

# Reef Trust Partnership



## Risk Management Plan



Australian Government

REEF TRUST



Great Barrier  
Reef Foundation

# Contents

---

Preface	3
Purpose of this document	4
Risk Management Framework	5
GBRF Risk Management Plan	6
Governance and Oversight	6
Risk Management Policy	7
Role of the Board in relation to risk and business continuity	7
Audit, Risk and Compliance Committee	7
Partnership Management Committee	8
Traditional Owner Working Group	8
GBRF Project Management Office	8
Risk and Compliance Manager	9
Business Continuity and Disaster Recovery Plan	9
GBRF Risk Appetite Statement	9
Enterprise Level Material Risks	10
Component Level Risk Management	12
APPENDIX 1 Risk Management Policy	13
APPENDIX 2 Risk Assessment Template	15
APPENDIX 3 Business Continuity and Disaster Recovery Plan	16

*Photography: Gary Cranitch, Queensland Museum*



## Preface

---

The Great Barrier Reef (the Reef) is the largest living structure on the planet and is so large it can be seen from space. It's home to the most extraordinary array of animals and birds, and is often referred to as the rainforest of the sea. Sir David Attenborough describes it as:

*“one of the greatest, and most splendid natural treasures that the world possesses.”*

Today, however, the Reef is under threat from climate change and local stresses. We need the help of all Australians to protect and restore the Reef. Over the last two decades, the Great Barrier Reef Foundation (GBRF) has drawn together the many groups who are working to protect the Reef. There are hundreds of people and organisations working to achieve this including universities, research institutions, government agencies, scientists, traditional owners and community groups. The GBRF is the place where these myriad groups (large and small) come together to work on the highest priority projects which will have the greatest impact on protecting and restoring the Reef.

Our projects have had a measurable impact on the health of the Reef including monitoring reef health in near-real time (eReefs) to securing the future of green turtles on Raine Island (Raine Island Recovery Project), to developing the first portfolio of projects to address the resilience of reefs adapting to climate change. We also have a track record in innovation, developing solutions such as the RangerBot which detects and addresses threats to coral reefs.

Underpinning this partnership is a record government investment of \$443.3 million to tackle critical issues of water quality and crown-of-thorns starfish control, harness the best science to restore reefs and support reef resilience and adaptation, enhance Reef health monitoring and reporting, and increase community engagement on the Reef.

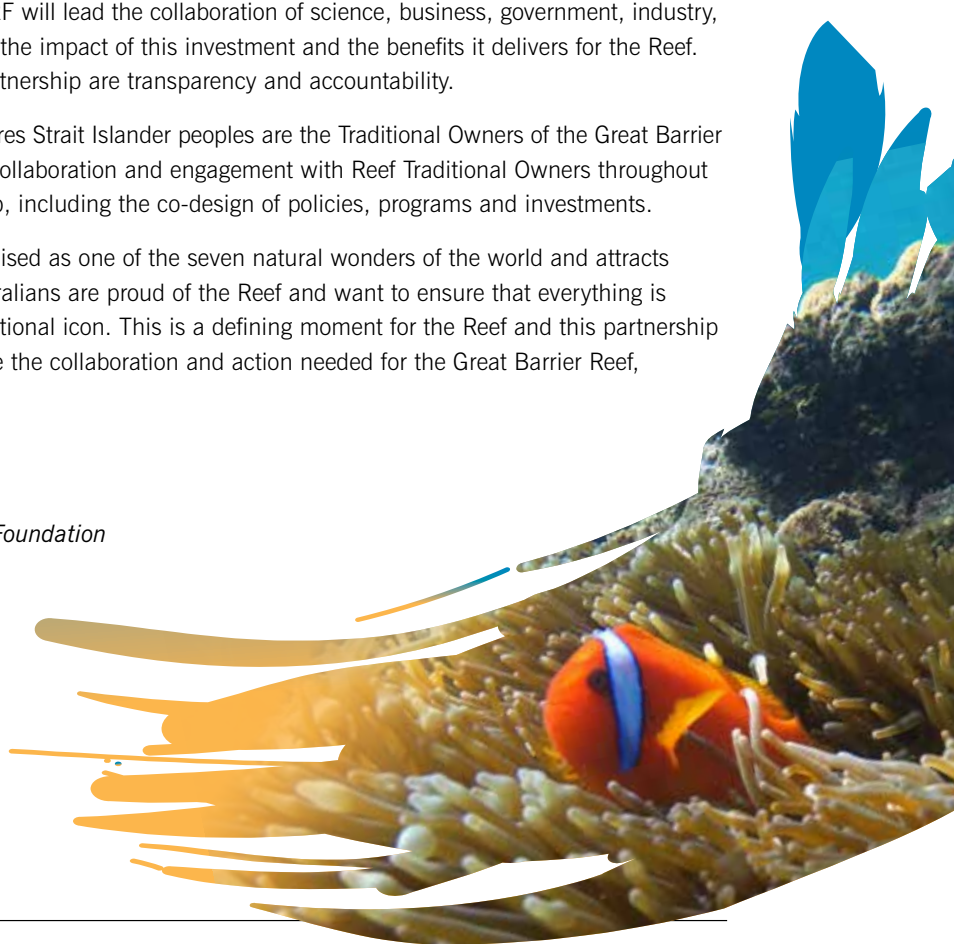
Through the Reef Trust Partnership, GBRF will lead the collaboration of science, business, government, industry, philanthropy and community to amplify the impact of this investment and the benefits it delivers for the Reef. Our guiding principles to deliver this partnership are transparency and accountability.

The GBRF recognises Aboriginal and Torres Strait Islander peoples are the Traditional Owners of the Great Barrier Reef. We are committed to meaningful collaboration and engagement with Reef Traditional Owners throughout the delivery of the Reef Trust Partnership, including the co-design of policies, programs and investments.

The Great Barrier Reef is globally recognised as one of the seven natural wonders of the world and attracts over two million visitors each year. Australians are proud of the Reef and want to ensure that everything is being done to protect and restore our national icon. This is a defining moment for the Reef and this partnership is an unprecedented opportunity to drive the collaboration and action needed for the Great Barrier Reef, now and for the future.

