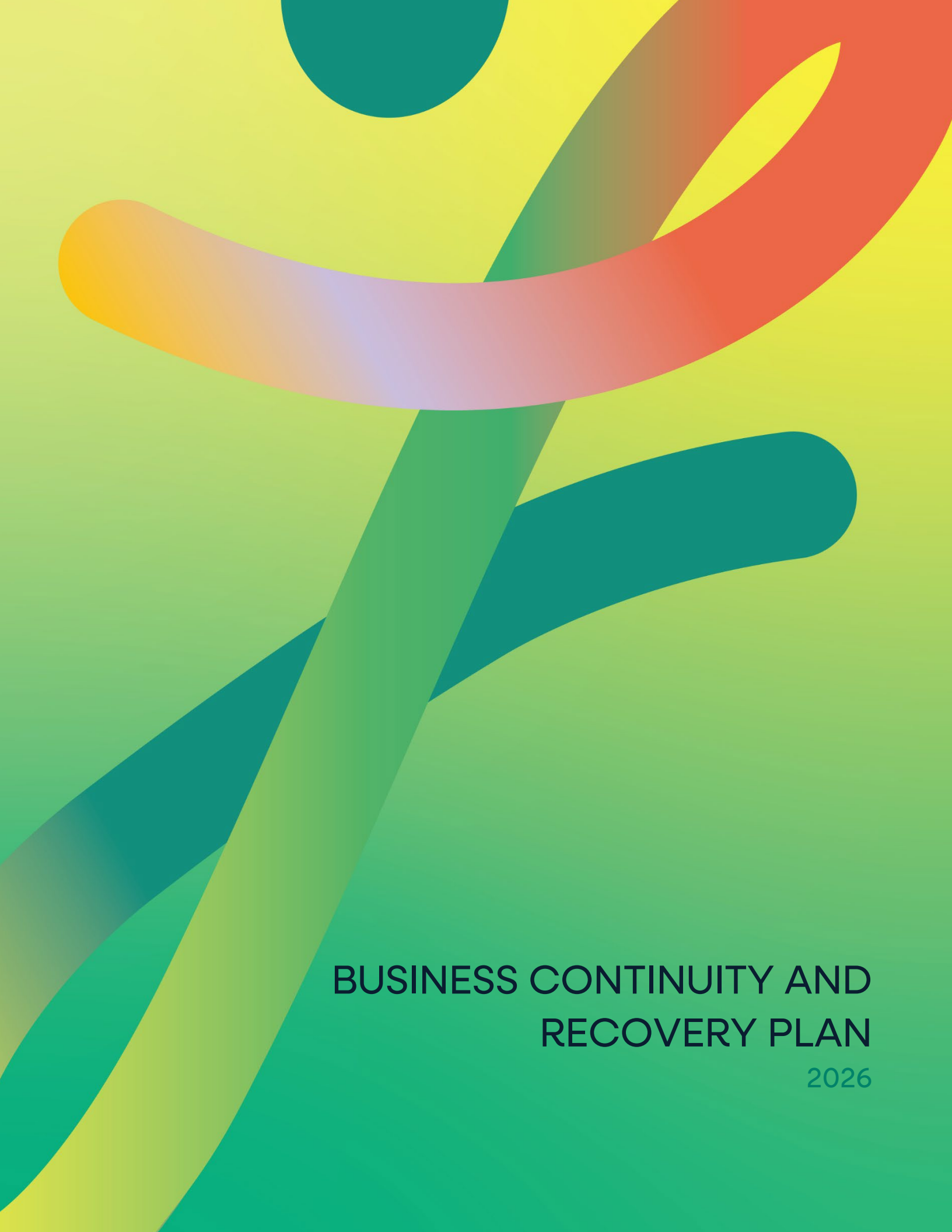




BUSINESS CONTINUITY AND RECOVERY PLAN

2026

Reference No	PLN-001	Business Continuity and Disaster Recovery Plan
--------------	---------	--

Current version number	1			
Review frequency	Annually	☒	Every two years	☐
	This plan will be reviewed at least every year, or earlier if required due to post incident review, organisational requirements or governance review.			
Approved by	Board	☐	CEO	☒
Date current version approved	2 April 2026			
Next review date	2 April 2027			
Applies to	The plan applies to employees, contractors, and volunteers engaged in delivering or supporting organisational functions.			

Plan context	
This plan relates to:	
Commonwealth and state legislation	Australian Commonwealth Acts - Privacy Act 1988 (Cth) - Corporations Act 2001 (Cth) Queensland Acts - Work Health and Safety Act 2011 (Qld) - Disaster Management Act 2003 (Qld) - Information Privacy Act 2009 (Qld) - Financial Accountability Act 2009 (Qld) NSW Acts - Work Health and Safety Act 2011 (NSW) - State Emergency and Rescue Management Act 1989 (NSW)
Regulatory requirements (Standards)	Strengthened Aged Care Quality Standards Standard 2 - The Organisation - Outcome 2.3 Accountability, quality system and policies and procedures - Outcome 2.5 Incident Management - Outcome 2.8 Workforce Planning - Outcome 2.10 Emergency and Disaster Management Human Services Quality Standards Standard 1 – Governance and Management Standard 2 – Service Access Standard 4 – Safety, wellbeing and Rights NDIS Practice Standards and Quality Indicators Core Module – Governance and Operational Management - Outcome 2.6 Incident Management - Outcome 2.8 Continuity of Supports - Outcome 2.9 Emergency and Disaster Management National Safety and Quality Mental Health Standards for Community Managed Organisations

