quickly after the unexpected occurs involves setting up a back-up team to do client work when there may be disruption on the unavailability of IT specialists. This ensures that everything can continue smoothly and ensures minimum interruption on projects, with clients waiting for more information about their assignments.

The measures taken to recover from an employee separation or illness and the tasks and activities required for continuity planning can drastically vary. For instance, XXXX is suffering mass layoffs due to reorganisation to stay competitive with other companies in their industry. XXXX will need different recovery methods than those used after one of its employees contracts Covid 19 while on vacation. Further, this shows how recovery methods vary from one incident to the next.

The tasks required to recover from a disruption to the XXXX recruitment process are separated into four phases. These steps will occur in chronological order.

1. **Incident occurrence**

This phase begins with the occurrence of the incident and continues until the recovery plans are activated. This phase is characterised by the following primary actions: emergency response measures, damage assessment activities, and incident declaration.

2. **Plan activation**

This phase implements the Business Continuity Plan. This phase will continue until vital business services are restored, human resource issues are resolved, and the recruitment process is fixed.

This phase is primarily concerned with receiving notification from the project client of the unavailability of recruited IT specialists, implementing interim procedures on filling the vacant position through established replacement procedures, and re-establishing the trust of the project client.

3. Backup/Replacement strategies

This phase begins upon establishing replacement requirements according to the client specifications, identifying required qualifications in the internal database, and choosing the potential replacement for ill or separated IT specialists. During this period, the critical recovery operations are backlog reduction of the client's work and building the internal database to include an alternative resource for various client projects.

4. Transition to normal operations of the firm

This phase encompasses any activities required to revert to normal operations of the business. This will align the recruitment process with attendant succession and replacement policy— Adherence to this policy using compliance risk assessment strategy to be done in the company's annual cycle. A compliance risk assessment will specifically accomplish XXXX adherence levels to succession planning and replacement policy. According to the enterprise risk management framework established, this assessment specifies the guidelines and procedures of carrying out compliance.

3. RECOVERY STRATEGIES AND MITIGATIONS

This portion of the plan details recovery strategies and the various mitigation plans for each critical incident. The mitigations are outlined against each incident to minimise the impact on the occurrence of the incident.

Scenario/incident/risk	Impact	Mitigations
IT consultants want to leave the project, which could have potential impacts on the delivery of the project	a) Impairment of business performance b) Disruption of client operations c) Damage to reputation	• Develop and design a contract template that ensures that consultants have a stipulated fixed notice period.

	d)Delays in project delivery	• Create a knowledge transfer framework to mitigate against the loss of knowledge through employee separation. • Provide a replacement of the same skills to ensure a smooth transition.
Consultant unavailability since most jobs might be remote.	a) Loss of effectiveness/trust with clients b) Loss of credibility in the external prospecting clients c) Delays in clients project execution	• Develop and implement a succession and replacement plan for all cadres of IT specialists roles. This will lead to a prompt replacement of specific functions. • Develop a tracking system for work done by IT specialists. • Daily log-in activities for work.
Pandemic A pandemic could substantially affect staff availability through illness and business interruptions.	a) Financial loss b) Loss of reputation c) Disruption to business activities d) Death and hospitalisation	• Develop business continuity plans to mitigate against pandemic risks • Develop a crisis management framework to offer support during pandemics • Inform alternate staff to resume work on available roles
Cyberattack on internal database and document repository.	a) Disruption to business activities b) Interruption of service c) Financial costs for emergency or repair d) Loss of goods/funds/assets	• Develop a business continuity plan and test the program annually to provide for the business resumption and ensure continuity of operations during emergencies or disasters • Develop and implement a data back-up mechanism • Establish an incident response capability to prepare for, recognise, report, and respond to the incident and return the IT system to operational status • Annual budget to cover for contingency plans to purchase technical equipment like servers.