Anna Marsden

*Managing Director, Great Barrier Reef Foundation*



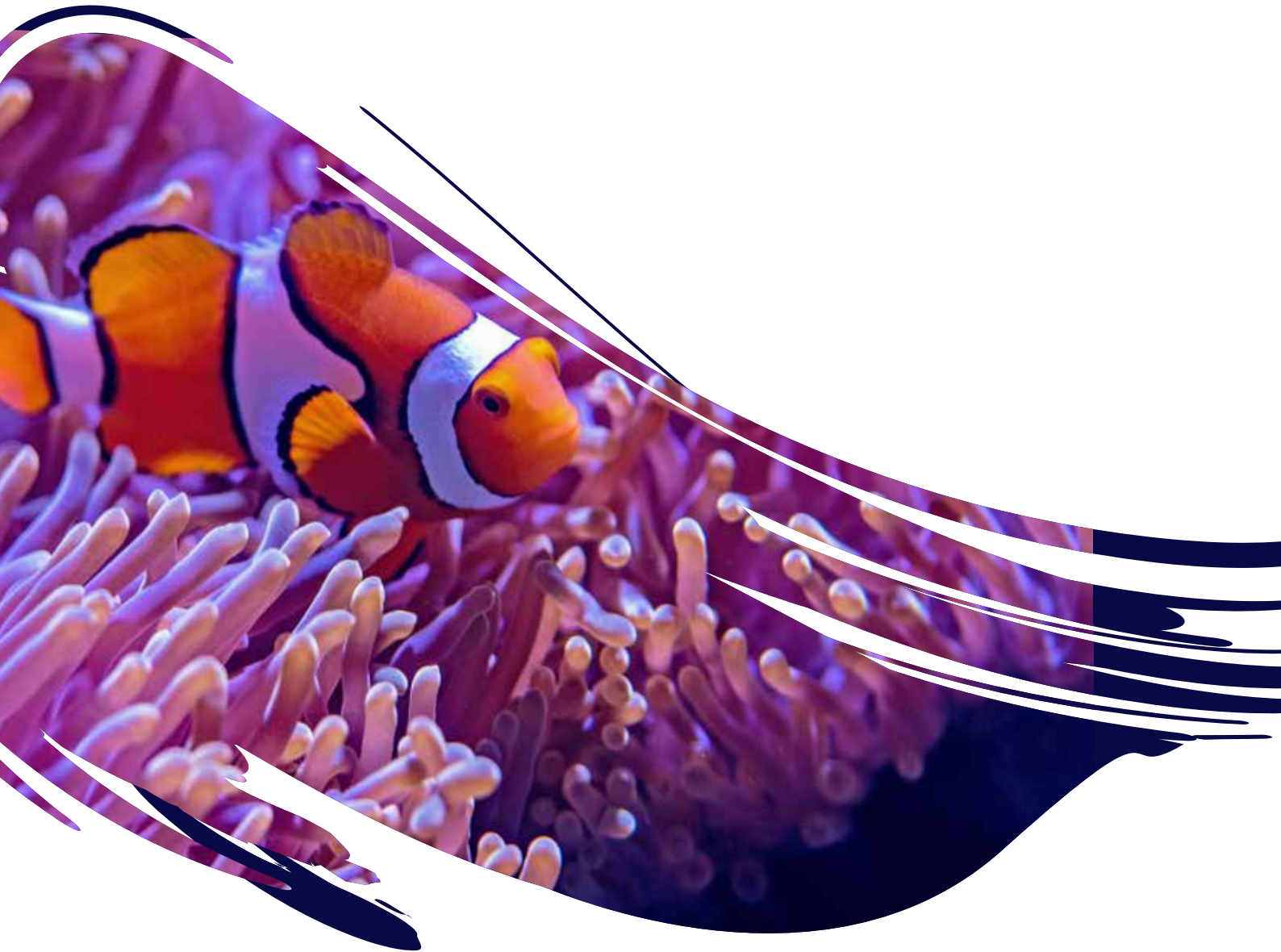


## Purpose of this document

---

The Grant Agreement (the Agreement) between the Department of the Environment and Energy and the Great Barrier Reef Foundation (GBRF) sets out the requirements for the Reef Trust Partnership.

This Risk Management Plan provides an overview of risk management of the Reef Trust Partnership and its alignment to the GBRF's Risk Management Policy, Risk Management Framework and Business Continuity. Key to this process is building on the GBRF's current Risk Management Plan and to further embed a culture of risk awareness. This plan will be reviewed annually.



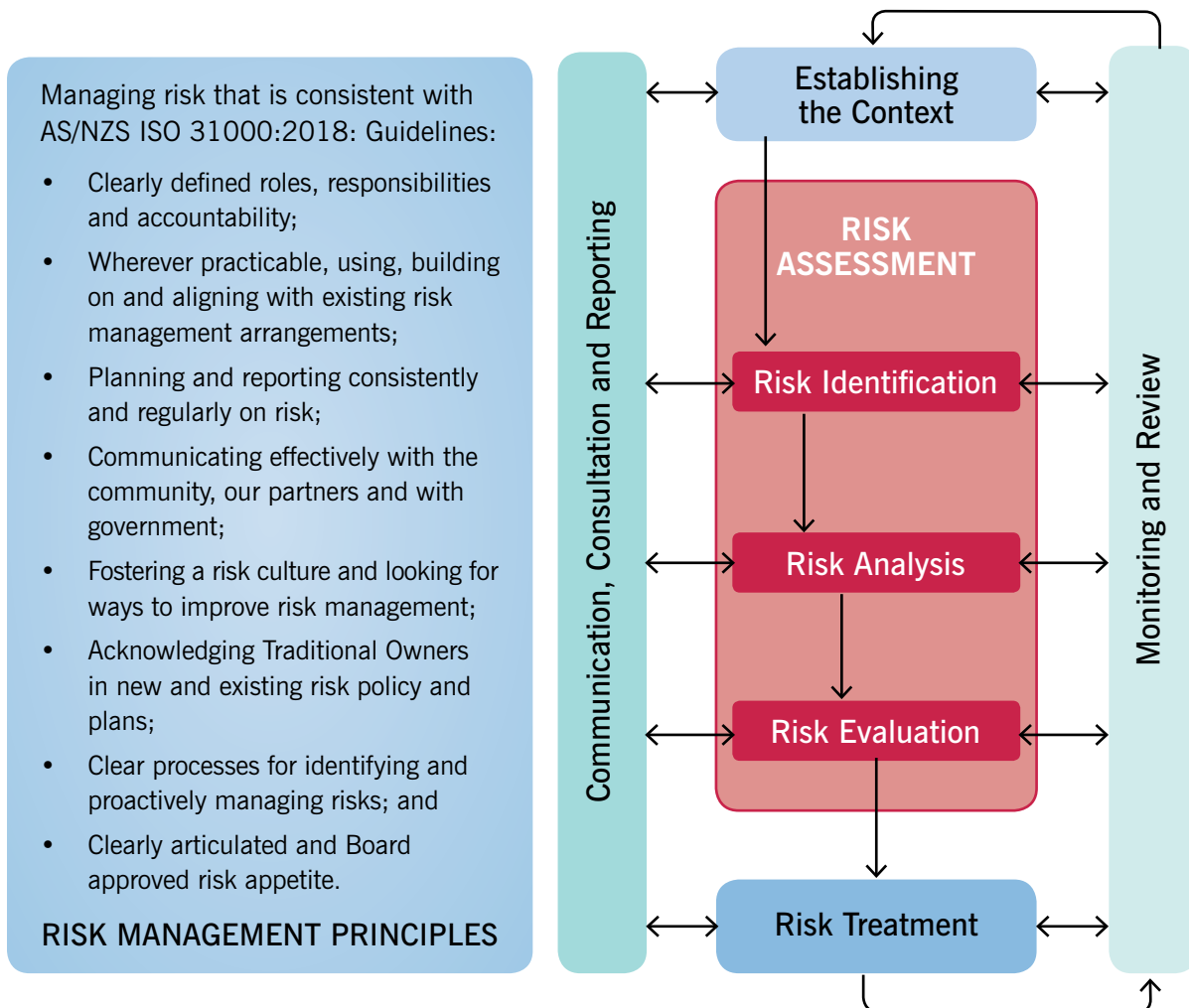
# Risk Management Framework

The Risk Management Framework (the Framework) is presented in Figure 1.1 and outlines GBRF’s approach to risk oversight and management consistent with Australian/New Zealand Standards (AS/NZS ISO 31000:2018: Risk Management – Guidelines). It encompasses the mandate and Board approved risk appetite statement; the risk management principles and policy; the plans, relationships, accountabilities, resources, processes, and activities employed to manage risk. It shows the process adopted by GBRF for the ongoing:

- identification, analysis and evaluation and monitoring of risks and any changes to those risks, including risk assessments and plans for individual projects;
- development and implementation of processes to monitor, treat and manage risks;
- reporting of risks and implementation of mitigating controls; and
- response to any emerging risks or risks that may materialise as a consequence of adverse events.

The component level risk assessments will be developed and progressed in line with the Reef Trust Partnership Investment Strategy.

