REMUNERATION POLICY

RAISE GLOBAL SA (PTY) LTD

2018/616118/07

An authorised Financial Services Provider with FSP No: 50506

August 2023

TABLE OF CONTENTS

1. INTRODUCTION

Raise Global SA (Pty) LTD (hereinafter referred to as the "FSP") is an authorized Financial Services Provider with FSP Number 50506. The FSP was incorporated in 2019 to carry out regulated activities in South Africa, under the regulatory framework of the Financial Services Conduct Authority of South Africa. The FSP has company number 2018/616118/07. The FSP current address is Oxford & Glenhove, Building 2, 114 Oxford Road, Rosebank, Johannesburg, 2196.

RaiseFX is a registered trading name of Raise Global SA (Pty) LTD, a legal entity part of RaiseGroup's group of companies which include the following:

RaiseGroup LLC, an authorised and regulated entity in Saint Vincent and the Grenadines under number 2635 LLC 2022 by the Registrar of International Business Companies, and registered by the Financial Services Authority. RaiseFX has another office in Lebanon, RAISE GROUP MENA MARKETS, a company registered in Lebanon with registration number 2019/126 and with registered address: Kojok Business Center 9th Floor, Saeb Salam St., Verdun, Beirut, Lebanon, as well as in Kazakhstan, RaiseGroup LLP, a company registered under identification number 10100540689586. RaiseGroup LLP holds a license issued by the Financial Supervision Committee of the Ministry of Finance of the Republic of Kazakhstan under the identification KZ12UWX00001735.

RaiseFX was founded by the CEO David Bottin. A team with over 35 years of experience hold Controlled Functions with the firm. And Pierre Vantomme as the Chief Operations Officer.

The Remuneration Policy is a sound and sustainable remuneration policy and practice which promotes the alignment of interests of the FSP with those of its clients and which avoid excessive risk taking and unfair treatment of customers. It also sets out the remuneration plan on an organization wide basis which supports the overall business strategy of the FSP. The main functions of the Remuneration Policy, are:

- to promote the achievement of strategic objectives within the FSP's risk appetite; and
- to promote and support positive outcomes across the economic and social context in which the FSP operates; and
- to promote an ethical culture and responsible corporate citizenship.
- to align the FSP with the principle of "Equivalence of Reward" relating to Advice, Outsourced Activities, and other activities raised in the FSCA's Retail Distribution Review

2. REMUNERATION PHILOSOPHY AND KEY PRINCIPLES:

The FSP's remuneration philosophy is based on the principles of fair and responsible remuneration and to recruit, motivate, reward and retain employees who believe in, and live by the FSP's values. We endeavour to encourage employees by creating a working environment that motivates high performance so that all employees can strive to positively contribute to the strategy, vision, goals and values of the FSP.

Any Remuneration or fee paid in respect of an activity or function for which a person is appointed as a representative-

(a) is reasonable and commensurate with the actual function the representative performs; and

(b) is not structured in a manner that may increase the risk of unfair treatment of clients

We believe the long-term success of the FSP is directly linked to the individuals that we employ. It is therefore vital that we make a concerted effort to align the best interests of our employees with that of our stakeholders.

3. REMUNERATION POLICY AREAS

3.1. SCOPE

- The Remuneration Policy is applicable to all divisions, subsidiaries and licenses within the FSP's organization.
- This Remuneration Policy does not apply to the following employees:
  - Employees on work experience or trial basis
  - Limited application to employees in their 'probation' period prior to full time employment
  - Limited application to employees within a formal disciplinary process

3.2. REMUNERATION STRUCTURE

3.2.1. Overview

The FSP's remuneration structure relating to salaried employees (including executive directors) comprises the following elements/categories: guaranteed remuneration package (fixed), variable remuneration (short term and long-term incentives) and recognition. Non-Executive directors' remuneration is explained separately in a separate section (section 4).

3.2.2. Guaranteed Remuneration/Package

a) Key Objective

To provide a reasonable fixed monthly salary that reflects the skill set and work required to execute a specified role. The Guaranteed Remuneration should ensure that an employee is sufficiently motivated to execute their tasks to a high standard whilst being able to afford a reasonable standard of life. The Guaranteed Remuneration should promote a responsible approach to tasks, whilst holding company policy and regulatory policy to the highest regard.

b) Structure

The Guaranteed Remuneration will be clearly set out within the employment contract and based upon the specified tasks of the role the employee is responsible. Remuneration will be paid monthly at an agreed date (usually the end of the month) to reflect that month's employment.

c) Eligibility

This will apply to all employees who are in a full-time employment with the company.

3.2.3. Short-Term Incentives

a) Key Objective

To provide appropriate incentives to encourage employees to improve performance or achieve expected performance. These incentives are applicable to tasks set out within the employment agreement but also for additional tasks that arise while in employment. These incentives would be designed to provide an achievable reward for employees, with no penalty if short term targets are not met.

b) Structure

A clear task and target payoff will be provided. These will be clear and communicated personably to all individuals and teams who are eligible and supported by email.

c) Eligibility

Dependent upon the task, employees who are directly involved in the project will be eligible.

3.2.4. Long-Term Incentives

a) Key Objective

To provided Personal Development Plans with attached longer-term incentives. These can be in the form of promotions and increases in responsibility, which will be achieved with upskilling and increases in overall remuneration packages. The Personal Development Plan serves to reward dedicated and committed employees who execute their roles to a high standard whilst abiding by company and compliance policies.

b) Structure

The Personal Development Plan is at the centre of the employment with Raise Global SA. This will be clearly defined to all employees and managed by their line managers and reported to the Board through the Branch Manager.

c) Eligibility

All employees with a full-time employment contract are eligible.

3.3. ELEMENTS OF THE REMUNERATION PLAN

The remuneration plan includes the following elements:

Remuneration element	Purpose
Guaranteed Package	Compensation for roles and tasks prescribed in the employment agreement.
Short-term incentives such as Performance bonus and/or Pay-for-Performance	Achievement of agreed targets, overtime work and additional duties performed.
Long-term incentives	Career Development Plans, Upskilling and Educational qualifications.
Recognition	Outstanding Achievements, overall company performance, adherence to regulation. Seasonal Bonus e.g. Birthdays, Christmas or other festival/holidays.

3.4. FAIR AND RESPONSIBLE REMUNERATION

The FSP is committed to fair and responsible remuneration across the organisation.

- Any possible remuneration disparities related to race, gender or other, will be identified. Any confirmed remuneration disparities will be investigated and addressed as soon as is practical and possible.
- Any unjustifiable differences in the terms and conditions of employment, including remuneration will be identified. Unjustifiable differences in pay and conditions of employment between employees at the same level will be addressed in accordance with the "Equal Pay for Work of Equal Value" philosophy/principles.

3.5. MARKET POSITION

The market view for all job categories is flexible enough to consider the economic and commercial environments as they affect the company and its employees. This implies continuous monitoring and assessing of the current labour market from which the FSP recruits.

3.6. MARKET BENCHMARKING/REMUNERATION SURVEYS

- In line with general market practice, the FSP compares itself to companies within its industry (by participating in Financial and Insurance Industry surveys as well as other relevant surveys).
- Where surveys indicate that a job grouping is significantly out of line with market pay bands, a remuneration adjustment may be considered.
- The main factor in assessing the influence that external salary levels (market pressure) should be allowed to exercise internally is the extent to which there is competition for the employees in question in the open market. The ability of the FSP to attract and retain the right calibre of employee is normally evidence of this.
- Discretionary elements of pay beyond benchmarked levels can be included for scarcity, attraction and retention purposes, where appropriate.
- Targeting remuneration to market level is generally done on the basis of total guaranteed package.
- In order to compare the variable remuneration component, market practice with regard to typical remuneration mixes and incentivization principles, serves as the basis for recommendations.
- To remain competitive, market-related premiums will be considered for certain skills, employment equity purposes and if there is a shortage of skills.

3.7. REMUNERATION REVIEW

A review of remuneration is conducted annually, and any resultant increase is effective from the begging of the quarter or each financial year.

3.8. REMUNERATION GOVERNANCE

The FSP has established a Remuneration Committee "Remco" to oversee the administration and implementation of the Remuneration Policy. The Remco governs the FSP's Remuneration Policy within the framework of its own Terms of Reference.

The REMCO sits as a function formed of the Branch Managers and the Board of Directors.

4. REMUNERATION OF EXECUTIVE DIRECTORS

Remuneration of executive directors (the CEO and other senior members of Management who are also members of the FSP's Board of Directors) is governed by the principles and practices as applicable to other salaried employees within the organization.

5. APPROVAL OF REMUNERATION

The FSP follows the recommendations of King Code IV ("King IV") in respect of shareholder approval of remuneration as follows:

In the event that either the remuneration policy or the implementation report, or both were voted against by 25% or more of the voting rights exercised, King IV proposes that the following be disclosed in the background statement of the remuneration report succeeding the voting:

- With whom the company engaged and the manner and form of engagement to ascertain the reasons for the dissenting votes; and
- The nature of steps taken to address legitimate and reasonable objections and concerns.

The fees of non-executive directors of organizations must be submitted to a binding special resolution approved by shareholders within the previous two years. The same binding special resolution for the remuneration of executive directors is not required in terms of King IV recommendations.

In the event that either the Remuneration Policy or the implementation report or both have been voted against by 25% or more of the voting rights exercised by shareholders at the FSP's Annual General Meeting, the FSP is committed to taking the following steps (at a minimum) as suggested by King IV to find resolution:

- An engagement process to ascertain the reasons for the dissenting votes.
- Addressing legitimate and reasonable objections and concerns raised, as is appropriate, and which may include amending the Remuneration Policy, or clarifying or adjusting remuneration governance or process.

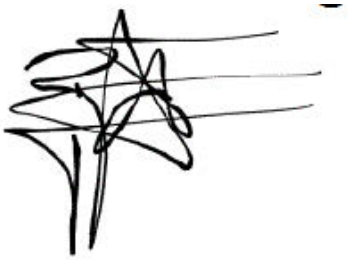
6. MANDATE AND AUTHORITY

- The Remuneration Policy shall be adopted by way of a binding special resolution of the Board.
- The management of the FSP as well as the Remco shall take into account the Remuneration Policy, and any other relevant documents such as the Remco's Terms of Reference (as applicable), when considering matters before it.
- The Remco has full discretion in determining appropriate remuneration policies and practices for the FSP, including but not limited to, annual remuneration increases, performance bonuses and share incentives for the FSP.
- The Remco shall, as deemed necessary, report significant deviations from the principles set forth in the Remuneration Policy to the FSP's Board.

This Remuneration Policy has been adopted as follows:

Signed this 28th day of August 2023.

Signature



VERSION HISTORY

Document number:	**#1**
Document version:	**V1.1**
Document approval authority:	**David Bottin**
Document approval date:	**August 2023**
Document owner:	**Kevin Wides**
Document author(s):	**Kevin Wides**
Last updated:	**August 2023**
Next review date:	**December 2023**
Visibility (where will it be displayed):	**Website**

OUTSOURCES ACTIVITIES POLICY

RAISE GLOBAL SA (PTY) LTD
2018/616118/07

An authorised Financial Services Provider with FSP No: 50506

August 2023

1. INTRODUCTION

Raise Global SA (Pty) LTD (hereinafter referred to as the "FSP") is an authorized Financial Services Provider with FSP Number 50506. The FSP was incorporated in 2019 to carry out regulated activities in South Africa, under the regulatory framework of the Financial Services Conduct Authority of South Africa. The FSP has company number 2018/616118/07. The FSP current address is Oxford & Glenhove, Building 2, 114 Oxford Road, Rosebank, Johannesburg, 2196.