Plan context	
This plan relates to:	
	Standard 1 – Practice Governance Safety and quality systems Safe environment for delivery of care Standard 3 – Model of Care Communicating for safety
Best practice standards	AS/NZS5050 Business continuity
Organisational policies	• Corporate Governance Policy • Risk Management Framework • Code of Conduct Policy • Privacy and Confidentiality Policy • Media and Communications Policy • Cyber Incident Response Plan • Information Security/ICT Policy • Quality Management Framework
Forms, templates and other organisational documents	• Program manuals • Emergency evacuation plans

Table of Contents

1. Introduction	6
1.1 Purpose.....	6
1.2 Scope and Applicability	6
1.3 Objectives	6
1.4 Statement.....	6
2. Governance and Responsibilities	7
2.1 Business Continuity Governance Framework	7
2.2 Roles and Responsibilities.....	7
2.4 Key External Stakeholders	8
3. Risk and Business Impact Analysis	8
3.1 Overview of Risk Context	8
3.2 Critical Business Functions.....	9
3.3 Dependencies	9
3.4 Impact Analysis.....	10
3.5 Priority Recovery Sequence	11
3.6 Review and Validation	11
4. Prevention and Preparedness	12
4.1 Risk Mitigation and Preventive Controls.....	12
4.2 Resource and Equipment Readiness	12
4.3 Staff Capability and Succession Planning	13
4.4 Awareness and Communication	13
4.5 Business Continuity Planning for Partnered and Funded Services.....	13
4.6 Review and Continuous Improvement.....	13
5. Incident Response and Activation.....	14
5.1 Activation Criteria and Decision Authority	14
5.2 Notification and Escalation Process	14
5.3 Roles of the Incident Management Team	15
5.4 Initial Response Steps	15
5.5 Communication Framework.....	15
5.6 Documentation and Record-Keeping	16
6. Critical Incident Management	16
6.1 Purpose.....	16
6.2 Definition of a Critical Incident	16
6.3 Prevention and Early Identification	17

6.4 Reporting and Escalation Process	17
6.5 Critical Incident Response Roles	17
6.6 Communication and Confidentiality	17
6.7 Investigation and Review	18
6.8 Wellbeing and Recovery Support	18
6.9 Documentation and Record Keeping	18
6.10 Integration with Business Continuity	18
7. Emergency management	18
7.1 Purpose	18
7.2 Scope	18
7.3 Types of Emergencies	18
7.4 Emergency Procedures	19
7.5 Training and Drills	19
7.6 Specific Emergency Procedures	19
8. Business Continuity Procedures	20
8.1 Continuity of Critical Client Services	20
8.2 Alternative Service Delivery Models	21
8.3 Workforce Redeployment and Rostering	21
8.4 Manual Workarounds and Paper-Based Systems	21
8.5 Coordination with Partners and Funding Bodies	21
8.6 Client Safety, Wellbeing, and Dignity Provisions	22
8.7 Critical Supplier and Subcontractor Continuity	22
9. ICT Recovery Procedures	22
9.1 Objectives	22
9.2 Systems and Application Inventory	22
9.3 Backup and Restoration Procedures	23
9.4 Network and Infrastructure Recovery	23
9.5 Cyber Incident Response	23
9.6 Validation and System Testing	23
9.7 Communication and User Access Restoration	23
9.8 Sign-Off and Resumption of Standard ICT Operations	23
9.9 Integration with Business Continuity	24
10. Return to Normal Operations	24
10.1 Recovery Handover Process	24
10.2 Verification of Business and Service Operations	24

10.3 Post-Incident Review and Lessons Learned	24
10.4 Corrective Actions and Continuous Improvement	25
10.5 Wellbeing and Support for Staff and Clients Post-Incident	25
10.6 Formal Closure	25
11. Testing, Training, and Maintenance.....	25
11.1 Testing Program	25
11.2 Roles in Testing	26
11.3 Staff Training and Awareness	26
11.4 Plan Review and Update Cycle	26
Appendices	27
Appendix 1 – Implementation/Activation Checklist.....	27
Appendix 2 – Communication templates	28
Appendix 3 – Continuous Improvement/Follow Up	34
Appendix 4 – Monitoring Checklist	35
Appendix 5 – Exiting/Recovery Checklist	36
Key Contacts.....	37

1. Introduction

1.1 Purpose

The purpose of this plan is to ensure Footprints can continue to deliver essential services and meet its obligations to clients, staff, and stakeholders during and following a disruptive event.

This plan integrates business continuity, disaster recovery, serious incident and emergency management functions to provide a coordinated organisational response that prioritises client safety, service continuity, and timely restoration of systems and operations.

The plan supports the organisation's mission to provide responsive, person-led services that create pathways to independence and wellbeing even in the face of emergencies or significant operational disruptions.

1.2 Scope and Applicability

This plan applies to all Footprints operations, programs, and service locations across Queensland and New South Wales. It covers:

- Client services - including aged care, disability, mental health, homelessness, and related community support programs.
- Corporate and shared services - such as governance, Information and Communication Technology, finance, Human Resources, communications, facilities, and logistics.
- Technology and data systems - required for service delivery, client record management, and regulatory reporting.

Type and potential length of disruption will determine which parts of this continuity and response plan are to be activated.