Figure 1.1 GBRF Risk Management Principles and the Framework



## GBRF Risk Management Plan

The GBRF’s Risk Management Plan consists of:

- Risk Management Framework;
- Risk Management Policy; and
- Risk Appetite Statement.

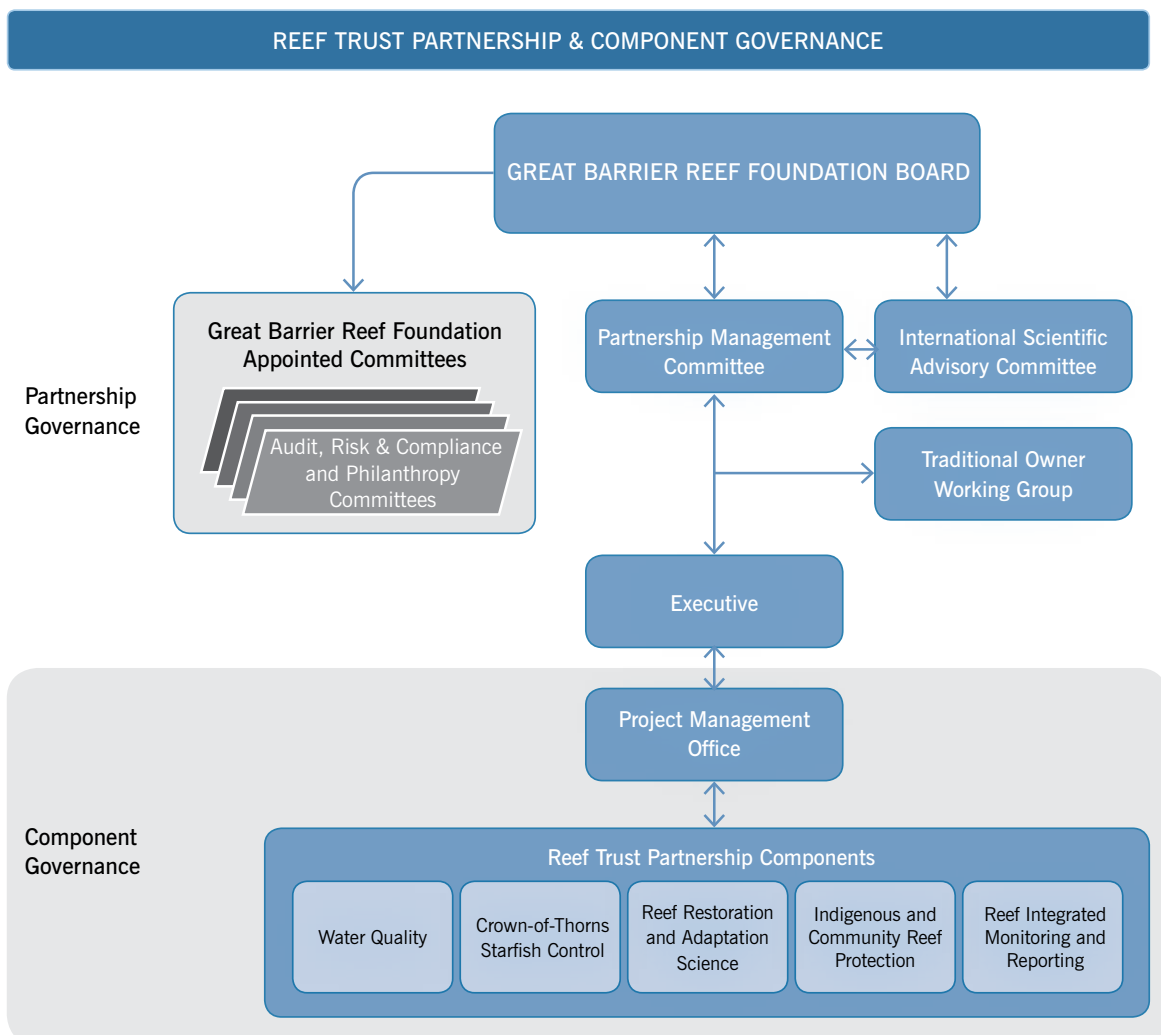
The Risk Management Plan is supported by:

- governance and oversight;
- qualified and trained staff;
- related strategic and operational plans and activities that manage risk controls (such as the Business Continuity and Disaster Recovery Plan); and
- template for project risk assessment.

## Governance and Oversight

The GBRF governance structure is shown in Figure 1.2.

Figure 1.2 Reef Trust Partnership and Component Governance Arrangements



## Risk Management Policy

The Risk Management Policy provides the specific link between the GBRF's strategic purpose and outcomes and sets out the organisation's approach to risk and responsibilities, also ensuring that management fosters an organisational culture with effective business risk management. The Risk and Compliance Manager is responsible for periodically reviewing the GBRF's Risk Management Policy (Appendix 1).

## Role of the Board in relation to risk and business continuity

The GBRF Board (the Board) is an independent, skills-based board. The Board has overall accountability for the Reef Trust Partnership, as is the case for all GBRF investments.

In relation to risk and business continuity, and guided by recommendations from the Audit, Risk and Compliance Committee and the Partnership Management Committee (PMC), the Board has responsibility for:

- ensuring appropriate risk governance arrangements across the activities of the Reef Trust Partnership;
- approval of the Risk Appetite Statement;
- oversight of risk management and compliance; and
- approval of annual work plans and relevant business and strategic plans that address enterprise level risk.

## Audit, Risk and Compliance Committee

The Audit, Risk and Compliance Committee is an independent committee, appointed by the Board to assist in fulfilling its oversight responsibilities in relation to GBRF's financial reporting, internal control processes and systems, risk management processes and systems, and the internal and external audit functions.

In relation to risk and business continuity the Audit, Risk and Compliance Committee has responsibility for:

- ensuring appropriate enterprise risk management and compliance;
- considering the effectiveness of internal controls and adequacy of systems and processes as identified by the internal and external auditor;
- reviewing compliance with statutory and financial reporting requirements;
- reviewing the details of directors' and officers' insurance;
- investigating instances of suspected or actual fraud;
- other matters that it considers should be reported to the Board; and
- oversight of ensuring compliance with relevant WHS legislation and required training.





## Partnership Management Committee

The Partnership Management Committee (PMC) is an independent committee appointed by the Board with its sole focus being the Reef Trust Partnership. In relation to risk and business continuity of the Agreement the PMC's role is to provide:

- oversight and implementation of appropriate risk governance arrangements, including Component level risk governance;
- oversight and implementation of the risk management policy and risk management framework;
- oversight and implementation of the business continuity plan;
- advice and make recommendations to the Board on risk and business continuity;
- strategic oversight of the Reef Trust Partnership portfolio activity and delivery consistent with the Agreement and the associated risk management and business continuity requirements; and
- oversight of portfolio risk management and risk reporting.

## Traditional Owner Working Group (TOWG)

The GBRF is committed to meaningful collaboration and engagement with Reef Traditional Owners throughout the delivery of the Reef Trust Partnership. The GBRF has identified Indigenous and Traditional Owners cultural capability training as a key aspect of managing risk and welcomes an ongoing productive relationship with Traditional Owners.

Additionally, to better understand risk, the GBRF has access to Traditional Owner perspectives through the TOWG, whose role is to:

- provide strategic advice to the PMC and GBRF Executive on matters relevant to operationalising and delivering actions in collaboration with Traditional Owners within the Reef Trust Partnership;
- ensure the views and knowledge of Great Barrier Reef Traditional Owners are reflected in the development and implementation of the Reef Trust Partnership;
- participate in strategic meetings, workshops and stakeholder forums to provide input and advice on matters affecting, or of high importance to, Great Barrier Reef Traditional Owners; and
- communicate with Great Barrier Reef Traditional Owners to ensure application of best practice approaches to respecting, recognising and engaging with Aboriginal and Torres Strait Islander peoples are maintained.