RaiseFX is a registered trading name of Raise Global SA (Pty) LTD, a legal entity part of RaiseGroup's group of companies which include the following:

RaiseGroup LLC, an authorised and regulated entity in Saint Vincent and the Grenadines under number 2635 LLC 2022 by the Registrar of International Business Companies, and registered by the Financial Services Authority. RaiseFX has another office in Lebanon, RAISE GROUP MENA MARKETS, a company registered in Lebanon with registration number 2019/126 and with registered address: Kojok Business Center 9th Floor, Saeb Salam St., Verdun, Beirut, Lebanon, as well as in Kazakhstan, RaiseGroup LLP, a company registered under identification number 10100540689586. RaiseGroup LLP holds a license issued by the Financial Supervision Committee of the Ministry of Finance of the Republic of Kazakhstan under the identification KZ12UWX00001735.

RaiseFX was founded by the CEO David Bottin. A team with over 35 years of experience hold Controlled Functions with the firm. And Pierre Vantomme as the Chief Operations Officer.

The FSP is committed to an outsourcing Activities Policy that follows the stringent rules and regulations set out in the Financial Advisory and Intermediary Services Act No. 37 of 2002 (the "FAIS Act") schedule, Board Notice 194 of 2017 'Determination of Fit and Proper Requirements for Financial Services Providers, 2017.

The FSP may outsource some functions to Third parties under appropriate agreements. The FSP has an obligation to ensure due skill, care and diligence is exercised when:

- Entering into, terminating and managing contracts with outsourced service providers;
- the activity is integral to the authorized services of the FSP; and
- the outsourced activity is material to the operation of FSP.

The Outsourcing Activities Policy sets out the framework for the process of assessment of outsourced service providers before engagement with the FSP as well as annual assessment (performance appraisals) of outsourced service providers once engaged in a service contracts with the FSP.

2. **PURPOSE:**

The purpose of the Outsourced Activities Policy is to ensure that all outsourced activities are performed in the best interests of the FSP's clients, with minimal risk to the operational activities of the FSP and with the view to obtain fair outcomes to the FSP's clients.

3. OUTSOURCING STRATEGY

3.1. OUTSOURCING REQUIREMENTS

The **Key Individual**, duly authorized by the FSP, will be tasked with reviewing and evaluating the following requirements and providing an analysis (due diligence) thereof when potentially onboarding a new outsourced service provider and such analysis and conclusion shall be presented in a report to the governing body and senior management of the FSP for review and potential appointment of the outsourced service provider.

The Outsourced Service Provider must:

- be appropriately licensed (i.e. if they are an FSP they need to be properly authorized) and approved to provide such service's from their jurisdiction of incorporation; and
- not further outsource its service's or sub-delegate the service/s to Third parties; and
- have appropriate training and qualifications to discharge the outsourced service provider's service/s; and
- the outsourced service provider must have the relevant capacity and facilities to provide the service's it has offered to the FSP; and
- have adequate controls, policies and processes to manage risks internally as well as risks to the FSP; and
- must have transparent accounting policies that accurately reflect the outsourced service provider's financial position as well as shareholder and director information; and
- must have appropriate facilities to effectively supervise the outsourced activity offered to the FSP, in order to mitigate risks of outsourcing service/s; and
- make sure the assets of the FSP and the FSP's clients and those of the outsourced service provider must be segregated.

3.2. DUTY OF THE FSP

The FSP must exercise due skill, care and diligence when entering into (including the selection process), managing or terminating any arrangement for the outsourcing to any person other than a representative of the FSP of-

a) ensure that the person to whom the function or activity has been outsourced-
    i. has the ability, capacity, and any authorisation required by law to perform the outsourced functions, services or activities reliably and professionally;

ii. is able to carry out the outsourced services effectively, to which end the FSP must establish methods for assessing the standard of performance of that person;

b) have a written contract or service level agreement that governs the outsource arrangement and which clearly provides for all material aspects of the outsourcing arrangement, including-
    i. addressing the rights, responsibilities, and service-level requirements of all parties;
    ii. providing for access by the FSP and the Authority, to the person's business and information in respect of the outsourced function or activity;
    iii. addressing sub-outsourcing; and
    iv. addressing confidentiality, privacy and the security of information of the FSP and clients of the FSP;

c) properly supervise the carrying out of the outsourced functions, and adequately manage the risks associated with the outsourcing, including any risks to the FSP's clients;
d) take appropriate action if it appears that the person may not be carrying out the functions effectively and in compliance with applicable laws and regulatory requirements;
e) retain the necessary expertise to supervise the outsourced functions effectively and manage the risks associated with the outsourcing;
f) be able to terminate the arrangement for outsourcing where necessary without detriment to the continuity and quality of its provision of financial services to clients;
g) establish, implement and maintain a contingency plan for disaster recovery and periodic testing of backup facilities;
h) have effective access to data related to the outsourced activities, including any data relating to the FSP's clients, as well as to the business premises of the person; and
i) ensure that the outsourcing arrangement does not-
    i. compromise the fair treatment of or continuous and satisfactory service to the FSP's clients; or
    ii. result in key decision-making responsibilities being removed from the FSP.

3.3. OUTSOURCING AGREEMENT'S

The FSP must ensure that all outsourcing agreements or SLA's concluded between the FSP and outsourced service providers cover the following requirements:

- The agreement will ensure that the outsourced service provider has mechanisms and processes in place to disclose immediately any activity that may disrupt its service/s to the FSP whether minimally or materially; and

- the outsourced service provider must be willing to cooperate with relevant authorities in relation to the outsourced service/s it provides to the FSP; and
- the outsourced service provider has an obligation to provide access to its premises and access to any data requested by the auditors of the FSP; and
- the outsourced service provider must ensure that all information is safe from destruction and that it has an adequate disaster recovery system in place as well as adequate back-up facilities and is subject to confidentiality as required by any relevant legislation; and
- the FSP remains fully responsible for all outsourcing activities, obligations and functions in terms of all relevant legislation and regulations; and
- the fee paid for the outsourced service's must be fair to commensurate with the service's provided and must not compromise the fair treatment of the FSP's clients.
-

The Outsourced activities of our FSP are:

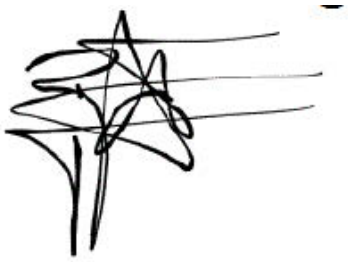
1. External Compliance — Oracle Compliance
2. External Auditing — N.A. Leibovitz and Company
3. External Accounting—Alan Menachemson CA
4. External Legal — SWVG INC

4. AUTHORITY AND MANDATE

The Outsourced Activities Policy is approved by way of approved resolution of the FSP's governing body. The FSP's governing body and senior management are responsible for the adherence to and implementation of this Outsourced Activities Policy throughout the organization.

This Outsourcing Activities Policy has been adopted as follows:

Signed this 28th day of August 2023

Signature 

VERSION HISTORY

Document number:	**#1**
Document version:	**V1.1**
Document approval authority:	**David Bottin**
Document approval date:	**August 2023**
Document owner:	**Kevin Wides**
Document author(s):	**Kevin Wides**
Last updated:	**August 2023**
Next review date:	**December 2023**
Visibility (where will it be displayed):	**Website**

RAISE GLOBAL SA (PTY) LTD

2018/616118/07

An authorised Financial Services Provider with FSP No: 50506

RESOLUTION POLICY

August 2023

TABLE OF CONTENTS

1. INTRODUCTION

Raise Global SA (Pty) LTD (hereinafter referred to as the "FSP") is an authorized Financial Services Provider with FSP Number 50506. The FSP was incorporated in 2019 to carry out regulated activities in South Africa, under the regulatory framework of the Financial Services Conduct Authority of South Africa. The FSP has company number 2018/616118/07. The FSP current address is Oxford & Glenhove, Building 2, 114 Oxford Road, Rosebank, Johannesburg, 2196.

RaiseFX is a registered trading name of Raise Global SA (Pty) LTD, a legal entity part of RaiseGroup's group of companies which include the following:

RaiseGroup LLC, an authorised and regulated entity in Saint Vincent and the Grenadines under number 2635 LLC 2022 by the Registrar of International Business Companies, and registered by the Financial Services Authority. RaiseFX has another office in Lebanon, RAISE GROUP MENA MARKETS, a company registered in Lebanon with registration number 2019/126 and with registered address: Kojok Business Center 9th Floor, Saeb Salam St., Verdun, Beirut, Lebanon, as well as in Kazakhstan, RaiseGroup LLP, a company registered under identification number 10100540689586. RaiseGroup LLP holds a license issued by the Financial Supervision Committee of the Ministry of Finance of the Republic of Kazakhstan under the identification KZ12UWX00001735.

RaiseFX was founded by the CEO David Bottin. A team with over 35 years of experience hold Controlled Functions with the firm. And Pierre Vantomme as the Chief Operations Officer.

The Resolution Policy sets out the strategic framework and resolution planning to be followed by the FSP in the event of financial crisis. The Resolution Policy is designed to be activated in situations where the FSP entity is no longer viable and there are no prospects of recovery, the financial recovery plan has failed, and the company needs to institute winding up proceedings or terminate the company in its existing form. Some areas of the company may be sold off while those that cannot be sold will be run off. Regulators may be involved in this, either assisting or taking on the resolution plan completely. Effective resolution means that the relevant authorities must have access to the resolution strategic framework and resolution planning to enable them to oversee the implementation of the resolution plan directly and either close the business, sell or hand it over to a custodian.

2. PURPOSE:

The Resolution Policy prepares for possible but unlikely future financial crisis situations by assessing importance of the FSPs through evaluation of their critical functions and possible repercussions in the event of the FSP's complete financial failure.

- To be implemented after the Financial Recovery Plans have failed
- Process must be orderly and restore or protect critical economic functions, prevent the spread of harm to other institutions, protect tax payers and policy holders
- The plan will be devised by the Chief Financial Officer, Risk, Legal and Compliance Manager with the support of the Board and other senior management at the point in time required

3. RESOLUTION PLAN

3.1. KEY ELEMENTS OF RESOLUTION PLANNING

In the event of complete financial failure, the FSPs may have to:

- Appoint an administrator or liquidator to manage the firm
- Remove and replace senior management and any other back office staff to leave only critical functions
- Transfer or sell assets or liabilities
- Close or wind down part or the whole company. The company will be closed to new business, Creditors will have to be lodged their claims and their claims ranked in order of preference.

The key elements of resolution planning involve determining the following factors:

- The time it will take to implement the resolution; and
- the impact it will have on the FSP's clients and the principle of fair outcomes based on the Financial Advisory and Intermediary Services Act No. 37 of 2002's ("FAIS") Treating Customers Fairly obligations; and
- the impact the resolution will have on the employees of the FSP; and
- how the process will be communicated both internally and externally to all stakeholders; and
- how the process will be financed for example: private sources, shareholder funds, resolution fund or insurance risk policies; and
- identify any impediments that may hinder the resolution process; and
- a description of the strategy and plans or tools to be used by the FSP in implementing the resolution plan; and
- a process to ensure that the FSP continues to operate and this must allow for access to critical functions of the FSP such as shared systems for example: IT or centralized risk management systems, financial infrastructures, payment systems and the possibility of importing client positions; and
- the FSP must consider whether the situation is resolvable, and if so the minimum funds required and the liabilities to be incurred; and
- the FSP will not assume accessibility to bank finance, public funds or expose clients to the risk of loss.

Where possible the Resolution Policy may be applied in proportion to each of the elements listed above. The greatest risk to the FSP in the event of financial crisis is reputational damage, and operational and financial risk. The FSP's governing body and senior management is responsible for mitigating these risks by ensuring that all internal controls, processes and policies are in place, effective and monitored regularly. These risks are also mitigated by warranting that Professional and Fidelity Insurance is available and valid.