Not all service locations are likely to be affected simultaneously due to their distribution across Queensland and New South Wales.

1.3 Objectives

The objectives of this plan are to:

- Safeguard the wellbeing, dignity, and safety of clients and staff.
- Ensure critical services continue, or are restored, within acceptable timeframes.
- Minimise operational, financial, and reputational impacts.
- Maintain compliance with regulatory and contractual obligations.
- Provide clear guidance for leadership and staff during an emergency.
- Support the timely recovery of ICT systems and infrastructure.
- Promote organisational resilience through preparedness, training, and continual improvement.

1.4 Statement

Footprints is committed to implementing and maintaining a proactive and robust approach to business continuity and recovery as an integral component of its governance and risk management framework. The organisation acknowledges its duty of care and its compliance

obligations under relevant standards and all relevant legislation to ensure the continuity of safe, effective, and high-quality services.

Business continuity and recovery planning form a critical element of Footprints' organisational resilience. These functions are overseen by the Executive Management Team and are subject to regular review to ensure ongoing effectiveness, alignment with regulatory requirements, and continuous improvement.

2. Governance and Responsibilities

2.1 Business Continuity Governance Framework

Footprints apply a governance-led approach to continuity and recovery, ensuring that oversight, responsibility, and decision-making are clearly defined.

The CEO provides strategic direction and approves all continuity and recovery activities, while operational implementation is coordinated through the Executive Management Team.

2.2 Roles and Responsibilities

Chief Executive Officer (CEO)

- Provides overall leadership and authorisation for plan activation. [Refer Appendix 1](#) for activation checklist. Also refer document CHK-001 Implementation/Activation Checklist.
- Approves strategic recovery decisions and resource allocation.
- Ensures compliance with regulatory and contractual obligations.

Executive Management Team (EMT)

- Oversees planning, preparedness and response coordination
- Review and approve continuity and recovery procedures
- Ensures business areas maintain up-to-date continuity subplans.
- Supports communication and coordination across all programs.
- Has standing agenda item every six months for business continuity readiness and updates.
- Ad hoc meetings during any major incident or recovery phase.

General Manager, Compliance and Reporting (Continuity Coordinator)

- Coordinates the development, maintenance, and testing of this plan.
- Ensures alignment between business continuity, risk management, and compliance frameworks.
- Leads post-incident reviews and continuous improvement activities.

Technology and System Lead

- Manages ICT disaster recovery planning, implementation, and testing.
- Ensures secure data backup, system redundancy, and rapid restoration of ICT infrastructure.
- Leads response to cyber incidents and works with the Compliance and Reporting team on data breach management.

Program Leads/Managers

- Maintain up-to-date continuity procedures (sub plans) for their respective programs and regions.
- Identify critical functions and dependencies.
- Ensure staff are aware of their responsibilities during disruptions.
- Report impacts and recovery status to the Executive Management Team.

Communications Officer / Media Lead

- Coordinates internal and external communications during a disruption.
- Ensures accurate, timely, and consistent messaging to staff, clients, families, and external agencies.
- Manages media engagement in consultation with the CEO.

All Employees and Volunteers

- Participate in training and awareness activities.
- Follow instructions during activation of this plan.
- Report incidents or risks that may impact service continuity.
- Reviewing outcomes and implementing lessons learned post-incident.

2.4 Key External Stakeholders

- Aged Care Quality and Safety Commission
- NDIS Quality and Safeguards Commission
- Funding and Partner Organisations
- Emergency Services (Police, Fire, Ambulance, SES)
- Critical Suppliers and Contractors
- Clients, families and carers

3. Risk and Business Impact Analysis

3.1 Overview of Risk Context

Footprints operates across diverse service environments supporting people who are aged, living with disability, experiencing mental health challenges, or at risk of or experiencing homelessness.

Given this broad client base, continuity of operations is essential to protect client wellbeing, maintain regulatory compliance, and preserve community trust.

Risks to business continuity may arise from:

- Environmental and natural disasters (flood, fire, storm, heatwave)
- Infrastructure failure (power, water, transport, communications)
- ICT or cyber incidents (data breach, ransomware, system failure)
- Workforce disruption (illness, pandemic, industrial action, workforce shortage)
- Loss of premises or facilities
- Supplier or contractor failure
- Public health emergencies
- Financial or reputational crisis

The organisation's approach to business continuity integrates with its Risk Management Framework, ensuring identified risks are assessed, mitigated, and reviewed on an ongoing basis.

3.2 Critical Business Functions

Critical business functions are those activities essential to safeguard client safety, meet legal or contractual obligations, and maintain organisational viability. To guide recovery activities, each critical function has established Recovery Time Objectives (RTO) — the maximum acceptable time to restore a function. These targets inform ICT backup schedules, staffing rosters, and escalation protocols. (Table 1).

Table 1: Critical business functions, impact and RTO

Service Area	Critical Function	Description / Impact if Interrupted	RTO
Aged Care Services	Client personal care and support	Essential to maintain client safety, hygiene, and wellbeing in home and community settings.	24 hours
Disability Services	Direct support and coordination of participant plans	Ensures continuity of funded supports, communication with participants, and delivery of essential personal and therapeutic care.	24 hours
Mental Health Services	Outreach, case management, and clinical care	Critical for client safety and mental health stability; disruption may lead to harm or crisis situations.	24 hours
Homelessness Services	Emergency accommodation and outreach support	Directly impacts client safety and access to shelter and basic needs.	24 hours
Corporate and ICT Services	Payroll, rostering, client record systems, and communication tools	Enables all other service areas to operate; essential for coordination, safety monitoring, and compliance.	48 hours
Finance	Financial transactions	Enables ability to process payments, manage revenue, and meet financial obligations.	48 hours
Governance and Risk / Communications	Regulatory reporting, incident escalation, stakeholder communication	Required to maintain compliance with regulatory bodies and transparent communication during crises.	48 hours

3.3 Dependencies

Each critical function depends on people, systems, suppliers, and infrastructure. Dependencies are reviewed regularly. (Table 2).