3.1 RECOVERY ACTIVITIES AND TASKS

The following activities and tasks cover the recovery from a disruptive event of consultant unavailability through separation and instances when they fall ill: -

PHASE I: Incident occurrence

TASKS:

1. Unavailability of IT specialists or through a written notice of intention to leave the client project. Assess the situation to determine whether to immediately send a replacement of the ill consultant, considering the nature of the client project status and the possibility of additional risk.

2. Assess the internal database on the number of replacements that can do the leaving consultant's work.

ACTIVITY: Management Notification

TASKS:

1. The team leader of the recruitment process informs management team members of BlockwithIT on the consultant's request to leave the project due to separation or ill-health.

2. The incident is communicated to the recruitment section according to succession planning and replacement procedures and policies.

3. Depending on the incident timing, personnel is briefed on what to do (i.e., replace the consultant or await expiry of the notice)

ACTIVITY: Preliminary assessment

TASKS:

1 Contact the XXXX Emergency Response Team Leader to ascertain the separation of IT specialists clients' roles and tasks.

2 Notify all team members of the changes to the client's profiles due to the exiting consultant. Draft an email to the recruitment section to notify them of the above changes in consideration of replacement.

3 Ascertain client project status to understand the immediacy of the replacement.

4   A meeting with the Emergency response Team and management teams from other departments to examine available resource for replacement purposes. Declaration

suggestion generated by the preliminary assessment and to identify the appropriate course of action. Determine the approach to recommend to Senior Management in collaboration with this group (the Emergency Management Team Leader will be responsible for communicating this to Senior Management).

PHASE II: Plan activation

ACTIVITY: Notification of the exiting/ill consultant

TASKS:

1. The team leader of the recruitment section contacts each member of the management team and informs them of the exiting /ill consultant and the importance of activation business continuity plan specific to that incident and discussing the various mitigation proposals.

2. With the assembled team, go over the recovery strategy and action plan.

3. Adjust the client project profile assignments as appropriate based on available IT specialists.

4. The Management Team notifies essential personnel and instructs them to replace the exit IT specialist.

ACTIVITY: Backup/Replacement strategies

TASKS:

1. Understand replacement requirements according to the client specifications. This encompasses creating a database for all clients and their specific needs. A pool of recruited IT specialists will be available with qualifications and skills matched with the client's projects. Additionally, information stored in the internal database and a repository created.

2. Identify required qualifications in the internal database and match these to the client's projects creating a database for alternative resources for each client work project. Regularly determine availability of alternative resources by either emails or calls depending on specified schedules. Determine the level of work, either flexible hours or several shifts.

3. Select the potential replacement for ill or separated IT specialists. This is after discussion with top management on the best available IT specialists for replacement purposes.

ACTIVITY: Manage work backlog reduction

TASKS:

1. Establish priorities for work backlogs to guarantee that the most critical activities of the client project are completed first. The replaced resource will be able to assess and work on the client prioritised work.

2. Determine a schedule for extra work, if necessary, based on employee and system availability.

3. Establish backlog priorities, create backlog status reports as necessary, and send these to the supervisor of the recruitment section.

4. Regularly communicate the backlog status to the recruitment section.

5. If backlogs look extremely big or take an extended time to clear, assess whether additional temporary staff could be used to assist in removing the backlogs. Arrange for temporary employees to be brought in if necessary.

PHASE IV: Transition to normal operations of the firm

TASKS:

1. The recruitment process needs a succession and replacement policy. There needs to exist a policy on succession planning of the recruitment process. This policy guides replacement, knowledge transfer and approved staff establishment ratios in the client's projects.

2. Carry out periodic compliance risk assessments in adherence to compliance strategies of the company. This will measure the level of compliance of XXXX to policies and procedures.

3. Conduct a full audit of the recruitment process and complete mitigations planned

4. Learn and apply key lessons to improve organisational resilience to prevent future occurrences of disruptions due to factors outside our control, such as a pandemic.