3.2. DYNAMIC NATURE OF RESOLUTION PLANNING

Resolution planning is a dynamic process and must be assessed at least annually or in the event of any material changes, the following elements are involved:

- Assessing the possibility and credibility of liquidation or Business Rescue and Involuntary Insolvency proceedings in terms of the applicable provisions of the Companies Act 71 of 2008 of South Africa ("Companies Act");
- The Resolution Plan will not be possible if resolving the financial crisis is not in the best interests of the public;
- The Resolution Plan will only be an option if applicable authorities are of the view that liquidation is neither credible nor feasible;
- Where liquidation is not feasible, the FSP will identify the appropriate resolution strategy and tools to be used in view of the FSP's:
    - License integrity and costs as advised by compliance and the Key individual; and
    - structure and operation as required by FAIS;
    - financial resources in line with the solvency and liquidity thresholds;
    - tax implications as advised by the FSP's auditors;
    - information safety in terms of FAIS and FICA;
    - legal and compliance issues in line with all applicable legislation and regulations.

3.3. EXTERNAL RESOLUTION STRATEGIES

- The resolution strategy may also involve the use of intrusive powers by relevant authorities to ensure the FSP's financial crisis resolvability. Possible measures may include organizational or structural changes, the prevention or restriction of activities, business lines or sale of products. The relevant authorities may take a supervisory or caretaker role that is cooperative to ensure the FSP's viability and to safeguard the FSP's client and investor funds. The intrusion of the authority is necessary to simplify the structure and operations of the FSP solely to improve resolvability of the financial crisis (Section 49 FAIS schedule Board Notice 194 of 2017).
- The FSP is obligated to comply with Section 49 mentioned above to facilitate early and prompt resolution of the financial crisis it faces.

3.4. RESPONSIBLE PERSONS

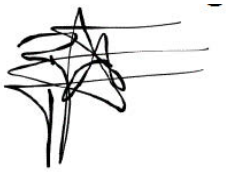
In case of insolvency risks to the business, the FSP's governing body, in its fiduciary responsibility, will assess any required actions that need to be taken. These may include additional fundraising from shareholders, or actions required in terms of the Companies Act, including potential Business Rescue or Voluntary Insolvency proceedings.

4. AUTHORITY AND MANDATE

The Resolution Policy is approved by way of approved resolution of the FSP's governing body. The FSP's governing body and senior management are responsible for the adherence to and implementation of the Resolution Policy throughout the organization.

This Resolution Policy has been adopted as follows:

Signed this 28th day of August 2023.

Signature_ 

VERSION HISTORY

Document number:	**#1**
Document version:	**V1.1**
Document approval authority:	**David Bottin**
Document approval date:	**August 2023**
Document owner:	**Kevin Wides**
Document author(s):	**Kevin Wides**
Last updated:	**August 2023**
Next review date:	**December 2023**
Visibility (where will it be displayed):	**Website**

RAISE GLOBAL SA (PTY) LTD

2018/616118/07

FINANCIAL RECOVERY PLAN

AUGUST 2023

1. INTRODUCTION

Raise Global SA (Pty) LTD (hereinafter referred to as the "FSP") is an authorized Financial Services Provider with FSP Number 50506. The FSP was incorporated in 2019 to carry out regulated activities in South Africa, under the regulatory framework of the Financial Services Conduct Authority of South Africa. The FSP has company number 2018/616118/07. The FSP current address is Oxford & Glenhove, Building 2, 114 Oxford Road, Rosebank, Johannesburg, 2196.

RaiseFX is a registered trading name of Raise Global SA (Pty) LTD, a legal entity part of RaiseGroup's group of companies which include the following:

RaiseGroup LLC, an authorised and regulated entity in Saint Vincent and the Grenadines under number 2635 LLC 2022 by the Registrar of International Business Companies, and registered by the Financial Services Authority. RaiseFX has another office in Lebanon, RAISE GROUP MENA MARKETS, a company registered in Lebanon with registration number 2019/126 and with registered address: Kojok Business Center 9th Floor, Saeb Salam St., Verdun, Beirut, Lebanon, as well as in Kazakhstan, RaiseGroup LLP, a company registered under identification number 10100540689586. RaiseGroup LLP holds a license issued by the Financial Supervision Committee of the Ministry of Finance of the Republic of Kazakhstan under the identification KZ12UWX00001735.

RaiseFX was founded by the CEO David Bottin. A team with over 35 years of experience hold Controlled Functions with the firm. And Pierre Vantomme as the Chief Operations Officer.

The Corporate Governance Policy sets out the framework on which the FSP's corporate governance structures and processes are based. The Corporate Governance Policy sets out the decision-making structures of the FSP and how the decision-making structures support and assess one another to achieve the King IV objectives of ethical leadership and effective leadership. It is also to facilitate the governance of the organisation in a fair, transparent, responsible, accountable and ethical manner by the board, management and all personnel. The framework will imbed the principles of Treating Customers Fairly (TCF) that run through the recently promulgated Fit and Proper requirements.

The Financial Recovery Plan (the "Recovery Plan") is designed for activation in cases of financial constraints and is not intended to be a business continuity plan or a succession plan. The Recovery Plan will be adopted and adjusted according to the financial circumstances of the FSP in line with changes in the business, strategy or operating environment of the FSP to assist in getting the business out of any financial crisis. External auditors and external compliance are closely involved in the business to monitor activities of early warning, solvency and liquidity requirements.

Whereas the Resolution Policy sets out the strategic framework and resolution planning to be followed by the FSPs in the event of financial crisis where the Financial Recovery Plan has failed. Effective resolution means that the relevant authorities must have access to the resolution strategic framework and resolution planning to enable them to oversee the implementation of the resolution plan directly.

2. PURPOSE

The purpose of the Recovery Plan is to mitigate financial loss by providing the framework for strategy and processes to be followed by the FSP should financial constraints or crisis arise.

The following will be considered in the plan:

- Ensure the company does not deteriorate further while devising recovery strategy
- The strategy adopted to respond to a financial crisis will depend on the root causes of the crisis and an appropriate response will be aligned adopted to suit each circumstance and appropriate short and long-term options implemented. Where numerous factors are responsible for the crisis then various measures will be considered.
- The recovery strategy is driven by the nature of the business, products employed, ownership structure (access capital from parent companies of subsidiary), nature of assets and liabilities, profitability, regulatory regime and credit history.

3. RECOVERY STRATEGIES

3.1. INDEMNITY AND INSURANCE

The FSP will ensure that the risk of financial loss is mitigated by ensuring effective implementation of some or all of the following recovery measures:

- that the FSP and its employees are covered by Professional Indemnity and Fidelity Insurance;
- the FSP's shareholders may apportion financial risks between them and provide capital injection for the FSP;
- governing body and senior management meetings will be held to discuss the state of the business and financial position to ensure that measures and controls to ameliorate financial loss are implemented.

3.2. CLIENT FUNDS

There is no risk exposure to clients if the FSP does not hold client funds however, in cases where the FSP does hold client funds the FSP will ensure that those funds are held in a Trust account.

3.3. SOLVENCY AND LIQUIDITY

The FSP will ensure that it at all times has sound, effective and comprehensive strategies, processes and systems to assess and maintain, on an ongoing basis, the amounts, types and distribution of financial resources that it considers adequate to cover the solvency and liquidity requirements as set out under FAIS.

3.3.1 The requirements for the various categories of FSP are as follows:

<u>Category 1 FSP that does not hold client funds</u>, assets, nor receive premiums :

Solvency: The assets of the FSP must at all times exceed the liabilities of that FSP

Category I FSP that holds funds:, controls or has access to client assets or that collects, holds or receives premiums:

a. **General Solvency :** The assets of the FSP must at all times exceed the liabilities of that FSP
b. **Working Capital:** The Current Assets of the FSP must at all times exceed the Current liabilities of the FSP
c. **Liquidity:** Liquid assets of the FSP must be equal to or greater than 4/52 weeks of annual expenditure

Category II FSP:

a. **General Solvency :** The assets of the FSP must at all times exceed the liabilities of that FSP
b. **Working Capital:** The Current Assets of the FSP must at all times exceed the Current liabilities of the FSP
c. **Liquidity:** Liquid assets of the FSP must be equal to or greater than 8/52 weeks of annual expenditure

Category IIA FSP:

a. **General Solvency :** The assets of the FSP must at all times exceed the liabilities of that FSP by at least R3 millionat all times
b. **Working Capital:** The Current Assets of the FSP must at all times exceed the Current liabilities of the FSP
c. **Liquidity:** Liquid assets of the FSP must be equal to or greater than 13/52 weeks of annual expenditure

Category IV FSP

a. General Solvency : The assets of the FSP must at all times exceed the liabilities of that FSP

b. Working Capital: The Current Assets of the FSP must at all times exceed the Current liabilities of the FSP

c. Liquidity: Liquid assets of the FSP must be equal to or greater than 4/52 weeks of annual expenditure

Mitigating Activities:

- Monthly finance meeting - management accounts are discussed between Directors of the Business (Board), The Head of Finance and Branch Manager. The Key Individual will be informed if anything outside of the normal financial status arises.

- Monthly dividends are declared, and full solvency, liquidity and cash flow reports are done by Financial Manager and signed off by the board of Directors.

- Monthly Management accounts produced with income statements and balance sheets, cash flow projections and discussed in detail at every board meeting.

3.4. SUFFICIENT MARKET SHARE

The FSP may face financial loss due to failure to gain sufficient market share. Factors that may contribute to this failure are setup costs, operational costs, other legal and regulatory cost and reputational risk.

The FSP will monitor and implement a high-level process of regular assessment of the aforementioned factors and the results of this assessment process will be put before the governing body and senior management on how to mitigate risk and keep all aforesaid factors in balance relative to the needs of the FSP.

3.5. BUSINESS ACTIVITY

The FSP is duly authorized by the Financial Sector Conduct Authority (the "FSCA") to provide financial services in South Africa, more specifically in the rendering or performance of "advice and "intermediary services" (as defined in section 1 of the Financial Advisory and Intermediary Services Act, 2002).

The FSP renders or intends to render the following products:

Derivative Instruments (CFD's) on an execution only basis (non advice/non-discretionery) under a Category 1 License

Should the FSP suffer significant financial deterioration, then the FSP's governing body will, in consultation with the FSP's shareholder/s decide:

- whether to wind down the FSP; or
- whether to increase funding from the shareholder/s of the FSP or other sources.

A possible closure or wind-down of the business of the FSP may mean that the employees of the FSP will be retrenched or redeployed into other areas of the FSP's affiliated business entities. All necessary retrenchments and redeployments will follow a formal consultative process in accordance with the Labour Relations Act 66 of South Africa (the "LRA").

4. PROCESS IN THE EVENT OF A SIGNIFICANT FINANCIAL DETERIORATION

The governing body, senior management, shareholders and the Compliance Officer will be kept abreast of the financial state of the FSP through the production of management accounts and financial projections using various methods relating to income statements and cash flow statements will be done and made available to the governing body, senior management, shareholders and the Compliance Officer. Whether projections indicate a likely deterioration in the financial position of the business, the FSP will consider the following:

- The FSP will explore other means to improve the revenue of the business. This may include but is not limited to increasing distribution channels of the products or improving market penetration rates.
- Scale down on the cost structures of the business to align with the expected future lower revenues of the business. This may include staff retrenchment, lower salaries, change of premises etc.

- Determine how long the financial crisis will last. If the position is likely to be prolonged the FSP will work off the existing client base, reduce costs of sales and not take on new clients.
- Consideration will be given to determine how long an investment/trading period takes for each client and this will be used to determine the period it will take to run off the period of existing clients until the last client is appropriately taken care of.
- The governing body and senior management will assess any financial loss and in line with their fiduciary position will take decisions in compliance with the Companies Act 71, of 2008 of South Africa to either commence business rescue or voluntary insolvency proceedings.
- The FSP will notify the FSCA in line with early warning provisions set out in Business Notice 194 of 2017.