Table 2: Examples of dependency categories

Dependency Category	Examples
People	Qualified support workers, clinical staff, case managers, and key management personnel.
ICT Systems	AlayaCare, Microsoft 365, Action HRM, ionMY, ProSpend, SAP, HR/Payroll systems, and secure file storage.

Facilities and Assets	Offices, vehicles, mobile devices, computers including portable devices, and secure storage for client records.
Suppliers and Contractors	ICT providers, telecommunications, PPE suppliers, clinical consumables, food and transport providers.
Information and Data	Client care plans, risk assessments, and communication records required to continue services.

Where dependencies are external (e.g. internet service provider or building landlord), alternate suppliers or contingency agreements are identified and documented in program continuity subplans.

3.4 Impact Analysis

An interruption to critical functions may result in:

- **Client safety risk:** harm, neglect, or deterioration in health or wellbeing.
- **Regulatory non-compliance:** breaches of Aged Care Quality Standards, NDIS Practice Standards, Mental Health Standards or contractual obligations.
- **Reputational damage:** loss of trust from clients, funders, and community partners.
- **Financial impact:** loss of funding, increased recovery costs, or delayed claims.
- **Service delivery disruption:** delays in assessments, missed care visits, or inability to access systems.
- **Staff impact:** loss of productivity, stress, or inability to deliver care effectively.

Each impact is rated in accordance with Footprints' Risk Matrix, ensuring recovery priorities align with the highest client and organisational risks. Likelihood ratings are combined with impact ratings to calculate overall risk scores. (Table 3).

Risk Impact Matrix – Critical Function Impact Analysis

Table 3: Risk impact matrix

	Insignificant	Minor	Moderate	Major	Critical
Client safety risk	No injury or deterioration. Near miss only.	Minor first aid injury or temporary discomfort; no ongoing harm.	Temporary deterioration in health or wellbeing; client support required.	Significant harm or neglect requiring medical attention or external investigation.	Fatality or permanent harm; systemic client safety failure.
Regulatory non-compliance	Minor non-conformance rectified immediately.	Low-level compliance issue; reported and resolved.	Noticeable breach requiring corrective action and reporting.	Major breach; formal investigation or sanction by regulator.	Critical breach; loss of accreditation, registration, or funding.
Reputational damage	No noticeable impact; managed internally.	Minor concern raised; no media or	Localised reputation damage; complaints	Regional or sector reputation impact; loss	Widespread reputation loss; long-term

		funder involvement.	from clients/funders.	of partner confidence.	community distrust.
Financial impact	Negligible cost (<\$5K). No funding risk.	Small financial impact (\$5K–\$20K).	Moderate loss (\$20K–\$100K) or temporary funding delay.	Major loss (\$100K–\$500K); potential loss of a funding stream.	Critical loss (>\$500K); major funding withdrawal or insolvency risk.
Service delivery disruption	Minor delay (<1 day); no client impact.	Short-term disruption (1–2 days); managed with rescheduling.	Disruption to multiple programs for several days.	Extended disruption (1–2 weeks) affecting multiple sites or programs.	Complete service shutdown (>2 weeks) or loss of critical systems.
Staff impact	Minimal stress; no disruption to roles.	Moderate workload stress; short-term reduction in efficiency.	Sustained stress, low morale, or short-term absenteeism.	High stress, burnout, or workforce instability.	Severe psychological impact; mass resignations or inability to operate safely.

This matrix should be applied when:

- Conducting risk assessments for critical functions.
- Prioritising continuity strategies (e.g., alternate sites, manual workarounds, backup systems).
- Reviewing incident severity and determining escalation pathways.
- Monitoring residual risk following mitigation or recovery actions.

3.5 Priority Recovery Sequence

Recovery efforts are prioritised based on impact severity and dependency. The following order of restoration is recommended:

1. Client safety and care functions
2. Communication systems (phones, email, emergency alerts)
3. Client management systems and records
4. Workforce systems (rostering, payroll, HR)
5. Finance and reporting functions
6. Administrative and non-essential services

3.6 Review and Validation

The Business Impact Analysis is reviewed annually by the Executive Management Team and whenever:

- A new service, program, or site is established.

- Major organisational or ICT changes occur.
- A disruption highlights new vulnerabilities.

4. Prevention and Preparedness

4.1 Risk Mitigation and Preventive Controls

Footprints maintains a proactive approach to minimise the likelihood and impact of disruptions across all service areas. Key risk mitigation measures include:

Environmental and Facility Controls

- Regular maintenance and safety audits of all facilities, vehicles, and equipment.
- Emergency exits, fire detection, suppression systems, and evacuation plan in compliance with WHS legislation.
- Flood, storm, and bushfire preparedness procedures for all locations.