## GBRF Project Management Office (PMO)

The PMO is comprised of GBRF staff. In relation to risk and business continuity the PMO's role is to:

- undertake project development and management activities including Component level risk identification;
- track and report on project progress in accordance with the Agreement and Board requirements (including reporting on material Component level risks that may prevent project delivery);
- maintain secretariat support to the Board and Committees appointed by the Board as appropriate, including risk reporting and business continuity management; and
- ensure all projects, grantees and delivery partners are compliant with relevant GBRF policies and procedures and the terms of the Agreement.



## Risk and Compliance Manager

The GBRF has a dedicated Risk and Compliance Manager who is responsible for ensuring that risks are identified, appropriately managed, and the Risk Management Plan is understood and applied by all GBRF employees.

The Risk and Compliance Manager is also responsible for developing and deploying a Business Continuity and Disaster Recovery Plan that supports the GBRF to manage its business continuity and to undertake business recovery activities should this be required.

Key responsibilities of the Risk and Compliance Manager:

- Build on, review and update the GBRF Risk Management Policy and Procedures;
- Raise the risk maturity of GBRF personnel;
- Prepare and report on risk and compliance to the PMO and the relevant committees and Board;
- Compliance, including regulatory, operational and financial;
- Undertake regular risk management reviews and make recommendations and improvements;
- Develop, review and improve the Business Continuity and Disaster Recovery Plan
- Fraud awareness and investigation; and
- Manage corporate and other insurance.

## Business Continuity and Disaster Recovery Plan

The Business Continuity and Disaster Recovery Plan (Appendix 2) is an important component of the GBRF's risk management approach. It identifies:

- the purpose of business continuity and disaster recovery planning;
- key roles and responsibilities;
- how the Plan is to be used;
- key information to support business continuity and disaster recovery;
- the frequency of business continuity testing; and
- when the Plan is to be reviewed.

## GBRF Risk Appetite Statement

The amount and type of risk the GBRF is willing to accept in pursuit of delivering the Reef Trust Partnership objectives is detailed in the risk appetite statement below.

*The GBRF has no risk tolerance for expenditure that is not in line with obligations detailed in the Agreement including capital losses on invested grant funds or co-contributions. The GBRF also has no risk tolerance for instances of fraud or activities that put at risk the health and safety of our people. The GBRF will have a higher risk tolerance when seeking innovative solutions to new or existing threats and challenges and taking advantage of new opportunities to ensure the objectives of the Reef Trust Partnership agreement are met.*

## Enterprise Level Material Risks

The GBRF has built on existing risk information and assessments to refine a consolidated list of enterprise level material risks. These are risks that may materially impact on the GBRF's ability to achieve its strategic outcomes. The following risks measures have been put in place to control or mitigate these risks. Oversight will be provided by the Risk and Compliance Manager.

The identified enterprise level material risks and controls are detailed below.

Enterprise Risk	Measures to Control Risk
1. Strategic outcomes not achieved due to a serious workplace incident resulting in severe consequences.	GBRF has adopted best-practice workplace health and safety policies and procedures where staff safety is of the highest priority with WHS training provided. Appropriate insurance is in place incorporating workers compensation and public liability cover. External contractors must provide details of workplace health and safety standards and details of insurance cover.
2. Strategic outcomes are not achieved due to funding being reduced or withdrawn.	GBRF maintains regular consultation, communication and reporting with the Department of the Environment and Energy and will adjust and communicate strategic outcomes in the event of funding reductions.
3. Strategic outcomes are not achieved due to GBRF not delivering against key objectives for each Component under the Agreement.	GBRF has in place clear governance and best practice processes along with an Investment Strategy and Annual Work Plan all of which receive regular review ensuring alignment with and tracking to Component objectives and timeframes as identified in the Agreement.
4. Strategic outcomes for the Reef Trust Partnership are not achieved due to ineffective governance.	GBRF has in place clear project oversight through robust governance arrangements of the Board, PMC, ISAC, and other relevant project committees and working groups.
5. Strategic outcomes are not achieved due to GBRF being unable to perform critical functions for more than two weeks e.g. natural disaster or infrastructure failure.	GBRF has in place a comprehensive Business Continuity and Disaster Recovery Plan which details response plans and staff responsibilities in the event of disaster or outage ensuring the GBRF can continue operation as soon as practically possible.
6. Strategic outcomes are not achieved due to failure by GBRF to meet stakeholder expectations.	GBRF engage with the various working groups, including the TOWG to ensure appropriate input and engagement across the various Components. GBRF also ensures engagement with other stakeholders through establishing and working with advisory bodies and key interest groups.
7. Strategic outcomes not achieved because additional funding not secured.	GBRF will develop and deploy a Collaborative Investment Strategy and develop a team to design and deliver collaboration and co-investment objectives.
8. Strategic outcomes not achieved due to misconduct by a delivery partner resulting in financial or economic loss and/or reputational damage.	When engaging partners, GBRF ensures peer reports and reference checks are obtained along with other due diligence checks. Contracts with partners and service providers have indemnity and liability clauses appropriate for the activity. There are also procedures in place to minimise the control or impact that any one partner may have on any project or activity.

Enterprise Risk	Measures to Control Risk
9. Failure to establish and maintain a GBRF culture that supports employees and the achievement of GBRF strategic objectives.	Ensure policies and frameworks for managing governance, IT, finance, and staff are in place to maintain workforce productivity and wellbeing whilst continuing to introduce cultural initiatives to ensure a positive and supportive working environment.
10. Capital loss of invested grant funds and co-contributions reducing the ability of the GBRF to achieve its strategic outcomes and meet its obligations under the RTP Agreement.	The Investment Committee has been appointed by the Board to oversee the investment policy, investment risk management and investment exposures over investment activities.  The investment policy reflects the risk appetite in setting counterparty / credit risk minimums.



## Component Level Risk Management

### Project Director

The Project Director for each Component takes the lead on identifying Component level risks and managing these with effective risk controls. Oversight will be provided by the Risk and Compliance Manager.

### Risk Management Approach for Components

As Components commence, a detailed risk assessment is undertaken to identify whether there are any material risks related to that Component. These assessments are complemented by a series of controls that are documented and actioned at Component level to mitigate and address the consequences of any identified risks.

Risk assessments and associated Action Plans are monitored by the Project Director and Risk and Compliance Manager to enable reporting to be provided to the PMO on a monthly and quarterly basis.

### Component Level Material Risks

The Project Directors assigned to the Reef Trust Partnership Components have undertaken a risk assessment to identify Component level material risks. These are risks that may materially impact on the Component's ability to achieve its deliverables.

The identified Component level material risks and controls are detailed below.

Component Risk	Measures to Control Risk
1. Outcomes not achieved due to lack of information, consensus and/or expert advice to prepare robust design.	GBRF ensures the program is backed by and aligned with the best available information and science with any critical knowledge gaps identified and addressed. Project oversight through robust governance arrangements of the Board, PMC, ISAC, and other relevant project committees and working groups.
2. Outcomes not achieved due to lack of suitable delivery partner capacity.	GBRF has in place robust procurement processes that identify appropriate partners incorporating pre-qualification requirements and due diligence. Active monitoring of deliverables and regular reporting in place with delivery partners ensuring objectives can be met and are on track. Control would be to profile funding to allow delivery partners to recruit, scale up capacity over reasonable time scales.
3. Outcomes not achieved due to changes in natural/socio-economic/regulatory environment.	GBRF maintains regular consultation, communication and reporting with the Department of the Environment and Energy, Queensland Government and GBRMPA along with close engagement with delivery partners and engaged communities ensuring GBRF is advised of any relevant changes that may impact on objectives.
4. Outcomes not achieved due to inability to demonstrate measurable change during project lifecycle.	GBRF is continually developing and implementing monitoring and evaluation frameworks, including modelling, throughout project lifecycles along with communication, engagement plans and expectation management. Appropriate communication is also maintained with the Department of the Environment and Energy and other relevant stakeholders.