5. TURNAROUND STRATEGY

The FSP will consider the following as a turnaround strategy:

- Increase the exposure the FSP has by partnering with other entities, penetrating new markets and establishing relationships with professional networks.
- The FSP may also consider media strategies to increase market share, such as below the line, low cost advertising via the internet, social media as well as participating in special events.
- The FSP will also reduce costs and increase efficiencies.

6. POLICY IN THE EVENT OF FAILURE

The FSP is committed to the policy of Treating Clients Fairly, thus should a financial crisis occur clients will be informed timeously. Appropriate steps will be taken to minimize risk to the client by giving the client the choice of:

a) Transferring their trading account/financial products to another FSP.

b) The client will be given the opportunity to terminate the existing relationship with the FSP, and that clients' assets will be distributed back to the client.

c) All existing obligations will be honored in terms of contracts held between parties.

7. EARLY WARNING REQUIREMENT

- The Financial Recovery strategy may include the oversight of the FSCA, which will take a supervisory or caretaker role that is cooperative to ensure the institutions viability and to safeguard client and investor funds. The involvement of the authority is set out in Section 49 of Board Notice 194 of 2017.
- The FSP's current assets must exceed current liabilities. The FSP must report to the FSCA whenever its assets/current assets or that of its Juristic Rep exceed liabilities/current liabilities by less than 10%.
- In the case of a CATII or IIA FSP, the FSCA must be informed when the additional assets of the FSP or that of its Juristic Rep exceed the minimum requirements by less than 10%.

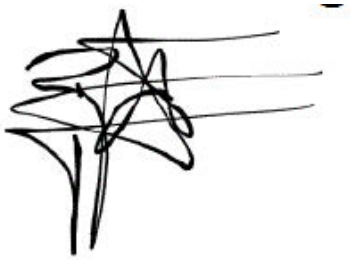
- Should the FSP become aware that any of the abovementioned events will or is likely to occur the FSP is obligated to ensure that it complies with this section to facilitate early and prompt resolution of financial issues.
- Should the FSP find itself in an early warning status, it may not directly or indirectly make any payment by way of a loan, advance, bonus, dividend, repayment of capital or a loan or any other payment or other distribution of assets to any director, officer, partner, shareholder, related party or associate without the written approval of the FSCA Registrar.
- Implementation and monitoring - Once the strategy has been finalised the implementation process will take place followed by monitoring the effectiveness of the strategy adopted to ascertain the impact on the liquidity and solvency position. Indicators will be used to monitor actions to highlight the risk. Various policies already in operation such as the risk management plan and business continuity plan will be used to flag some of the areas of risk and to monitor compliance with controls imbedded.

8. AUTHORITY AND MANDATE

The Financial Recovery Plan is approved by way of approved resolution of the FSP's governing body. The FSP's governing body and senior management are responsible for the adherence to and implementation of this Financial Recovery Plan throughout the organization.

This Financial Recovery Policy has been adopted as follows:

Signed this 28th day of August 2023.

Signature_ 

VERSION HISTORY

Document number:	**#1**
Document version:	**V1.1**
Document approval authority:	**David Bottin**
Document approval date:	**August 2023**
Document owner:	**Kevin Wides**
Document author(s):	**Kevin Wides**
Last updated:	**August 2023**
Next review date:	**December 2023**
Visibility (where will it be displayed):	**Website**

RAISE GLOBAL SA (PTY) LTD
2018/616118/07

An authorised Financial Services Provider with FSP No: 50506

SUCCESSION PLAN

August 2023

Introduction

Succession Planning is the practice of identifying, mentoring and training key persons to fill vital positions in an organization to ensure a smooth transition if such resources resign or change roles.

It is highly recommended that every company should plan for every key position within an organization and that a good organization must look internally for potential candidates. Businesses that cannot afford to buy expensive skills must look within their organizations to mentor and develop leadership qualities in current and future employees. Management has to identify the resource that could continue with the mission, value and objectives that have been set out as the long-term business strategy.

1. Legislation

There is nothing specific in the legislation about succession planning. There are, however, certain requirements in the FAIS General Code of Conduct that could be construed as encompassing succession planning, i.e. Section 2, 11 and 12.

Section 2 of the General Code of Conduct: stipulates that a FSP must at all times render financial services *honestly, fairly, with due skill, care and diligence, and in the interests of clients and the integrity of the financial services industry*. A FSP must thus ensure the client's affairs are not left in a void when the provider dies or ceases practice.

Section 11 of the General Code of Conduct: stipulates that a FSP *must at all times have and effectively employ the resources, procedures and appropriate technological systems that can reasonably be expected to eliminate as far as reasonably possible, the risk that clients, product suppliers and other providers or representatives will suffer financial loss through inter alia, poor administration, negligence or culpable omissions.* It could be construed as poor administration or even culpable omission if a FSP does not make provision to ensure that clients and product suppliers do not suffer financial loss should he die.

Section 12(a) of the General Code of Conduct: requires a FSP to *structure the internal control procedures concerned so as to provide reasonable assurance that the relevant business can be carried on in an orderly and efficient manner.*

2. The Plan

It is important to take note of the following in the event of death, resignation, retirement or permanent disability of a Key Individual:

Companies - If the actual owner of the business dies - be this the sole member of a close corporation or sole shareholder in a company - the authorisation granted to the juristic entity (the close corporation or company) continues - but it requires human agents to conduct its affairs. If the owner wants to be sure that there will be a properly authorised person available to continue running the business should anything happen to him, such person must be appointed while the owner is still alive. It is important to take note that the FSP will not be allowed to perform any regulated function until such time as the new key individual is approved by the FSCA.

Succession Planning Table:

	Current	If in case of Death/Resignation/Retirement/ Permanent Disability etc – they will be replaced by:
Shareholders	David Bottin	Kevin Wides (KI)
CEO	David Bottin	Kevin Wides (KI))
Directors	David Bottin Pierre Vantomme	If a director requires replacement, a representative of the Board of one of the other entities, part of the RaiseGroup's group of companies will step in. The FSP would need to remove the impacted person from CIPC and the FSP's profile.
Key Individual	Kevin Wides	Mr Tota Tsotsotso will be added onto the license as a second KI. Therefore, Raise Global SA has a second KI for its Cat1 license if anything should happen to Mr Wides.

3. Acceptance of Appointment as Replacement Key Individual

DECLARATION OF ACCEPTANCE OF APPOINTMENT AS REPLACEMENT KEY INDIVIDUAL FOR RAISE GLOBAL SA (PTY) LTD

It is hereby recorded that the Key Individual for Raise Global SA shall be replaced in terms of Section 8 (4) (b) of the FAIS Act 37 of 2002 in the event of the following;

(i) the Key Individual is replaced by another Key Individual; or
(ii) a new Key Individual is appointed or assumes office; or

(iii) changes occur in the circumstances of the key individual that affect their fit and proper status rendering them unfit for office

Therefore, Raise Global SA (Pty) Ltd has identified the following key individual as being fit and proper to replace the current key individual:

Full Names of Replacement Key Individual	Mr. Tota Tsotsotso
FSP Number currently licensed under:	42734
Email Address:	Tota@bataungcapital.com

VERSION HISTORY

Document number:	**#1**
Document version:	**V1.1**
Document approval authority:	**David Bottin**
Document approval date:	**August 2023**
Document owner:	**Kevin Wides**
Document author(s):	**Kevin Wides**
Last updated:	**August 2023**
Next review date:	**December 2023**
Visibility (where will it be displayed):	**Website**

RAISE GLOBAL SA (PTY) LTD

2018/616118/07

DISASTER RECOVERY PLAN

An authorised Financial Services Provider FSP No: 50506

AUGUST 2023

VERSION HISTORY

Document number:	**#1**
Document version:	**V1.1**
Document approval authority:	**David Bottin**
Document approval date:	**August 2023**
Document owner:	**Kevin Wides**
Document author(s):	**Kevin Wides**
Last updated:	**August 2023**
Next review date:	**December 2023**
Visibility (where will it be displayed):	**Website**

FOREWARD

This Disaster Recovery Plan (DRP) describes the strategy and procedures for recovering vital information systems, records and data should a disaster substantially disrupt operations.

The plan contains information about the organisation that should be controlled and closely held. This information could be leveraged by your adversaries to compromise your information systems and personnel. This information should be restricted to management and the individuals who will be responsible for recovering Data Center operations.

The plan will be updated routinely to reflect changes in hardware, software, procedures, applications, and staffing. Updated revisions are distributed to the disaster recovery team members at least twice a year following disaster recovery tests.

When copies of the plan are no longer required, please return them to the Business Continuity Coordinator (BCC). It is strongly recommended that outdated copies of the plan be destroyed by crosscut shredding when updated versions are received. All corrections are welcome at any time and should be directed to the BCC:

CONFIDENTIALITY STATEMENT

Employees, consultants, officers and directors must maintain the confidentiality of confidential information entrusted to them by the Company or other companies, including our suppliers and customers, except when disclosure is authorized by a Line Manager or legally mandated. Unauthorized disclosure of any confidential information is prohibited. Additionally, employees and consultants should take appropriate precautions to ensure that confidential or sensitive business information, whether it is proprietary to the Company or another company, is not communicated within the Company except to employees who have a need to know such information to perform their responsibilities for the Company.

Third parties may ask you for information concerning the Company. Subject to the exceptions noted in the preceding paragraph, employees, consultants, officers and directors (other than the Company's authorized spokespersons) must not discuss internal Company matters with, or disseminate internal Company information to, anyone outside the Company, except as required in the performance of their Company duties and, if appropriate, after a confidentiality agreement is in place. This prohibition applies particularly to inquiries concerning the Company from the media, market professionals (such as securities analysts, institutional investors, investment advisers, brokers and dealers) and security holders. All responses to inquiries on behalf of the Company must be made only by the Company's authorized spokespersons. If you receive any inquiries of this nature, you must decline to comment and refer the inquirer to your supervisor or one of the Company's authorized spokespersons. The Company's policies with respect to public disclosure of internal matters are described more fully in the Company's Disclosure Policy, copies of which are available from the Company's Managing Director.

You also must abide by any lawful obligations that you have to your former employer. These obligations may include restrictions on the use and disclosure of confidential information, restrictions on the solicitation of former colleagues to work at the Company and non-competition obligations.

Table of Contents

INTRODUCTION

A disaster will result in real losses, both for the Information Systems themselves, and for much of the stored data. At a minimum, time, money, and operational capability will be lost. A physical disaster (hurricane, flood, explosion, etc.) would lead to the loss of at least some data and software. A Disaster Recovery Plan is an essential element of a comprehensive Business Recovery Program. Other elements include the Business Continuity Plan, the Business Impact Analysis, the Vital Records List, and the Emergency Response Plan.

SCOPE

This plan addresses all preparation and steps necessary to restore processing on the above described system(s) so that dependent applications can resume processing after a disaster has rendered any or all of the systems inoperable.

PURPOSE

This Disaster Recovery Plan documents Raise Global SA (Pty) Limited's (herein referred to as "Raise") Disaster Recovery Program for recovering limited information systems operations after a disaster. The plan describes the preparation and actions required to effectively respond to a disaster, assign responsibilities, develop strategies and specific procedures, and conduct testing and after-action activities and update and maintain the plan.