ICT and Data Security

- Daily automated backups of all critical systems stored offsite and/or in secure cloud environments.
- Redundancy for critical ICT infrastructure to minimise downtime.
- Cybersecurity controls including antivirus software, firewalls, multi-factor authentication, and staff awareness training.

Workforce Preparedness

- Succession planning and cross-training of staff to maintain continuity of essential services.
- Clear escalation pathways and delegation of authority during emergencies.
- Rostering contingency plans to cover staff absences due to illness, industrial action, or other disruptions.

Supply Chain Resilience

- Identification of critical suppliers and alternate providers for essential goods and services (transport, PPE).
- Regular communication with suppliers to ensure service continuity in emergencies.

Regulatory and Compliance Controls

- Compliance with Strengthened Aged Care Quality Standards, NDIS Practice Standards, Human Services Quality Standards, Mental Health Standards and relevant legislation.
- Regular internal audits and monitoring to ensure all continuity and safety requirements are maintained.

4.2 Resource and Equipment Readiness

Footprints maintains resources required for uninterrupted service delivery:

Alternate Locations

- Identified backup facilities for essential services where primary sites are compromised.
- Agreements with partner organisations to support temporary relocation of programs and staff.

Critical Equipment and Supplies

- Emergency kits including first aid, PPE, and essential medications.
- Portable ICT devices, power backups, and communication equipment for staff and mobile service delivery.

Transportation

- Contingency plans for staff and client transportation, including vehicles, and supplier agreements.

4.3 Staff Capability and Succession Planning

To ensure resilience, staff preparedness is reinforced through:

Training Programs

- Annual induction and refresher training on business continuity, disaster response, and incident management.
- Role-specific drills, including clinical, administrative, and ICT-focused scenarios.

Succession and Delegation

- Identification of key personnel for critical functions with clearly defined alternate staff.
- Documentation of role responsibilities to enable rapid handover in case of staff absence.

Volunteer Preparedness

- Volunteers involved in service delivery receive orientation on emergency procedures and reporting channels.

4.4 Awareness and Communication

Staff Awareness

- All staff receive accessible guidance on their responsibilities in an emergency, including escalation pathways and reporting.
- Internal communication channels maintained and tested regularly (email, phone, SMS alerts).

Client and Stakeholder Communication

- Pre-prepared communication templates for clients, families, regulators, and partner/funding organisations. [Refer Appendix 2.](#)
- Strategies for maintaining engagement and support for clients during service interruptions.

4.5 Business Continuity Planning for Partnered and Funded Services

Footprints collaborate with funding bodies, partner organisations, and suppliers to:

- Align continuity plans across joint services.
- Ensure obligations under contracts and funding agreements are maintained during disruptions.
- Share critical information and coordinate service delivery in emergencies.

4.6 Review and Continuous Improvement

Business continuity procedures are tested annually or following a major incident. Lessons learned from incidents, audits, and exercises are incorporated into:

- Region level contingency sub plans
- Program level contingency sub plans
- Staff training programs
- Updated procedures
- Communication protocols

Continuous improvement ensures resources, staff readiness, and contingency measures evolve with client needs, regulatory changes, and organisational growth.

5. Incident Response and Activation

5.1 Activation Criteria and Decision Authority

The Footprints Community BCRP may be activated when:

- A disruption significantly impacts client services (e.g., aged care support, NDIS supports, mental health outreach, homelessness programs).
- ICT systems or data are compromised or unavailable, threatening operational continuity.
- Facilities, transport, or essential infrastructure are unavailable or unsafe.
- Regulatory, contractual, or legislative obligations cannot be met under normal operations.
- Public health emergencies or environmental disasters affect service delivery.

Decision to activate the plan rests with the Chief Executive Officer (CEO), or Delegate from Executive Management Team (EMT) in absence of the CEO.

Table 4: Stages of activation

Stages of Activation	Definition
Lean forward	An operational state prior to 'Stand Up' characterised by a heightened level of situational awareness of an incident (either current or impending) and a state of operational readiness. Resources are on stand-by; prepare but not activated.
Stand up	The operational state following 'Lean forward' whereby resources are mobilised, personnel are activated, and operational activities commenced.
Stand down	Transition from responding to an event back to normal core business and/or recovery operations. There is no longer a requirement to respond to the event and the threat is no longer present.

5.2 Notification and Escalation Process

- Staff who identify an incident must report it immediately through the incident reporting system or to their manager.
- The Executive Management Team assesses the severity
- Escalation occurs based on predefined thresholds (e.g., client safety risk, regulatory breach, system downtime).

Notification hierarchy example:

1. Program Lead
2. Regional Managers
3. Executive Management Team
4. CEO
5. Board
6. External stakeholders as required (regulators, funders, emergency services)

5.3 Roles of the Incident Management Team

Upon activation, the Incident Management Team (IMT) coordinates response activities:

Table 5: Role responsibilities within IMT

Role	Responsibilities
CEO / EMT Lead	Strategic oversight, authorisation of plan activation, media liaison, resource allocation.
Executive Management Team	Operational coordination, monitoring recovery actions, liaising with all service areas, escalate actions to restore services if required, maintain an incident log noting all actions taken. Complete incident analysis report when incident has been stood down.
Regional Managers	Implement service-level continuity procedures, manage staff, ensure client safety, report status.
Technology and System Lead	Restore critical systems, data, and communications infrastructure.
Communications Officer	Manage internal and external communications, prepare messaging for clients, families, regulators, and media.
Facilities / Logistics Coordinator	Ensure availability of alternate sites, vehicles, and resources.
Safety and Wellbeing Lead	Monitor staff and client wellbeing, arrange psychological support if required.
All staff	Follow the direction given by leads. All staff may be required to assist in activities that are not normally part of their duties.