# Appendix 1: Risk Management Policy

---

## 1. Background

Risk management is about understanding and managing the risk environment in which the Great Barrier Reef Foundation (GBRF) operates and taking measures, where necessary, to ensure that risks are contained to acceptable levels consistent with GBRF's risk appetite as outlined in the Risk Management Framework. This Policy sets out, at a high level, GBRF's policy on managing this process.

## 2. Purpose

This Policy is a statement of the overall approach to risk management for GBRF. The overriding purpose of this Policy is to ensure that:

- (a) appropriate systems and processes are in place to identify material risks that may impact on GBRF's business;
- (b) the financial or non-financial impact of risks is understood, and appropriate internal control systems are in place to limit GBRF's exposure to such risks;
- (c) appropriate responsibility is delegated to control the identified risks effectively; and
- (d) a core management capability is fostering an organisational culture that ensures effective business risk management.

This Policy is supported by the Risk Management Framework and is to be read in conjunction with GBRF's other policies and procedures, particularly the Fraud, Anti-Bribery and Anti-Corruption Policy, Whistleblowing Policy, and the terms of any employment or engagement arrangement entered into by any individual or entity with GBRF.

## 3. Risk Management Framework

GBRF will develop and implement an enterprise wide Risk Management Framework that is consistent with Australian / New Zealand Standard (AS/NZS ISO 31000:2018: Risk Management – Guidelines) and that GBRF considers is appropriate having regard to the nature and extent of GBRF's business and operations and the associated risk profile of that business and operations.

The Risk Management Framework will outline GBRF's approach to risk oversight and management and set out the methodologies adopted by GBRF for the ongoing:

- (a) identification, analysis and evaluation of risks and changes in those risks;
- (b) development and implementation of processes to monitor, treat and manage risks;
- (c) reporting of risks and mitigating controls; and
- (d) response to risks that materialise as adverse events

## 4. Responsibilities

### 4.1 The Board

The Board is responsible for defining the overall risk appetite of the GBRF, and satisfying itself annually, or more frequently as required, that management has developed and implemented an effective Risk Management Framework. Detailed work on this task is delegated to the Audit, Risk and Compliance Committee.

## 4.2 The Audit, Risk and Compliance Committee

The Audit, Risk and Compliance Committee is responsible for the implementation and management of the Policy and the Risk Management Framework. The Audit, Risk and Compliance Committee will:

- (a) review the suitability and effectiveness of the Risk Management Policy and Risk Management Framework annually or on another more frequent basis as requested by the Board;
- (b) receive and review reports quarterly concerning the appropriateness of the Risk Management Framework and approve or vary it as necessary;
- (c) review and make recommendations to the Board on GBRF's overall risk profile and risk appetite; and
- (d) assess the Risk Management Framework against the expectations of relevant regulators.

## 4.3 Risk and Compliance Manager

The Risk and Compliance Manager will:

- (a) provide quarterly risk reports to the Audit, Risk and Compliance Committee in accordance with the Risk Management Framework;
- (b) maintain a list of project specific risks in accordance with the Risk Management Framework;
- (c) conduct a monthly meeting with the Managing Director and Head of Operations to review GBRF risks; and
- (d) regularly review and report to the Audit, Risk and Compliance Committee on any actual and reported or observed failures to implement this Policy or the Risk Management Framework.

## 4.4 Management

Management is required to embed risk management processes into GBRF's daily practices to achieve the objectives of this Policy.

Management is expected to:

- (a) set a culture that encourages the management of risk in all aspects of the business and oversee the implementation of sound risk management practices throughout GBRF including under the terms of the Risk Management Framework;
- (b) identify, monitor and assess material risks affecting GBRF's business activities on an ongoing basis;
- (c) report to the Risk and Compliance Manager regarding GBRF's risk management activities and the status of material risks affecting GBRF's business activities; and
- (d) adhere to the Risk Management Framework in carrying out GBRF's business activities.

## 5. Supporting Documents

- GBRF Fraud, Anti-Bribery and Anti-Corruption Policy
- GBRF Whistleblowing Policy

## 6. Authorisation

Endorsed by Managing Director, Anna Marsden	18/09/2018
Endorsed by Audit, Risk and Compliance Committee	18/09/2018
Approved by Board	30/09/2018

## Appendix 2: Risk Assessment Template

Risk identification					
Risk Reference No					
Risk Description					
Risk Appetite					
Risk Owner					
Sources (what could cause the risk to exist?)					
Consequences (what are possible impacts if the risk materialises?)					
Inherent Risk Rating					
Likelihood rating	1 – Rare	2 – Unlikely	3 – Possible	4 – Likely	5 – Almost Certain
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Consequence rating	1 - Insignificant	2 - Minor	3 - Moderate	4 -Major	5 -Catastrophic
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Overall inherent risk rating					
Accept inherent risk?					
Current controls					
Control effectiveness rating	Weak	Moderate	Good	Excellent	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Residual Risk Rating					
Risk Treatment					
Proposed risk treatment			Responsibility	Timing	







# Purpose

---

The purpose of this Business Continuity and Disaster Recovery Plan (the Plan) is to prepare the Great Barrier Reef Foundation (GBRF) in the event of extended business outages caused by factors beyond its control (e.g. natural disasters, man-made events, technology outages), and to restore business activities to the widest extent possible in a minimum time frame. The GBRF will implement preventive measures whenever possible to minimise operational disruptions and to recover operations as rapidly as possible when an incident occurs.

## 1. Scope

The scope of this plan is limited to detailing the steps and actions required to be taken in the event of an outage encountered by GBRF. This is a business continuity plan, not a daily problem resolution procedures document.

## 2. Plan objectives

- Serves as a guide for the GBRF recovery team.
- References and points to the location of critical data.
- Provides procedures and resources needed to assist in recovery.
- Identifies vendors that must be notified in the event of a disaster.
- Assists in avoiding confusion experienced during a crisis by documenting, testing and reviewing recovery procedures.
- Identifies alternate sources for supplies, resources and locations.
- Documents storage, safeguarding and retrieval procedures for vital records.

## 3. Assumptions

- Key people will be available and contactable at the time of a disaster.
- This document and all vital records are stored in a secure off-site location and not only survive the disaster but are accessible immediately following the disaster.
- This plan consists of unique recovery procedures, critical resource information and procedures.

## 4. Disaster definition

Any loss of utility service (power, water), connectivity (system sites), or catastrophic event (weather, natural disaster, vandalism) that causes an interruption in the service provided by GBRF operations. This would also include similar events impacting GBRF funded projects and project delivery partners (e.g. cyclone threat, lost vessel at sea, fire threat to a land rehabilitation team).

The plan recommends measures to prevent extended service outages.

## 5. Emergency Management Team (EMT)

- Anna Marsden (Managing Director) – EMT Leader
- Theresa Fyffe (Executive Director, Projects and Partnerships)
- Kerri Ryan (Head of Operations)
- Damien Dennis (Risk and Compliance Manager)
- Amber Hawkins (Head of Corporate Affairs)

## 6. Team member responsibilities

- Each team member will designate an alternate.
- All members will keep both at home and at work an updated calling list of their work team members' work and mobile phone numbers.

## 7. Instructions for using the business continuity plan

### Invoking the plan

This plan becomes effective when a disaster occurs. Normal problem management procedures will initiate the plan and remain in effect until operations are resumed at the original location or a replacement location and control is returned to the appropriate functional management.