In the event of a disaster, the Damage Assessment/Salvage Team (reference Section 2.6.1) will evaluate the damage to the facility and hardware and functional capability of the Information Systems and report its findings to the Executive Management Team (reference Section 2.6.2). The Executive Management Team will consider the findings together with other available information and make a decision regarding a formal disaster declaration. In order to declare a disaster, the Executive Management Team will apply a balancing test to determine if the potential financial and outage impact resulting from the disaster exceeds the cost of recovering the system(s) at an alternate site. Only the Executive Management Team has the authority to declare a disaster.

DISASTER DEFINITION

For the purposes of this plan, a disaster is any unplanned event that prevents the provision of services needed by the participating applications for a period of 24 hours. Conditions that could be declared a disaster include, but are not limited to, extended electrical power outage to the computer room, or extensive fire, smoke, water, or explosion damage to computing equipment.

ASSUMPTIONS

The Disaster Recovery Plan has been developed under the following assumptions:

- Only applications identified as being necessary to maintain mission essential functionality in the Business Impact Analysis will be supported.

- A disaster will result in real losses, both for the Information Systems themselves, and for much of the stored data.

AREA-WIDE DISASTERS

If Raise is adversely affected in an area-wide disaster, the first priority is the well-being of staff members and their families. After the first 24 to 48 hours, the Executive Management Team (reference Section 3.1) will meet to determine if and when the Disaster Recovery Plan is to be activated. The decision will be coordinated with the Business Continuity Coordinator, the Business Continuity Executive Management Team and with application owners participating in the Disaster Recovery Program.

External Contacts

Name	Phone	Email	System	Role Description
Clinton Forlee	***082 450 3376***	***Clinton@forlee.co.za***	***IT***	***IT vendor***

SYSTEM RESOURCES

Category	Resource Type	Name	Resource Description
Hardware			
Software			
Peripherals			
Telecom			
Database			
Other			

CRITICAL CONTACTS AND RESOURCES

Critical Contacts/Roles		*Critical Resources*		
TBC	***TBC***	***TBC***	***TBC***	***Regional Manager***
TBC	***TBC***	***TBC***	***TBC***	***Head of Operations***
TBC	***TBC***	***TBC***	***TBC***	***Head of Finance***

DISRUPTION IMPACT

Resource	*Outage Impact*	*Allowable Outage*
TBC		

RESOURCE RECOVERY PRIORITY

Priority	*Resource*	*Comments*
TBC		

DISASTER RECOVERY STRATEGY

SYSTEM INFORMATION

BACKUP AND OFFSITE STORAGE PROCEDURES

OFFSITE STORAGE SERVICES

Raise has contracted with a commercial vendor to provide lockable space in a secure, environmentally controlled facility suitable for housing computing equipment. The facility is located at the offices of Forlee Communications, Johannesburg and authorised staff have 24x7 access.

Raise has contracted with a commercial vendor to provide secure offsite tape storage services. The vendor's facility and procedures meet industry standards for secure storage. The following services are provided under our contract:

Contracted Tape Storage Services
The vendor can respond within minutes
Delivery of the backup tapes between the storage facility and the primary operating facility on a weekly schedule
Delivery of backup tapes (both those stored at the storage facility and at the primary operating location) to the alternate site upon request and as directed by the Business Continuity Coordinator (both for disaster recovery tests and for an actual disaster
Delivery of the backup tapes from the alternate site back to primary operating location

Both the alternate recovery facility and the offsite tape storage services facility are sufficiently geographically separated from the primary operating facility that they are on different power grids to minimize disruption during a power outage at the primary location. The two facilities are not susceptible to the same hazards, such as fire damage or water damage, which could cause disruptions to the primary location

DISASTER RESPONSE

In the event of a disaster, the following actions will be taken. The responsible teams are indicated with the designated action. Team make-up is defined in the company Business Continuity Plan.

Example:

- Assess the damage to the facility, data center, and Information Systems to determine if a disaster should be declared. The facility should only be re-entered if re-entry is safe. (Damage Assessment/Salvage Team)
- Present findings to Executive Management Team.
- Make the decision to formally declare a disaster. (Executive Management Team)
- Establish an Emergency Operations Center, if necessary, at a location as designated in the company emergency response plan having appropriate communications and support equipment. (Executive Management Team)
- Activate Notification Plan – Notify Team Leads to Mobile Recovery Teams. (Executive Management Team)
- Activate Teams. (Team Leads)
- Notify the offsite storage facility, the alternate site, key executives, and the participating application sponsors of the disaster declaration. (IT/Telecommunications Team)
- Work with the alternate site staff to recover the designated operating systems and applications at the alternate site and establish the communications link to the alternate site in preparation for operating at the alternate site for the duration of the emergency. (IT/Telecommunications Team,)
- Restore email services at the alternate site in preparation for operating there for the duration of the emergency. (IT/Telecommunications Team)
- Develop Project Plan to reconstruct/relocate the Data Center at Primary Site. (Facility/Security Team)
- Conduct operations at the alternate site until able to resume operations at the primary operating facility or a new permanent facility. (IT/Telecommunications)
- Begin reconstruction/relocation to (new) Primary Site.
- Continue to conduct business as normally as possible remotely or at alternate workspace. (All Teams)
- Develop Transition Plan to move IT operations from Alternate Site to Data Center.
- Following transition plan, conduct preparations to leave the alternate site and to resume operations at the Data Center. (Facilities/Security Team, IT/Telecommunications Team)
- Restore operations at (new) Primary Site. Validate data and functionality.
- Notify Executive Management Team and users.

Reference Section 2.6, Functional Teams and Responsibilities, for details regarding the responsibilities of the disaster recovery teams and the actions required to accomplish the above listed tasks.

FUNCTIONAL TEAMS AND RESPONSIBILITIES

The following subsections describe each functional team's role as well as its responsibilities in preparing for and responding to a disaster. The responsibility for planning, coordinating, and managing this program is assigned to the Business Continuity Coordinator (BCC) with assistance from technical advisors. Team makeup is documented in the Business Continuity Plan.

DAMAGE ASSESSMENT/SALVAGE TEAM

The Damage Assessment/Salvage Team assesses the extent of the damage to the company information systems, reports to the Executive Management Team, and makes a recommendation on declaring a disaster. The team is disbanded upon completion of their tasks. Members of the Damage Assessment/Salvage Team are often personnel with subject matter expertise regarding hardware, telecommunications, and networking. Once the Damage Assessment/Salvage Team is disbanded, those team members will join the IT/Telecommunications Team in recovery efforts.

The team has the following responsibilities and actions before and during a disaster:

Pre-Disaster	
☐	Determine appropriate considerations/criteria for identifying the extent of the damage and the estimated duration of the outage. Ensure Damage Assessment/Salvage Team members receive appropriate training in estimating and evaluating damage and potential disaster impacts.
☐	Notify the BCC or alternate regarding the potential disaster.
Post Disaster	
☐	Coordinate with the police and/or fire department to provide for safety, security, and access to the damaged facility.
☐	Assess the damage to each area of the facility and the Data Center.
☐	Assess the damage to the Information Systems and telecommunications cabling and report findings with recommendations to the Executive Management Team and the BCC.
☐	Organise the recovery of salvageable equipment, supplies, and furnishings.

EXECUTIVE MANAGEMENT TEAM

The Executive Management Team officially declares that a disaster has occurred, authorizes the execution of the Disaster Recovery Plan, and oversees the execution of the plan during the emergency.

Pre-Disaster	
☐	Approve the Disaster Recovery Plan and all major or material modifications to the plan.
☐	Establish primary and alternate company Emergency Operations Centers ensuring that these locations are adequately prepared for a disaster.
Post Disaster	
☐	Notify the alternate site and the offsite storage facility of a possible disaster.
☐	Review the report of the Damage Assessment/Salvage Team.
☐	Declare a disaster: Establish the command post and maintain communications with Team Leads Notify Team Leads Approves activation of the alternate site.
☐	Notify Team Leads to activate IT/Telecommunications Team.
☐	Receives status updates and monitor the performance of the functional teams and the execution and effectiveness of the Disaster Recovery Plan.
☐	Deactivates plan upon notification from IT/Telecommunications Team that transition is successful and normal operating status returned.

IT/TELECOMMUNICATIONS TEAM

The IT/Telecommunications (IT/T) Team brings the Information Systems at the alternate site to operational mode by managing the relocation of services to the alternate site initiating and managing the recovery procedures at the alternate site and responding to operational problems at the alternate site. The IT/T Team also manages the transition of services back to our primary operating facility.

Pre-Disaster	
☐	Establish and maintain the recovery procedures for the alternate site information systems.
☐	Manage and maintain the backup procedures.
☐	Establish and maintain the disaster recovery data communications link to the alternate site.
☐	Plan and conduct regular full scale recovery tests.
☐	Ensure that appropriate backups are made on the prescribed, rotating basis and are regularly stored offsite.
☐	Maintain current copies of equipment inventory lists, physical plant layout/diagrams (floor plans), and other pertinent documentation including procedures, system architecture, and hardware configurations in a suitable offsite location.
Post Disaster	
☐	Mobilise IT/Telecommunications Team at alternate site. Recall backup tapes.
☐	Coordinate recovery procedures with alternate site personnel.
☐	Restore the operating systems on the alternate site servers.
☐	Establish the data communications link to the alternate site.
☐	Verify the operating systems and telecommunication services are working properly.
☐	Restore the application and databases. Run batch files if appropriate.
☐	Run system and operation jobs, as required.
☐	Implement and maintain a problem log.
☐	Support the operations at the alternate site.
☐	Order and request Procurement expedite replacements for unusable IT equipment.
☐	Ensure the backup tapes that were sent to the alternate site are returned to offsite storage.
☐	Ensure all required full-system backups are completed in preparation for leaving the alternate site.
☐	Provide information to the Executive Management Team regarding the status of the system and IT operations.

☐	Coordinate the shutdown of alternate site operations and the transition of information systems back to the Primary/New Data Center.
☐	Restore information systems to normal operations.
☐	Notify Executive Management Team to deactivate Recovery Teams.

PR/Communications/Marketing Team

The PR/Communications/Marketing Team provides assistance to customers during the disaster from the time the disaster is declared until operations resume at the primary operating facility.

Pre-Disaster	
☐	Establish relationships with local Community Groups on behalf of organisation.
☐	Pre-draft and review disaster recovery press release for immediate access in case of a disaster with Executive Management Team and Legal Team.
☐	Maintain accurate customer records including past order preferences.
☐	Make recommendations to Executive Management Team regarding pre-positioning of adequate inventory in case of a disaster.
Post Disaster	
☐	Release pre-approved press release to media outlets.
☐	Help draft flash page for website with appropriate information about disaster status.
☐	Review draft flash page message with Legal Team.
☐	Notify customers that a disaster has been declared.
☐	Advise customers of the company's disaster recovery system status, availability, and accessibility.
☐	Reach out to families of injured or dead. Establish fund in organisation's name to defray medical and funeral expenses and provide scholarships for survivors.
☐	Work with community groups to evaluate community needs. Begin/Assist in community fund to provide aid to victims. Appear at community events prepared to physically assist victims on behalf of organisation.
☐	Collect and distribute household items for victims.
☐	Continue to monitor corporate status and provide internal updates and periodic press releases as directed.

Facilities and Security Team

The Facilities and Security Team provides facility and security support for the organization.

	Pre-Disaster
	Prepare up-to-date property management lists, inventory lists, and other pertinent documentation.
	Ensure current copies of this documentation are suitably stored offsite.
	Post Disaster
	Coordinate with the police and/or fire department to provide for safety, security, and access to the damaged facility.
	Provide for personnel and physical plant security at both the alternate site and the disaster site.
	Initiate, coordinate, and expedite construction and work requests to prepare the primary operating facility to receive equipment, supplies, tools, machinery, and utilities (electrical power, telephones, network connectivity, air conditioning, plumbing, water, gas, and HVAC) if reoccupation is feasible.
	Monitor the construction of the new/repaired facility, and the installation of all utilities and other essentials.
	Inform the Executive Management Team when the new/restored facility is ready for reoccupation.