5.4 Initial Response Steps

Upon incident detection:

1. Ensure immediate safety of staff, clients, and visitors.
2. Assess impact on services, systems, and critical functions.
3. Activate BCR Plan if thresholds are met.
4. Mobilise Incident Management Team and assign responsibilities.
5. Implement temporary workarounds to maintain critical service delivery.
6. Document all actions and communications for accountability and regulatory reporting.

5.5 Communication Framework

Internal Communication:

- Staff and volunteers are updated on incident status, safety instructions, and role assignments.
- SMS alerts, and secure email channels are used where appropriate.

External Communication:

- Clients and families are informed about service impacts, alternative arrangements, and safety instructions.
- Regulators (Aged Care Quality and Safety Commission, NDIS Commission) are notified where required.
- Partner organisations and funding bodies are advised of disruptions impacting joint services.
- Media communications are coordinated centrally by the CEO and Communications Officer.

Templates

- Pre-prepared communication templates for staff, clients, families, regulators, and media ensure timely and consistent messaging.

5.6 Documentation and Record-Keeping

All incidents and response actions are documented in the Incident Management System. Records include:

- Incident description and timeline
- Decisions and authorisations
- Communications issued
- Actions taken for mitigation and recovery
- Resource allocation and staff assignments

Documentation supports post-incident review, compliance audits, and continuous improvement.

6. Critical Incident Management

6.1 Purpose

The Critical Incident Management section outlines Footprints coordinated approach to preventing, responding to, and recovering from critical incidents that may impact the safety, wellbeing, or dignity of clients, staff, or the wider community.

This section compliments the broader Business Continuity and Recovery Plan (BCRP) by focusing on incidents involving serious harm, high-risk events, or situations requiring immediate escalation and external reporting.

6.2 Definition of a Critical Incident

A critical incident is any actual or alleged event that:

- Causes or poses serious harm to a client, staff member, or volunteer.
- Involves abuse, neglect, violence, or exploitation.
- Threatens the health, safety, or security of clients, staff, or the public.
- Results in a significant service disruption or regulatory breach.
- Attracts media attention or impacts organisational reputation.
- Triggers mandatory reporting under applicable legislation.

6.3 Prevention and Early Identification

Preventive measures include:

- Staff training in recognising and reporting early warning signs of abuse, neglect, or risk escalation.
- Risk assessments for all clients and programs.
- Safe environments and adherence to WHS and safeguarding policies.
- Ongoing supervision and debriefing for frontline workers.

6.4 Reporting and Escalation Process

All staff and volunteers must report critical incidents immediately to their manager and/or through the incident management system.

Escalation Pathway:

1. Staff/Volunteer → Notify Manager and/or record in Incident System.
2. Manager → Escalate to Executive Management Team (EMT).
3. EMT → Notify CEO and, if applicable, activate BCRP.
4. CEO → Report to Board, Regulators and Funders as required.

Mandatory reporting timeframes are observed in accordance with:

- NDIS (Incident Management and Reportable Incidents) Rules 2018
- Aged Care Quality and Safety Commission Act 2018
- Work Health and Safety Act 2011 (Qld)
- Mental Health Act 2016 (Qld)

6.5 Critical Incident Response Roles

Table 6: Role responsibilities for critical response

Role	Responsibilities
CEO / Delegate	Authorises escalation, liaises with regulators and media, allocates resources.
Executive Management Team	Coordinates response, ensures safety, and oversees investigation.
Regional Manager	Secures site, ensures client/staff safety, gathers evidence, and documents details.
Communications Officer	Manages internal and external communication, ensuring confidentiality.
Safety and Wellbeing Lead	Provides immediate and follow-up psychological support.
Compliance and Reporting Manager	Ensures all incidents are recorded, reported, and reviewed in line with policy.

6.6 Communication and Confidentiality

All communications must be accurate, timely, and respectful. Client information is shared strictly on a need-to-know basis and in accordance with privacy legislation. Media engagement is approved only by the CEO or delegate.

6.7 Investigation and Review

Each critical incident triggers a formal review to:

- Identify root causes and contributing factors.
- Assess adequacy of response actions.
- Determine corrective and preventive measures.
- Ensure regulatory and contractual compliance.

Findings are reported to the EMT and Board and integrated into the continuous improvement cycle [Refer Appendix 3](#). Also refer document CHK-002 Continuous Improvement/Follow Up Checklist

6.8 Wellbeing and Recovery Support

Footprints prioritise the wellbeing of all persons affected by a critical incident by:

- Providing immediate psychological first aid and follow-up counselling.
- Facilitating access to Employee Assistance Programs (EAP) for staff.
- Implementing tailored support for clients impacted by trauma or disruption.

6.9 Documentation and Record Keeping

All reports, communications, and corrective actions must be recorded in the Incident Management System and stored securely in accordance with privacy and audit requirements.

6.10 Integration with Business Continuity

Critical incident management processes are directly linked to the BCRP to ensure:

- Rapid activation of continuity measures for impacted services.
- Alignment of regulatory reporting and recovery activities.
- Shared learning and improvement across all programs.

Individual program manuals should include critical incident management relevant to services delivered aligned to their continuity sub plans.