### Disaster declaration

The Managing Director is responsible for declaring a disaster and activating the EMT as outlined in this plan.

### Notification

Regardless of the disaster circumstances, or the identity of the person(s) first made aware of the disaster, the EMT must be activated immediately in the following cases:

- Systems used on a daily basis for the operation of GBRF are down or unable to be accessed by GBRF staff concurrently for two weeks.
- GBRF office location is unable to be accessed for a period of 24 hours due to an unforeseen event.
- In the case of an adverse or unforeseen event at one the GBRF funded project sites, the EMT will then decide what actions need to be taken considering that all funding recipients will have Business Continuity and Disaster Recovery Plans in place. The EMT will also decide, depending on the severity of the event, the chain of communications that will need to take place e.g. media statements, Board, government.

### External communications

The Corporate Affairs team is designated as the principal contact with the media (radio, television, social media, online and print), government agencies, and other external organisations following a formal disaster declaration.

### Data backup policy

The GBRF's Document Management System and email is cloud based with Microsoft Office 365 applications and backed up daily basis along with a further back up to Cloud Ally.

Other software used by the GBRF, including finance, payroll, fundraising, customer relationship management and board meeting solutions, have reliable backup solutions maintained by software vendors. When non-portal legacy systems are used, a back-up on an external hard drive is stored offsite at the Head of Operations' home.

### Emergency management procedures

IT support functions used by GBRF are 100% outsourced to external providers and as such reliance is on the provider to support the continuity of system availability in the event of an outage.

### Alternate locations – Staff work from home

- All staff are required to work from home if the building cannot be accessed. All staff can access Microsoft Office 365 via provided laptop or via their own internet connection and specially provided password to access GBRF files and emails.

### In the event of a natural disaster

In the event of a major catastrophe affecting GBRF premises or any GBRF funded projects, immediately notify the Managing Director.

#### Procedure

STEP	ACTION
1	Notify EMT of pending event, if time permits.
2	If the impending natural disaster can be tracked, begin notification to staff or any requirement to work from home.
3	<b>24 hours prior to event:</b> <ul style="list-style-type: none"> <li>• Create an image of the system and files.</li> <li>• Back up critical system elements.</li> <li>• Ensure backups of e-mail and files.</li> </ul>

### In the event of a fire

If fire or smoke is present in the facility, evaluate the situation, determine the severity, categorise the fire as major or minor, and take the appropriate action as defined in this section. Call 000 as soon as possible if the situation warrants it.

- Personnel are to attempt to extinguish minor fires (if safe to do so).
- In the event of a major fire, call 000 and immediately evacuate the area.
- In the event of any emergency situation, system security, site security and personal safety are the major concerns. If possible, the Head of Operations and Risk and Compliance Manager will remain present at the facility until the fire department or police have arrived.
- In the event of a major catastrophe affecting the facility, immediately notify the Managing Director.

#### Procedure

STEP	ACTION
1	Dial 000 to contact the Fire Department.
2	Immediately notify all other personnel in the facility of the situation and evacuate the area.
3	Alert the EMT. Note: During non-staffed hours, security personnel will notify the Head of Operations or Risk and Compliance Manager responsible for the location directly.
4	Notify Building Security. Local security personnel will establish security at the location and will not allow access to the site unless notified by the Head of Operations or Risk and Compliance Manager.
5	Contact appropriate vendor personnel to aid in the decision regarding the protection of equipment if time and circumstance permit.
6	All personnel evacuating the facilities will meet at their assigned outside location (assembly point) and follow instructions given by the designated authority. Under no circumstances may any personnel leave the designated assembly point without the consent of the supervisor.

## In the event of a flood or water damage

In the event of a flood or broken water pipe within any computing facilities, the guidelines and procedures in this section are to be followed.

### Procedure

STEP	ACTION
1	Assess the situation and determine if assistance is required. In the first instance contact building management (Cornerstone Properties 3034 0529). If outside assistance is needed dial 000 immediately.
2	Immediately notify all other personnel in the facility of the situation and be prepared to cease operations accordingly and leave the building.

## 8. Plan review and maintenance

This plan must be reviewed semi-annually and exercised on an annual basis. The test may be in the form of a walk-through, mock disaster, or component testing. Additionally, it is important to review the listing of personnel and phone numbers contained within the plan regularly.

The hard-copy version of the plan will be stored in a common location where it can be viewed by the EMT. Electronic versions will be available via a restricted access folder which can be viewed by the EMT.

## 9. BCP checklist

Response and recovery checklists are presented in the following two sections. The checklists should be used as “quick references” when implementing the plan or for training purposes.

INITIALS	TASK TO BE COMPLETED
	Do Emergency Services need to be contacted?
	Have EMT been notified?
	Are all staff accounted for?
	Have Building Management been informed?
	Do staff need to be evacuated if within working hours?
	Do staff need to be informed not to attend the building if out of hours? If yes, have all staff been notified?
	If building cannot be accessed have office phones been diverted to staff mobile numbers?
	Can all staff access systems remotely?
	Contact technology providers to advise of situation.
	Review insurance policies.
	Has timing of non-access to premises been ascertained?
	Can the premises be safely accessed? Do alternative premises need to be found?
	Will MD need to contact Board Chair/Government officials/Funders or Grantors?
	Will Communications need to make a statement - social media/website etc?



## 10. Notification of incident affecting the site

### On-duty personnel responsibilities

**During normal business hours:** Upon observation or notification of a potentially serious situation during working hours at the site, ensure that personnel on site have enacted standard emergency and evacuation procedures if appropriate and notify the EMT.

**Outside hours:** Personnel should contact a member of the EMT.

## 11. Provide status to EMT

Contact EMT and provide the following information:

- Location of disaster
- Type of disaster (e.g. fire, hurricane, flood)
- Summarise the damage (e.g. minimal, heavy, total destruction)
- Meeting location that is a safe distance from the disaster scene
- An estimated timeframe of when a damage assessment group can enter the facility (if possible)
- The EMT will contact staff and report that a disaster has taken place.

## 12. Decide course of action

Based on the information obtained, the EMT need to decide how to respond to the event: mobilise IT, repair/rebuild existing site with staff, or relocate to a new facility.

## 13. Inform team members of decision

If a disaster is not declared, the EMT will continue to address and manage the situation through its resolution and provide periodic status updates to staff.

If a disaster is declared, the EMT will notify IT Support.

**Declare a disaster** if the situation is not likely to be resolved within predefined time frames. The person who is authorised to declare a disaster must also have at least one backup person who is also authorised to declare a disaster in the event the primary person is unavailable.

## 14. Contact EMT: Decide whether to continue to business recovery phase

The EMT gathers information regarding the event, contacts Managing Director and provides detailed information on status.

Based on the information obtained, Managing Director decides whether to continue to the business recovery phase of this plan. If the situation does not warrant this action, continue to address the situation at the affected site.



## Business recovery phase

This section documents the steps necessary to activate business recovery plans to support full restoration of systems or functionality at the site, coordinate resources to reconstruct business operations at the temporary/permanent system location, and to deactivate recovery teams upon return to normal business operations.

1. Detail of system and facility operation requirements
2. Notify IT staff/Coordinate relocation to new facility
3. Secure funding for relocation
4. Notify staff of recovery startup
5. Operations recovered

Assuming all relevant operations have been recovered to an alternate site, and employees are in place to support operations, the company can declare that it is functioning in a normal manner at the location.