Resuming Normal Operations

While recovery operations are ongoing at the alternate site, the Facilities/Security Team will be managing the restoration or rebuilding of the primary location.

Information Security

While operating at the alternate site, information security must be assured by industry best practices firewall configuration and the appropriate security controls. The information system operating at the alternate site must be configured in accordance with the policies and procedures governing our corporate information systems. As processing continues at the alternate site, information systems located at the alternate site must be closely monitored to ensure the systems are not compromised.

The security controls on the email messaging servers must be configured in accordance with the policies and procedures governing the security of our normal messaging services.

While processing in recovery mode, all information systems must be monitored to ensure they are not compromised.

TESTING THE DISASTER RECOVERY PLAN

Testing and exercising the Disaster Recovery Plan helps to verify that the recovery procedures work as intended and that the supporting documentation is accurate and current. Testing also provides an opportunity to identify any omissions in recovery procedures or documentation, and to determine whether personnel are adequately prepared to perform their assigned duties. Therefore, we will regularly schedule exercises of the Disaster Recovery Plan at the vendor alternate site, referred to as alternate site tests (full scale tests).

Alternate Site Test Procedures

Resources permitting, the BCC schedules two full scale tests per year with sufficient time to test the operating system and application recovery procedures. The initial hours are dedicated to exercising the system recovery procedures and establishing the communications link. The remaining hours are dedicated to testing the recovery of participating applications. The full-scale tests are managed and conducted by members of the IT/Telecommunications Team.

Prior to the full scale tests, the IT/Telecommunications Team determines which backup tapes will be used for the tests; establishes a test plan which outlines the IT/Telecommunications Team, goals and activities for the given test; conducts the necessary preparations for the test; and assists application owners in their preparations for the full scale test. (Application owners may set their own full scale test objectives.) During the tests, in addition to providing tester assistance, the IT/Telecommunications Team participants maintain a running log of the test activities and requests input from all participants, including testers, to assist in the post-test review and lessons learned.

After every test, the IT/Telecommunications Team conducts an after action briefing to present lessons learned to all participants and Management in order to improve the recovery procedures and the plan documentation.

Alternate Site Test Schedule

The bi-yearly tests are scheduled approximately six months apart. To date, no tests have been conducted. The next scheduled tests are:

Test #	***Test Date***	***System to be Tested***

The following are the dates of the previous tests for the indicated systems:

Test #	***Test Date***	***System Tested***

ALTERNATE SITE TEST PLANNING

To ensure a successful full-scale test, the full scale tests team will:

90 Days Prior	
☐	Confirm with the alternate site vendor that the alternate site information systems and data communications configurations will meet the organisational information systems requirements, and that the alternate site will be ready for the test.
60 to 45 Days Prior	
☐	Set the IT/Telecommunications Team objectives for the test and establish action items for the team in preparation for the test.
☐	Disseminate information to the internal IT community regarding the test.
30 Days to 10 Days Prior	
☐	Confirm that preparatory tasks are being completed and review the schedule of events for the days of the full scale tests.
☐	Distribute Player Handbook to participants.
☐	Schedule facilitator training (if required).
☐	Complete the Exercise Data Sheet.
☐	Finalie PowerPoint™ presentation and exercise documentation.
☐	Confirm facilitators, scribes and other support personnel attendance and responsibilities.
10 Days Prior to Exercise Start	
☐	Discuss the final test preparations with the alternate site vendor to confirm the alternate site configurations, to obtain the information required for the backup tapes, and to reconfirm the alternate site will be ready.
☐	Send the backup tapes and tape lists to the alternate site.
Post-Exercise	
☐	Conduct Exercise Hot Wash immediately after the exercise to capture initial lessons learned.
☐	Collect and analyse scribe data collection forms and produce an After Action Report.
☐	Formulate lessons learned and next steps to address areas of improvement identified during the exercise.
☐	Develop a corrective action plan to ensure improvements are implemented.

Application Testing Support

The IT/Telecommunications Team offers user support during a full-scale test to assist the application owners/participants in successfully running their applications at the alternate site. The assistance includes help with test preparations, on-call information systems support during the duration of the test, resolving reported problems, and serving as the liaison between the tester and the IT/Telecommunications Team.

Test preparation support includes:	
☐	Ensure testers have identified test data for the full scale test.
☐	Ensure testers have developed detailed test scripts for the full scale test and have no further questions.
☐	Ensure users have the necessary contact phone numbers for IT/Telecommunications Team member support during the full scale test.

Full scale tests support includes:	
☐	Ensure Database Administrators validate datasets and functionality before testing begins.
☐	Notify testers when the system is ready for testing.
☐	Respond to system-specific questions and to application problem reports, ensuring they are resolved.
☐	Record all problem reports and general notes to a log that is made available to the entire IT/Telecommunications Team, application owners, and testers.

Post-Test Wrap-Up

Two debriefings are scheduled on the days immediately following the full scale test. One is for the IT/Telecommunications Team and testers to discuss the recovery procedures and testing results. The second will be a briefing for Management and will include recommendations for corrective actions.

These meetings are opportunities to address:

- Areas where the exercise was successful,
- Problems that were encountered, and
- Recommendations for improvements.

Based on the conclusions, an “action list” of improvements to be made prior to the next test is developed and responsibility for implementing each action item is assigned.

TRAINING

In addition to regular testing, it is recommended that team members and managers receive annual refresher training regarding the emergency alert and notification procedures. The following are the completed training sessions:

Date	***Training***

MAINTAINING THE PLAN

The Business Continuity Coordinator, in coordination with the IT/Telecommunications Team Leader, is responsible for the maintenance of this document. The plan is updated as needed:

- In response to events such as office moves, telephone number changes, new personnel on the functional teams, retirements, duty changes, and additions or deletions of participating applications;
- after each full-scale test to reflect the recommendations resulting from the post-test wrap-up debriefings; and
- after a review of the plan.

As sections of the plan are updated, the revised sections are posted to the internal BCP web site to ensure the most current information is available to DR team members. DR participants are notified of the changes and are encouraged to produce printouts for their copies of the disaster recovery plan.

Additionally, the plan will be updated in the event an actual disaster occurs. The plan will be reviewed and updated at a convenient point after the initial responses to the disaster have been completed.

Revision History

Revision Date	***Summary of Changes***

Plan Approval:

Revision	***Signed,***	***Date***

Appendix A: BUSINESS CONTINUITY GLOSSARY

Alternate Site – An alternate location, other than the main facility, that is designated for emergency use by an organisation's Emergency Operations Center (EOC), business units for business operations, and/or data processing services (IT) when the primary location(s) are inaccessible.

Auditing – A thorough examination and evaluation of an organisation's Business Continuity Plan and procedures to verify their correctness and viability.

Backlog – A measure of unfinished work in hours or days.

BIA – Acronym for Business Impact Analysis.

Business Continuity – The ability of an organisation to provide service and support for its customers and to maintain its viability before, during, and after a business continuity event.

Business Continuity Coordinator (BCC) – A member of the Executive Management Team and/or the Crisis Management Team with the responsibility for the development, coordination, training, testing, and implementation of the Business Continuity Plan.

Business Continuity Plan (BCP) – Process of developing and documenting arrangements and procedures that enable an organisation to respond to an event that lasts for an unacceptable period of time and to return to performing its critical functions after an interruption.

Business Continuity Planner – An individual responsible for the design, development, and maintenance of a Business Continuity Plan.

Business Continuity Planning – The process of developing advance plans and procedures that enable an organisation to respond to an event so that Critical Business Functions can continue without significant or unacceptable Financial Impacts and/or Operational Impacts.

Business Continuity Program – A comprehensive, collaborative approach to protecting an organisation from threats and vulnerabilities. A robust program incorporates specific plans, such as a Business Continuity Plan, that target different aspects of the continuity process to ensure an organisation can respond to and recover from all hazards.

Business Continuity Strategy – A management-approved, documented, and funded course of action to be used in the development and implementation of an organisation's Business Continuity Plan.

Business Function – A separate, discrete function or process performed by a Business Unit. For example, the Accounting Business Unit in a smaller organisation may include accounts payable and accounts receivable as Business Functions, while a larger organisation may have separate business units that perform these Business Functions.

Business Impact Analysis – The process of developing and distributing a questionnaire to determine the Financial Impact and Operational Impact on an organisation if its business offices and/or data center facilities are not available for an extended time (usually at least one month). The objective of the BIA is to provide a management-level analysis that specifically documents the daily financial impact and Recovery Time Objective (RTO) for each Business Unit and associated Processes.

Business Recovery Program – A program designed to ensure continuity of an organisation's business processes by documenting manual and alternative work-arounds so that the mission critical work can continue in the event of a loss of the IT processing environment.

Business Resumption Planning – See Business Continuity Planning.

Business Unit – A separate, discrete organisational entity that performs a specific business function or process. A Business Unit may be as small as two people or as large as an entire company.

Call List – A list of all team members and their phone numbers (home, work, cell, pager, etc.) on a Team for the Business Continuity Plan.

Cold Site – An Alternate Site consisting of space that can be configured to support business unit recovery and/or data center recovery operations. A Cold Site is basically "four walls" with access to Voice Communications and Data Communications circuits and sufficient available electrical power and HVAC to support the recovery operations. A Cold Site may or may not have raised floor, and ALL furniture and hardware must be delivered, installed, connected, and tested. May also be called a Shell Site. See also Hot Site and Warm Site.

Contingency Planning – Process of developing advance arrangements and procedures that enable an organisation to respond to an event that could occur by chance or unforeseen circumstances.

Controls – A term usually associated with Auditing and defined as procedures or other measures designed to ensure that plans and systems function correctly.

Crisis – An event that threatens the security, integrity, or facilities of an organisation and/or the safety of its employees. A Crisis may range from a building evacuation due to a bomb threat to a full-scale, easily recognised disaster. For planning purposes, a Crisis includes, but is not limited to, severe weather threats or occurrences (snow, tornadoes, etc.), senior management succession planning, power and communications outages, medical emergencies, hostage situations, bomb threats, earthquakes, elevator entrapments, etc., in addition to an obvious, easily-recognised disaster.

Critical Functions – Essential Business Functions that are time-sensitive and must be restored first in the event of a disaster or interruption to avoid unacceptable financial or operational impacts to ensure the ability to protect the organisation's assets, meet organisational needs, and satisfy regulations.

Customer List – An inventory list of all primary customers –including name, address, telephone number, and contact (if required)– that must be notified during the recovery of a business unit or an entire company. The Customer List is an essential part of an organisation's Business Continuity Plan. It is a best practice to have a complete inventory list of ALL existing customers compiled for an organisation.

Damage Assessment / Salvage Team – A trained group of personnel, made up of representatives from security, facilities, and IT, who upon notification from the Security Team that the facility is safe to re-enter, goes into the damaged facility or data center to assess and document damage to the structure, infrastructure, equipment, and furnishings. In addition, they identify assets that can be removed from the site and salvaged through repairs, refurbishing, or cleaning for re-use. This information along with recommendations for action is then compiled into a report and is presented to the Executive Management Team.

Data Communications – The transmission of data, usually in a digital form, between geographically separate locations via public and/or private electrical or optical transmission systems. Contrast with Voice Communications.

Declaration Fee – A one-time charge normally paid to a commercial vendor who provides an Alternate Site (usually a Hot Site) facility at the time a disaster is officially declared.

Department – A separate, discrete entity defined by each organisation or company. A department usually performs a specific business function or process. See also Business Unit.

Disaster – A sudden, unplanned calamitous event causing great damage or loss. In the business environment: any event that creates an inability on an organisation's part to provide essential products and/or services for an indefinite period of time.