7. Emergency management

7.1 Purpose

The Emergency Management component of this plan ensures that Footprints can effectively prepare for, respond to, and recover from emergencies that may impact clients, staff, or service operations.

7.2 Scope

Applies to all Footprints sites, vehicles, outreach operations, and community settings across aged care, disability, mental health, and homelessness programs.

7.3 Types of Emergencies

- Fire, flood, or severe weather
- Gas leak, chemical spill, or utility failure
- Medical emergency or infectious disease outbreak

- Threats to personal safety or security
- Vehicle accidents or community safety events

7.4 Emergency Procedures

1. **Immediate Safety:** Evacuate, shelter, or isolate as directed by emergency services.
2. **Notification:** Dial 000 and notify Manager or On-Call Lead.
3. **Evacuation and Assembly:** Follow site-specific emergency diagrams and procedures.
4. **Client Care:** Support clients to evacuate safely, with attention to mobility or cognitive needs.
5. **Communication:** Use SMS alerts or phone cascades to inform staff and emergency contacts.
6. **Liaison with Emergency Services:** Site lead coordinates with Police, Fire, or Ambulance.
7. **Incident Logging:** Record actions in the Incident Management System.
8. **Recovery:** Activate BCRP if service operations are disrupted.

7.5 Training and Drills

Emergency drills are conducted at least annually at each site and reviewed as part of the BCRP testing program (Section 11).

7.6 Specific Emergency Procedures

Footprints maintains detailed, site-specific emergency procedures to ensure the safety of clients, staff, volunteers, and visitors during any emergency or hazardous event. These procedures are part of the organisation's site-specific Emergency Evacuation Plans and are displayed and accessible at each service location, and available in the Action HRM document store.

They provide step-by-step instructions for managing a range of foreseeable events, including but not limited to:

- **Fire or smoke** – activation of alarms, evacuation procedures, and use of firefighting equipment.
- **Flood or severe weather** – relocation to safe areas, communication with emergency services, and activation of the BCR Plan if required.
- **Medical emergency** – provision of first aid, calling emergency services, and incident documentation.
- **Bomb threat or suspicious package** – notification of Police, isolation of the area, evacuation, and communication management.
- **Gas leak or chemical spill** – containment, isolation, ventilation, and emergency services engagement.
- **Threats of violence or security incidents** – lockdown or shelter-in-place procedures to protect staff and clients.
- **Power outage or utility failure** – activation of backup power or relocation of services where safe.
- **Earthquake or structural damage** – immediate safety actions (“drop, cover, hold”), evacuation, and site safety assessment prior to re-entry.

Each location maintains:

- Emergency diagrams reviewed every five years, or when there is a change in location of fire safety installations, evacuation routes or assembly areas.

- Evacuation plans reviewed annually, including evacuation and lockdown instructions tailored to the site layout and located at the Emergency Control Point at each site.
- Warden and First Aid Officer roles, trained and recorded under WHS obligations. Each site has a minimum of a Chief Warden and Deputy Chief Warden/Warden. General warden training is provided and recorded through Action HRM.
- Emergency contact lists for internal leaders, emergency services, and critical suppliers. The relevant list for each site is included in the emergency evacuation plan.

Emergency drills and reviews are conducted at least annually, or after any significant change to the workplace environment. Outcomes of drills and actual incidents are recorded and used to improve preparedness.

Note: These detailed emergency response procedures are not duplicated within this Business Continuity and Recovery Plan to ensure consistency and version control. They are maintained under Footprints' Emergency Evacuation Plans and form a key supporting component of the organisation's overall resilience framework.

8. Business Continuity Procedures

8.1 Continuity of Critical Client Services

Footprints prioritise the continuation of services that directly impact client safety, wellbeing, and regulatory compliance. [Refer Appendix 4](#) for monitoring checklist. Also refer document CHK-003 Monitoring Checklist.

Service-Specific Procedures

Table 7: Service area critical functions and continuity measures

Service Area	Critical Functions	Continuity Measures
Aged Care	Personal care, in-home support, clinical monitoring, transport services	• Use alternate staff and cross-trained personnel. • Deploy mobile care units and telehealth options • Coordinate with partner aged care providers for temporary coverage • Ensure supply and emergency kits kept up to date and accessible from various locations. • Prioritise high-need participants for immediate support
Disability (NDIS)	Participant plan delivery, daily support, therapy services	• Prioritise high-need participants for immediate support. • Implement remote support via phone/video when in-person services are interrupted. • Maintain communication with participants and families regarding alternate arrangements.

Mental Health	Case management, outreach, clinical care	• Assign staff to critical caseloads • Use telehealth and virtual check-ins • Establish temporary outreach hubs if facilities are compromised • Coordinate with partner agencies for crisis support
Homelessness and Housing Services	Emergency accommodation, outreach, tenancy support	• Activate temporary shelter locations • Coordinate with local councils and partner organisations for capacity support • Maintain mobile outreach teams and communication channels • Ensure access to food, hygiene, and essential supplies

Program-specific contractual obligations must be incorporated into relevant procedures and documented as sub-continuity plans within individual service delivery manuals.

8.2 Alternative Service Delivery Models

- Remote Delivery: Use phone, video, or online platforms to maintain client contact and care continuity.
- Temporary Relocation: Pre-identified sites for service relocation if primary sites are compromised.
- Mobile Units: Vehicles equipped with essential supplies for outreach to clients in home or community settings.
- Partnerships: Collaboration with external providers to ensure uninterrupted care in critical situations.