## 15. GBRF recovery teams

### Emergency management team (EMT)

#### Support activities

##### The EMT:

- Evaluates which recovery actions should be invoked and activates the recovery teams
- Evaluates damage assessment findings
- Sets restoration priority based on the damage assessment reports
- Provides Chair of the Board with ongoing status information
- Acts as a communication channel to functional teams
- Works with vendors and IT support to develop a rebuild/repair schedule

## 16. Emergency numbers

Name	Contact Name	Phone
Police		000
Ambulance		000
Fire Brigade		000
Building Management	Cornerstone Properties	3034 0529



# Appendix A: Forms

## Incident/disaster form

Upon notification of an incident/disaster situation the on-duty personnel will make the initial entries into this form. It will then be forwarded to the EMT, where it will be continually updated. This document will be the running log until the incident/disaster has ended and “normal business” has resumed.

### INCIDENT/DISASTER FORM

TIME AND DATE:	
TYPE OF EVENT:	
LOCATION:	
BUILDING ACCESS ISSUES:	
PROJECTED IMPACT TO OPERATIONS:	
RUNNING LOG (ongoing events):	



# Appendix B: Building evacuation information

EVACUATION DIAGRAM


11.2

**first 5 minutes**  
Experience makes all the difference.

Phone: 1300 321 120  
Website: first5minutes.com.au

**Issue Date: 14 December 2016**  
(valid for a period of 5 years)

**Diagrams used on this sign are NOT to scale.**



**R.A.C.E.**  
When an emergency occurs, the R.A.C.E. procedure offers a list of immediate, generic actions which are easily understood and appropriate for most circumstances. They are:

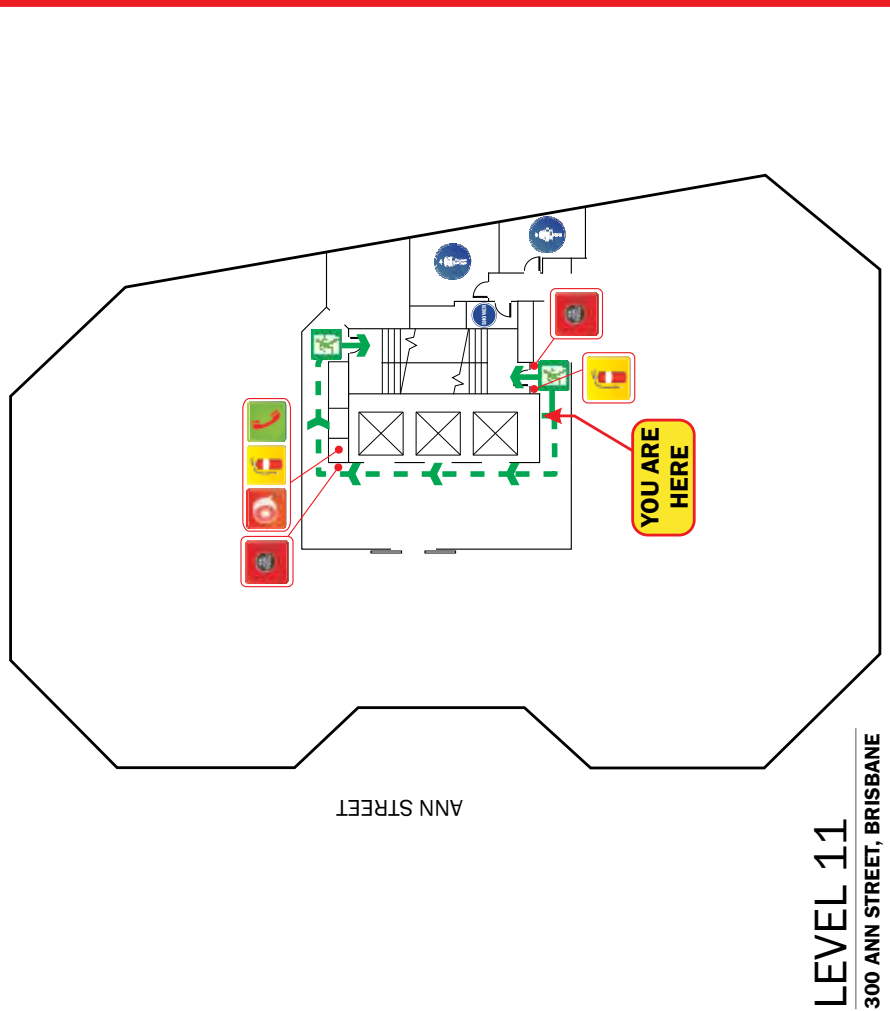
**R**EMOVE - If safe to do so, remove or relocate any persons in immediate danger.

**A**LERT - Notify appropriate personnel or contacting authority. This usually involves sounding the emergency bell and opening fire doors to clear.

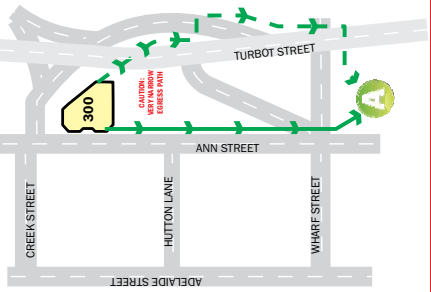
**C**ONTROL / **E**XTINGUISH - Close doors, use of walk to do so, wait with retreat.

**E**VACUATE - Remove all other persons from danger. Evacuate to the Assembly Area and remain there until advised otherwise by the Civil Warden.

**RESPONSE TO AN EMERGENCY**



LEVEL 11  
300 ANN STREET, BRISBANE



ASSEMBLY AREA

**STAGES OF EVACUATION**

Evacuation should be conducted in three distinct stages depending on the severity of the incident.





**STAGE 1 - REMOVAL OF PERSONS FROM THE IMMEDIATE DANGER AREA**  
Occupants are removed from the affected compartment into the next compartment, e.g. from a room into a corridor. Doors should be closed to confine smoke and fire in the affected compartment.

**STAGE 2 - REMOVAL TO A SAFE AREA**  
If the severity of smoke or heat warrants further evacuation, occupants and visitors should be moved to safe areas on the same level.

**STAGE 3 - COMPLETE EVACUATION OF THE FLOOR**  
Should the emergency necessitate evacuation of the affected floor, Wardens are to direct occupants to the assembly area via the emergency exits.

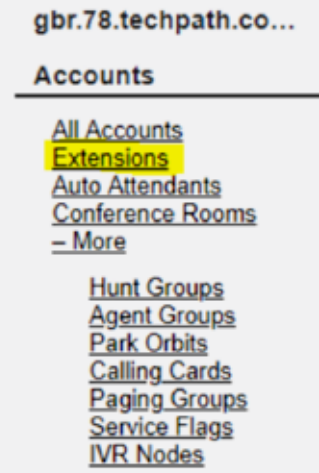
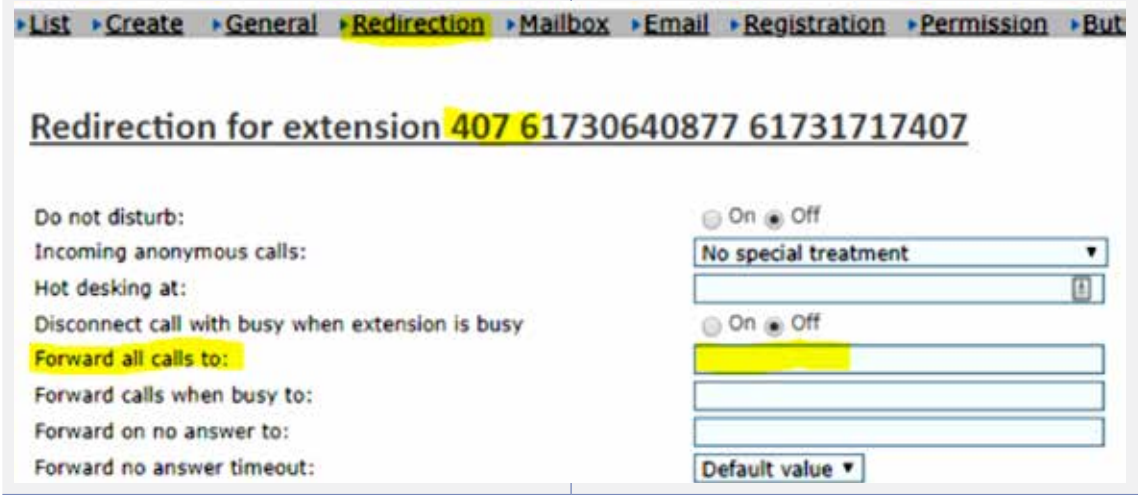