Disaster Mitigation – Actions, plans, and activities to reduce or eliminate the effects of a disaster on business and/or data center operations.

Disaster Preparedness – Activities, plans, programs, and systems developed prior to a disaster that are used to support and enhance mitigation, response, and recovery to disasters.

Disaster Recovery Plan – The management approved document that defines the resources, actions, tasks, and data required to manage the technology recovery effort. Usually refers to the technology recovery effort.

Disaster Recovery Program – The process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organisation after a natural or human-induced disaster. Disaster recovery is a subset of business continuity.

Electronic Vaulting – The transmission of journal transactions or data records to an Alternate Site or Offsite Storage using telecommunications facilities.

Emergency Operations Center (EOC) – An Alternate Site with sufficient Voice Communications capabilities and work space used to manage the initial recovery efforts including emergency notifications using the Call List from the Business Continuity Plan. The EOC may initially be a temporary location (e.g., hotel, trailer) used by the management team to begin coordinating the recovery operations or it may be the designated Cold Site, Warm Site, or Hot Site designated for recovery operations.

Emergency Response – The initial activities and plans designed to address and mitigate a disaster's immediate and short-term effects.

EOC – Acronym for Emergency Operations Center.

Equipment List – An inventory list of all equipment and associated vendors that are required for the recovery of a business unit or an entire company. Equipment includes, but is not limited to, fax machines, printers, computer systems, monitors, cables, scanners, mail processing hardware, etc. The Equipment List is an essential part of an organisation's Business Continuity Plan. It is a best practice to have a complete inventory list of ALL existing equipment compiled and used by an organisation.

Escalation Plan – A plan that documents decision-making criteria, usually based on the Recovery Time Objective (RTO), to determine whether a Disaster declaration and implementation of the Business Continuity Plan is in the best interest of the organisation or company.

Executive Management Team – A team of senior management personnel with the ability to obligate funds and make decisions on behalf of the organisation.

Exercise – An opportunity provided to demonstrate, evaluate, and improve the combined capability and interoperability of elements to perform assigned missions and tasks to standards necessary to achieve successful outcomes.

Exercise Types –

- **Drill** – A coordinated, supervised activity usually used to test a single specific operation or function in a single agency. Drills are commonly used to provide training on new equipment, develop or test new policies or procedures, or practice and maintain current skills. Typical attributes include the following: a narrow focus, measured against established standards; instant feedback; performance in isolation; realistic environment.

- **Full Scale Exercise (FSE)** – A multi-agency, multi-jurisdictional, multi-organisational activity that tests many facets of preparedness. They focus on implementing and analysing the plans, policies, procedures, and cooperative agreements developed in discussion-based exercises and honed in previous, smaller, operations-based exercises. In FSEs, the reality of operations in multiple functional areas presents complex and realistic problems that require critical thinking, rapid problem solving, and effective responses by trained personnel. During FSEs, events are projected through a scripted exercise scenario with built-in flexibility to allow updates to drive activity. FSEs are conducted in a real-time, stressful environment that closely mirrors real events.
- **Functional Exercise (FE)** – An activity designed to test and evaluate individual capabilities, multiple functions, activities within a function, or interdependent groups of functions. Events are projected through an exercise scenario with event updates that drive activity at the management level. An FE simulates the reality of operations in a functional area by presenting complex and realistic problems that require rapid and effective responses by trained personnel in a highly stressful environment.
- **Tabletop Exercise (TTX)** – An activity that involves key personnel discussing simulated scenarios in an informal setting. This type of exercise can be used to assess plans, policies, and procedures or to assess the systems needed to guide the prevention of, response to, and recovery from a defined incident. TTXs typically are aimed at facilitating understanding of concepts, identifying strengths and shortfalls, and achieving changes in attitude. Participants are encouraged to discuss issues in depth and develop decisions through slow-paced problem solving, rather than the rapid, spontaneous decision making that occurs under actual or simulated emergency conditions.

Financial Impact – A tangible impact, measured in dollars and usually negative, resulting from the unavailability of an organisation's business office and/or data center facilities. Financial impacts are usually reported during a Business Impact Analysis (BIA) and are typically estimated on a daily basis. See also Operational Impact.

Hot Site – An alternate facility with ready-to-use equipment and resources to recover the critical business functions affected by a disaster. Hot sites vary depending on the type of facilities offered (such as data processing equipment, communications equipment, electrical power, etc.). Commercial vendors typically provide separate space/facilities with monthly subscriptions for recovering business unit operations and computer operations. See also Cold Site and Warm Site.

HVAC – Acronym for heating, ventilation, and air conditioning.

Initial Assembly Point (IAP) – A pre-defined location, such as a parking lot, hotel or person's home, where all designated team leaders and members can meet if the organisation's business offices and/or data center are not accessible for any reason.

Inventories – Specific lists of items required for the Business Continuity Plan which includes the Customer List with contact information, Equipment List (with Vendor List and contact information), Supplies List (with Vendor List and contact information), Software List (with Vendor List and contact information), Telecommunications List (with Vendor List and contact information), Vital Records List (with location of vital records). See the specific inventory item (shown in italics) for additional information.

IT – Acronym for Information Technology. A Department or Business Unit that provides computing systems support to an organisation or company.

Infrastructure – The basic supporting installations and facilities upon which the continuance and growth of a community or company depend, such as power plants, water supplies, transportation systems, and communications systems, etc. A company's infrastructure includes the physical plant and utilities necessary for essential operations.

LAN – Acronym for Local Area Network.

Local Area Network (LAN) – A short-distance network used to connect terminals, computers, and peripherals under a standard topology, usually within one building or a group of buildings. A LAN does not use public carriers to link its components, although it may have a "gateway" outside the LAN that uses a public carrier. See also Wide Area Network.

Loss – Unrecoverable business resources that are impacted or removed as a result of a disaster. Such losses may include loss of life, revenue, market share, competitive stature, public image, facilities, or operational capability. See also Financial Impact and Operational Impact.

Mission-Critical Business Activities – The critical operational and/or business support activities (either provided internally or outsourced) required by the organisation to achieve its objective(s)) i.e. services and/or products.

Mitigate – To make or become milder, less severe, or less painful.

Mobile Recovery Facility (MRF) – A mobile Warm Site, normally a large tractor-trailer available from a commercial vendor, that can be transported to a pre-determined location so that needed equipment can be obtained and installed near the original location. Depending on the vendor, an MRF may be available in a "business office" and a "data center" configuration.

Modem – An acronym for modulator/demodulator, a device that converts analog signals to digital signals and back again, usually on Voice Communications circuits.

Operational Impact – An intangible impact resulting from the unavailability of an organisation's business office and/or data center facilities. An Operational Impact cannot be

quantified in dollars, but may be critical because of its effect on an organisation. Examples of operational impacts include, but are not limited to, customer service, stockholder confidence, industry image, regulatory, financial reporting, employee morale, vendor relations, cash flow (that cannot be quantified), and increases in liability. Operational impacts are usually reported during a Business Impact Analysis (BIA) and are typically estimated on an arbitrary scale, such as 1-5, with the highest number representing the most severe impact. See also Financial Impact.

Operational Risk – The risk of loss resulting from inadequate or failed procedures and controls. This includes loss from events related to technology and infrastructure, failure, business interruptions, staff related problems, and from external events such as regulatory changes.

Offsite Storage – A designated storage facility, other than the main facility, where duplicate Vital Records and critical documentation may be stored for emergency use during the execution of an organisation's Business Continuity Plan.

Plan Maintenance – The management process of keeping an organisation's Business Continuity Management Plans up-to-date and effective. Maintenance procedures are a part of this process for the review and update of the BC plans on a defined schedule.

POTS – Acronym for Plain Old Telephone Service.

Preventative Measures – Controls aimed at deterring or mitigating undesirable events from taking place.

Prioritisation – The ordering of critical activities and their dependencies are established during the BIA and Strategic-planning phase. The business continuity plans will be implemented in the order necessary at the time of the event.

Project Management – The development, planning, organising, and management of tasks and resources to accomplish a defined objective, such as a Business Continuity Plan, usually under time and cost constraints.

Project Team – A group of people representing key organisational areas that work together and follow documented responsibilities for the design, development, and implementation of a Business Continuity Plan.

Reciprocal Agreement – An agreement between organisations with basically the same business processes and/or data processing hardware that allows one organisation to continue business operations for the other in case of disaster.

Recovery – Implementing the prioritised actions required to return processes and support functions to operational stability following an interruption or disaster.

Recovery Point Objective (RPO) – The measure of how much data loss, in hours or days, is acceptable to an organisation. The point in time at which backup data (e.g., backup tapes) must be restored and synchronised by IT to resume processing. Most IT organisations usually have an RPO of at least –1 day (–24 hours) because backups are

usually performed daily (usually at night) and transported to Offsite Storage early the following day. The best RPO is zero (0) which basically means that all affected computer systems utilise “mirroring” (real-time data/transaction copying) technology to concurrently copy all incoming data/transactions to another identical system in a remote location that is sufficiently remote from the primary site.

Recovery Time Objective (RTO) – The period of time within which systems, applications, or functions must be recovered after an outage (e.g. one business day). RTOs are often used as the basis for the development of recovery strategies and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.

The RTO has five (5) components:

(1)The time before a disaster is declared (see Escalation Plan);
(2)The time required to activate the Business Continuity Plan;
(3)The time required for the IT organisation to restore computer systems;
(4)The time required by an affected business unit to perform assigned tasks to the point at which business operations can be resumed including the time to verify that restored computer systems data is accurate and synchronised to the last available backup; and
(5)The time for each business unit to re-enter/process all Backlog (including manually processed work, if applicable) to bring business operations into current status.

Resource Requirements – The resources (e.g., people, equipment, supplies, vendors, telecommunications, vital records) required for the recovery of a business unit or an entire company as documented in the Business Continuity Plan.

Risk – Potential for exposure to loss, which can be determined by using either qualitative or quantitative measures.

Risk Assessment / Analysis – Process of identifying the risks to an organisation, assessing the critical functions necessary for an organisation to continue business operations, defining the controls in place to reduce organisation exposure, and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.

Risk Categories – Risks of similar types are grouped together under key headings, otherwise known as ‘risk categories’. These categories include reputation, strategy, financial, investments, operational infrastructure, business, regulatory compliance, outsourcing, people, technology, and knowledge.

Risk Controls – All methods of reducing the frequency and/or severity of losses, including exposure avoidance, loss prevention, loss reduction, segregation of exposure units, and non-insurance transfer of risk.

Risk Management – The culture, processes, and structures that are put in place to effectively manage potential negative events. As it is not possible or desirable to eliminate all risk, the objective is to reduce risks to an acceptable level.

Risk Transfer – A common technique used by Risk Managers to address or mitigate potential exposures of the organisation. A series of techniques describing the various means of addressing risk through insurance and similar products.

Single Source Supplier – The purchasing policy of using one supplier for a particular component or service. Single sourcing can result in higher quality and a greater level of cooperation in product development than the traditional Western approach of multiple sourcing. Single sourcing has risen in prominence, encouraging closer relationships with a smaller number of suppliers.

Software List – An inventory list of all software and associated vendors (see Vendor List) which is required for the recovery of a business unit or an entire company. The Software List is an essential part of an organisation's Business Continuity Plan. It is a best practice to have a complete inventory list of ALL existing software compiled and used by an organisation.

Supply Chain – The movement of materials as they flow from their source to the end customer. Supply Chain includes purchasing, manufacturing, warehousing, transportation, customer service, demand planning, supply planning, and Supply Chain management. It is made up of the people, activities, information, and resources involved in moving a product from its supplier to customer.