## Appendix C: Emergency Procedures

<p><b>IN AN EMERGENCY TELEPHONE:</b></p> <p><b>FIRE BRIGADE            000</b></p> <p><b>POLICE                    000</b></p> <p><b>AMBULANCE            000</b></p>	<p><b>WHEN YOU DIAL THE EMERGENCY NUMBER:</b></p> <p>Ask for the relevant service operator (Fire, Police or Ambulance) and pass on the following details:</p> <ul style="list-style-type: none"> <li>- The type of emergency;</li> <li>- Street name &amp; number and nearest cross street;</li> <li>- Suburb; and</li> <li>- Street Directory reference (if known)</li> </ul> <p>and any other information requested by the operator.</p>
<p><b>IN ALL CASES, ADVISE THE PROPERTY MANAGER</b></p>	
<p><b>EVACUATION PROCEDURES</b></p> <p><b>IF IN IMMEDIATE DANGER or on being instructed to evacuate:</b></p> <ol style="list-style-type: none"> <li>1. If safe to do so secure your office and evacuate the building via the nearest exit and proceed in an orderly manner to the assembly area.</li> </ol> <p style="text-align: center;"><b>DO NOT USE LIFTS</b></p> <ol style="list-style-type: none"> <li>2. Do not re-enter the building unless advised it is safe to do so by an authorised person.</li> </ol>	<p><b>KNOW YOUR EXITS</b></p> <div style="text-align: center;">  </div> <p><b>FOR YOUR SAFETY MAKE SURE YOU KNOW THE LOCATION OF THE NEAREST EMERGENCY EXIT</b></p>
<p><b>FIRE EXTINGUISHERS AND HOSE REELS</b></p> <p><b>IF SAFE TO DO SO :</b></p> <p><b>FIRE EXTINGUISHERS</b></p> <p>Select the correct extinguisher</p> <div style="display: flex; align-items: center;">  <ol style="list-style-type: none"> <li>1. Remove from bracket.</li> <li>2. Carry to scene of fire.</li> <li>3. Whilst clear of fire remove pin and test the fire extinguisher.</li> <li>4. Proceed to fire and initially from a distance of no closer than 2 metres direct the agent in a sweeping motion at the base of the fire.</li> </ol> </div> <p><b>FIRE HOSE REEL</b></p> <div style="display: flex; align-items: center;">  <ol style="list-style-type: none"> <li>1. Open valve (ensure that hose reel is turned off at nozzle).</li> <li>2. Run out hose towards scene of fire.</li> <li>3. Open nozzle and direct stream at base of fire.</li> </ol> </div> <p><b>NB. FIRE HOSE REELS ARE NOT TO BE USED ON FIRES WITH AN ELECTRICAL HAZARD</b></p>	<p><b>BOMB OR SUBSTANCE THREAT PROCEDURES</b></p> <ol style="list-style-type: none"> <li>1. Remain Calm..</li> <li>2. Record exact wording of threat.</li> <li>3. Keep the caller talking - try to obtain as much information as possible using the Threat Checklist.</li> <li>4. Report call to: <b>CHIEF WARDEN, YOUR MANAGEMENT and POLICE ON "000"</b>.</li> <li>5. Record details of caller's voice and background noise.</li> <li>6. Await instructions from authorised persons.</li> </ol> <div style="text-align: right; margin-top: 20px;"> <p><b>first 5 minutes</b> </p> <p><small>Experience makes all the difference. www.first5minutes.com.au</small></p> </div>

# Appendix D: Phone System Help Sheet

## TechPath Help Sheet

Issue	Resolution
How to divert incoming direct numbers to individual mobile phones	<ul style="list-style-type: none"><li>• Navigate to extensions</li><li>• Edit the required extension</li><li>• Navigate to “Redirection” tab</li><li>• Adjust the “Forward all calls” to the required destination</li></ul>  <p>The screenshot shows a web interface for 'gbr.78.techpath.co...'. Under the 'Accounts' section, there is a list of links: 'All Accounts', 'Extensions' (highlighted in yellow), 'Auto Attendants', 'Conference Rooms', and '- More'. Below this, there is a list of other account types: 'Hunt Groups', 'Agent Groups', 'Park Orbits', 'Calling Cards', 'Paging Groups', 'Service Flags', and 'IVR Nodes'.</p>
 <p>The screenshot shows a configuration page for 'Redirection for extension 407 61730640877 61731717407'. The breadcrumb trail is: List &gt; Create &gt; General &gt; Redirection &gt; Mailbox &gt; Email &gt; Registration &gt; Permission &gt; But. The page contains several settings:</p> <ul style="list-style-type: none"><li>Do not disturb: <input type="radio"/> On <input checked="" type="radio"/> Off</li><li>Incoming anonymous calls: No special treatment (dropdown menu)</li><li>Hot desking at: [input field]</li><li>Disconnect call with busy when extension is busy: <input type="radio"/> On <input checked="" type="radio"/> Off</li><li>Forward all calls to: [input field]</li><li>Forward calls when busy to: [input field]</li><li>Forward on no answer to: [input field]</li><li>Forward no answer timeout: Default value (dropdown menu)</li></ul>	

Issue	Resolution
<p>How to divert incoming reception calls to mobile</p>	<p><b>To turn on diversion:</b></p> <ul style="list-style-type: none"> <li>• In TechPath web portal</li> <li>• Click 'More' on left hand side</li> <li>• Click 'service flags'</li> <li>• Click '9998' for Manual</li> <li>• In the drop down for Current State select 'set'</li> <li>• Click Save</li> </ul> <ul style="list-style-type: none"> <li>• Click 'All Accounts' on left hand side</li> <li>• Click '300' for Inbound Calls</li> <li>• Within Night Service Number replace '8498' with the mobile number.</li> <li>• Click Save</li> </ul> <p><b>To cancel diversion:</b></p> <ul style="list-style-type: none"> <li>• In TechPath web portal</li> <li>• Click 'More' on left hand side</li> <li>• Click 'service flags'</li> <li>• Click '9998' for Manual</li> <li>• In the drop down for Current State select 'clear'</li> <li>• Click Save</li> </ul> <ul style="list-style-type: none"> <li>• Click 'All Accounts' on left hand side</li> <li>• Click '300' for Inbound Calls</li> <li>• Within Night Service Number replace mobile number with '8498'.</li> <li>• Click Save</li> </ul>
<p>To have phones open on a weekend/outside of business hours or change business hours</p>	<ul style="list-style-type: none"> <li>• In TechPath web portal</li> <li>• Click 'More' on left hand side</li> <li>• Click 'service flags'</li> <li>• Click '9999' for business hours</li> <li>• Amend hours as required: <ul style="list-style-type: none"> <li>– To open on a weekend copy and paste hours from a weekday to Saturday or Sunday</li> <li>– Or overtype existing times to adjust hours as required</li> <li>– Note that it is 24-hour setting</li> </ul> </li> <li>• Click save</li> <li>• Back on the Service Flags page make sure the status is clear.</li> </ul>