Supplies List – An inventory list of all supplies and associated vendors which are required for the recovery of a business unit or an entire company. Supplies include, but are not limited to, forms (e.g., check stock), special rubber stamps, pens, pencils, paper, paper clips, staplers, etc. The Supplies List is an essential part of an organisation's Business Continuity Plan. It is a best practice to have a complete inventory list of ALL existing supplies compiled and used by an organisation.

Task List – A list of all tasks, usually in a checklist form, which must be performed by a Team to recover a specific portion of an organisation, business function, and/or business unit. The Task List is an essential part of an organisation's Business Continuity Plan.

Team – A group of individuals assigned to work together to perform a specific function in the Business Continuity Plan. A Team consists of a Team Leader, Alternate Team Leader, and Team Members. The Team Leader is responsible for the successful completion of all tasks assigned (See Task List) to a Team.

Telecommunications – A general term that applies to analog or digital data transmitted (See also Data Communications and Voice Communications) by electrical, optical, or acoustical means over public or private communications carriers.

Telecommunications List – An inventory list of all Voice Communications and Data Communications circuits which are required for the recovery of a business unit or an entire company. The Telecommunications List is an essential part of an organisation's Business Continuity Plan. It is a best practice to have a complete inventory list of ALL existing telecommunications circuits compiled and used by an organisation.

Threat – A potential event that may cause a risk to become a loss. Threats consist of natural phenomena such as tornadoes and earthquakes and man-made incidents such as terrorist attacks, bomb threats, disgruntled employees, and power failures.

Vendor List – An inventory list of all primary vendors (suppliers) –including name, address, telephone number, and vendor representative (if required)– that provide an essential service or product required for the recovery of a business unit or an entire company. The Vendor List is an essential part of an organisation's Business Continuity Plan. It is a best practice to have a complete inventory list of ALL existing vendors compiled and used by an organisation.

Vital Record – A critical business record required for recovering and continuing an organisation's business operations. This may include employee information, financial and stockholder records, business plans and procedures, and the Business Continuity Plan. Vital records may be contained on a wide variety of media including, but not limited to, electronic (including tape, disk, and CD-ROM), hard copy (normally paper), microfilm, and microfiche.

Vital Records List – An inventory list that contains the name and offsite location of vital records (see Vital Record) required for the recovery of a business unit or an entire company. The Vital Records List is an essential part of an organisation's Business Continuity Plan.

Voice Communications – The transmission of sound at frequencies within the human hearing range which may be in digital or analog form. Contrast with Data Communications.

WAN – Acronym for Wide Area Network.

Warm Site – An Alternate Site consisting of designated office space and/or data center space that has installed voice and data communications access and is partially equipped with telecommunications interfaces, such as a Private Branch Exchange (PBX) telephone system and/or a router. A Warm Site is usually pre-wired for Voice and Data Communications so that telephones, PCs, and other computer hardware (e.g., servers) can literally be "plugged-in" as required. See also Cold Site and Hot Site.

Wide Area Network (WAN) – A network linking geographically separate metropolitan, campus, or local area networks across greater distances, usually accomplished using common carrier lines. See also Local Area Network.

Workstation – A single-person work area which usually includes office furniture (e.g., a desk), computer equipment (e.g., a PC), a telephone, and a wastebasket.

Appendix B: ADDITIONAL SUGGESTED MATERIALS

- Applications and Contact Information
- Directions to Alternate Work Site (Alternate Site)
- Disaster Alert Procedures, Team Members, and Contact Information
- Alternate Site Contact Information and Procedures
- Offsite Storage Contact Information and Emergency Procedures
- Windows Restore Procedures
- Data Communications
- Vendor Contacts
- Contents of the Documentation Box (Doc Box)
- Guidelines for Application Alternate Site Tests
- Mainframe Communications
- Electronic Messaging Recovery
- Backup Listings
- Calendars with Julian Dates
- Alternate Site Contract
- Communications Architecture and Configuration
- Disaster Recovery Communication Topology
- Instructions for Completing Shipping Labels
- Hardware Configuration
- Electronic Payroll Contingency Procedures
- Payment Processing Points of Contact

Appendix C: BUSINESS IMPACT ANALYSIS

Purpose: Identify the impacts of disruptions and disaster scenarios that result in denied access to the critical services, buildings and facilities.

Process:

- Determine your critical functions.
- Prioritise your critical functions.
- Assess the impact of denied access to normal workspaces.
- Identify the resources necessary to continue critical functions at an alternate site.
- Determine your recovery priorities and interdependencies so that recovery time objective(s) and recovery point objective(s) can be set.

Outcomes:

- A prioritised list of Mission Critical Functions.
- A list of all supporting equipment, personnel, and vital records necessary to perform your essential functions.
- A concept of operations for return to operation after an interruption of business.

Definitions:

Business Function – A separate, discrete function or process performed by a Business Unit. For example, the Accounting Business Unit in a smaller organisation may include accounts payable and accounts receivable as Business Functions, while a larger organisation may have separate business units that perform these Business Functions.

Critical Functions – Essential Business Functions that are time-sensitive and must be restored first in the event of a disaster or interruption to avoid unacceptable financial or operational impacts to ensure the ability to protect the organisation's assets, meet organisational needs, and satisfy regulations.

Supporting Functions – Essential Business Functions that are routinely performed in order for business operations to run smoothly but are **not** critical to avoiding unacceptable financial loss, satisfy safety concerns or meet other organisational needs.

Action:

1. Identify Knowledgeable Functional Area Representatives

These are your department heads and team leaders. These individuals perform your business processes or have in the past. They know what is required to successfully complete their tasks.

2. Identify Organisation Functions including information and resources (people, technology, facilities, etc.)

When identifying organizational functions it is important to identify and write down what tools you need (people, raw materials, equipment, technology, etc.). The ability to perform a function is dependent not only on assigning a body to the job but also on all of the underlying resources that support the function. So, if a function requires office supplies, include those in your list. If it is critical that personnel stay onsite for their entire shift, make sure that you include things like a fully equipped break room.

3. Identify and Define the Priority of Criticality Criteria

Now that you've identified your functional experts, systems, equipment, records and supplies that are necessary to accomplish your critical functions, you need to determine the criticality of those functions. It is important to recognise that not every function is critical or even required in a crisis environment. Your functional experts should brainstorm to develop a list of criteria that are used to determine criticality. The easiest way to do this is to give each item on your criticality list a numeric value. This is a simple way to see what is most important to consider about a function and what is not. Once all of your functions are scored against the criteria, those with the highest score are the most critical.

4. Senior Management Review

Once your functional experts have developed your list of criteria and assigned a value to each, it is important to the process to obtain senior management approval of the criteria and values. They may want to add or subtract criteria, or change values. With their understanding of the entire business process, they may see things at the macro level that have been lost while the functional experts have been focusing strictly on step by step processes.

5. Coordinate Analysis

At this point, you and your team must coordinate your lists. You may be the boss, but if you want the plan to work you need buy-in from the people you work with on a daily basis. Working together to develop a rank-ordered list of critical functions helps to build consensus and buy-in. Once you have each of the functions rank ordered by priority, the analysis continues to refine the product. You need to determine whether or not it is feasible to attempt to perform all of the functions in a crisis environment, if the leadership wants to delegate some functions, if it is necessary to establish a cut off point that you won't drop below, if you can maintain your supply chain for critical materials, etc. This process is likely to be the most difficult step of the analysis. Everybody considers their function a priority. However, in a crisis that isn't always possible. Equally important in this process is determining those personnel, systems, records, etc. that are non-essential and how you are going to handle them.

6. Identify Interdependencies (Internal and External to the Organisation)

Now that you have a prioritised list, you can further define and refine it by examining where functions are dependent upon other entities both inside and outside the organisation. Once you have identified the interdependencies, you have to coordinate with those other entities to develop a support plan for emergencies.

Finally, you have your final draft list of functions, essential personnel, systems, records, supplies and other equipment to perform the most essential functions of your business. You have also developed the critical information that will determine your concept of operations in the crisis environment.

7. Define Restoration Objectives and Timeframes

Up to this point, you have focused on what and how to function during a crisis. Continuing operations during a crisis is hard work. Maintaining recovery operations will take so much of your attention, returning to normal operations is sometimes forgotten in the process. Now is the time to decide how to get back to full operations at a permanent site.

This is often the most difficult step. Moving to a new permanent location may require phased operations. Rebuilding at your current site may require shifting all or part of your operations to temporary facilities. You may lack the resources to make a move or to immediately start rebuilding because of the nature or magnitude of the emergency. In those cases, you need to time-phase the process. Whatever your requirements are for return to your full operational capabilities, they need to be identified here.

Do not skimp in this area. You can have the best plan for crisis operations in the world, but if you can't get your facility back to full capability at a permanent site then ultimately you have failed. Remember, you will rely on outside help from the government, insurance companies, utilities, and construction companies, among others. All of these will have many demands on them for attention in a large scale emergency.

Enclosures: **1. BIA Form**
2. Application Impact Analysis form

C. 1 Business Impact Analysis Questionnaire

Department Name:	
Completed By:	

Organisational Impact				
The loss of this business unit would have the following effect on the organisation:				
☐ **Catastrophic**	☐ **Moderate**	☐ **Minor**		
Comments:				
How long can your organisation perform without this business unit?				
Check only one.	☐ **Up to 3 days**	☐ **Up to 1 week**	☐ **Up to 1 month**	☐ **Other:**
Comments: (*Assume that the loss of this business unit occurred during your busiest or peak period*.)				
Does this business unit have peak operational periods?			☐ **Yes**	☐ **No**
If yes, identify peak periods for this business unit: **Day:** **Week:** **Month(s):**				
Have you developed/established workaround procedures (manual or otherwise) to continue operations in the event the business unit is unavailable?			☐ **Yes**	☐ **No**
If yes, please indicate when the procedures were last tested and explain the results:				

Use the following codes for the next four questions:

A. Up to $10,000
B. $10,000 - $100,000
C. $100,000 - $1,000,000
D. $1,000,000 - $10,000,000
E. Over $10,000,000

	Day 1	***Day 3***	***Week 1***	***Week 2***	***Week 3***
1. Losing this unit will result in lost revenue from fees, collections, interest, penalties, etc.					
2. Losing this unit will erode our customer base. The cost our to the organisation from lost business is estimated at:					
3. Losing this unit will result in the following fines and penalties due to regulatory requirements (federal, state, local):					
4. The loss of this business unit has legal ramifications due to regulatory statutes, contractual agreements, etc. Specify potential areas of exposure:					

C.2 Application Impact Analysis Questionnaire

Preliminary System Information	
Organisation:	Date BIA Completed:
System Name:	BIA POC:
System Manager Point of Contact (POC):	
System Description: (*Discussion of the system purpose and architecture, including system diagrams*):	

A. Identify System POCs	**Role**
Internal (*Identify the individuals, positions, or offices within your organisation that depend on or support the system; also specify their relationship to the system*)	
External (*Identify the individuals, positions, or offices outside your organisation that depend on or support the system; also specify their relationship to the system*)	

B. Identify System Resources (*Identify the specific hardware, software, and other resources that comprise the system; include quantity and type*)	
Hardware	
Software	
Other Resources	

C. Identify Critical roles (*List the roles identified in Section A that are deemed critical****)***

D. Link critical roles to critical resources (*Identify the IT resources needed to accomplish the roles listed in Section C***)**

Critical Role	Critical Resources

E. Identify outage impacts and allowable outage times (*Characterise the impact on critical roles if a critical resource is unavailable; also, identify the maximum acceptable period that the resource could be unavailable before unacceptable impacts resulted***)**

Resource	Outage Impact	Allowable Outage Time

F. Prioritise resource recovery *(List the priority associated with recovering a specific resource, based on the outage impacts and allowable outage times provided in Section E. Use quantitative or qualitative scale {e.g., high/medium/low, 1-5, A/B/C})*

Resource	***Recovery Priority***