8.3 Workforce Redeployment and Rostering

- Staff may be reassigned to critical services based on need and skillset.
- Rostering adjustments consider staff availability, safety, and workload to maintain sustainable operations.
- Volunteers may be engaged for non-clinical support functions under supervision and appropriate training.
- Cross-training ensures flexibility in critical service delivery across programs.

8.4 Manual Workarounds and Paper-Based Systems

In the event of ICT or system outages:

- Maintain paper-based client records for critical care functions.
- Use manual checklists for service delivery and incident reporting.
- Ensure secure storage and later digital upload of manual records to maintain data integrity and regulatory compliance.

8.5 Coordination with Partners and Funding Bodies

- Communicate disruptions and continuity measures promptly with funders and regulators.
- Engage partner organisations to support service delivery gaps, including temporary staffing, facilities, or transport.

- Share recovery priorities to ensure continuity aligns across all stakeholders.

8.6 Client Safety, Wellbeing, and Dignity Provisions

- Prioritise the physical and psychological safety of clients during service disruptions.
- Implement risk assessments for each client, identifying high-risk individuals who require immediate attention.
- Ensure clients have access to medications, food, water, and essential personal care.
- Maintain confidentiality and privacy even in alternative or emergency service arrangements.
- Document all decisions and interventions in line with regulatory standards.

8.7 Critical Supplier and Subcontractor Continuity

- Maintain a register of critical suppliers and alternate providers, this should be documented in individual service delivery manuals
- Ensure contractual arrangements include emergency provisions or continuity clauses.
- Monitor supplier status during incidents and activate contingency agreements as needed.
- Communicate regularly with suppliers regarding service continuity expectations.

9. ICT Recovery Procedures

9.1 Objectives

The primary objectives of ICT disaster recovery are to:

- Restore critical systems and infrastructure in accordance with Recovery Time Objectives (RTOs)
- Ensure data integrity, security, and confidentiality in compliance with the Privacy Act 1988 (Cth) and sector-specific standards.
- Maintain continuity of client-facing services, governance, and operational support.
- Minimise service disruption across aged care, disability, mental health, and homelessness programs.

9.2 Systems and Application Inventory

Critical ICT systems include:

- Client Management Systems: CRM databases, client records.
- Quality Management System: Incident management, audit and compliance registers
- Communication Platforms: Email, phone systems, telehealth applications, SMS alert systems.
- Finance and HR Systems: Payroll, rostering, financial reporting.
- Shared Infrastructure: Network servers, storage devices, cloud services, backup servers.

All critical systems are classified by priority to ensure high-risk or high-impact systems are recovered first.

9.3 Backup and Restoration Procedures

- Daily Backups: Automated daily backups of all critical data stored securely offsite or in encrypted cloud storage.
- Regular Testing: Backup integrity and restoration procedures tested quarterly.
- Restoration Protocols: Step-by-step instructions for restoring data and systems in order of priority, starting with client-facing applications.
- Documentation: All recovery actions recorded to maintain accountability and facilitate post-incident review.

9.4 Network and Infrastructure Recovery

- Validate connectivity and access to critical systems for staff and service delivery teams.
- Implement temporary infrastructure solutions (e.g., mobile hotspots, VPN access) to maintain operational continuity during recovery.

9.5 Cyber Incident Response

In the event of a cybersecurity incident (e.g., ransomware, malware, data breach):

1. Activate Cyber Incident Response Plan, coordinated by the Technology and Systems Lead.
2. Isolate affected systems to prevent spread or further compromise.
3. Assess impact on client data, service delivery, and regulatory compliance.
4. Notify regulatory bodies if required, including the Office of the Australian Information Commissioner (OAIC) and relevant funding bodies.
5. Restore systems from the most recent verified backup.
6. Document all actions taken, including communications and decisions.

9.6 Validation and System Testing

- After recovery, all systems are tested for functionality, data integrity, and user access.
- Staff confirm operational readiness for client-facing activities.
- Critical logs and system reports are reviewed to ensure compliance and prevent recurrence.

9.7 Communication and User Access Restoration

- Notify all staff when systems are restored, providing guidance for safe and secure access.
- Ensure client-facing teams have access to necessary systems, records, and communication tools.
- Maintain communication with external stakeholders if recovery affects reporting, funding, or regulatory compliance.

9.8 Sign-Off and Resumption of Standard ICT Operations

- The ICT Disaster Recovery Lead, in consultation with the EMT, signs off on full restoration of operations.
- Systems return to normal operational procedures, with any temporary measures decommissioned.
- Lessons learned from the incident are incorporated into plan updates, staff training, and preventive controls.

9.9 Integration with Business Continuity

- ICT recovery is aligned with service continuity priorities outlined in Section 6.
- Recovery sequencing ensures that critical client services are supported by ICT availability, data access, and communication tools.
- Post-incident reviews integrate business and ICT recovery learnings, strengthening overall organisational resilience.

10. Return to Normal Operations

10.1 Recovery Handover Process

- Upon stabilisation of services and ICT systems, the Executive Management Team (EMT) formally hands over operational control back to the business managers.
- A handover checklist ([Refer Appendix 5](#)) is used to verify that:
 - All critical client services have resumed.
 - Systems and infrastructure are fully functional.
 - Staff and volunteers are informed of status and any continuing temporary procedures.
- Clear communication is issued to all staff, clients, families, and external stakeholders confirming resumption of standard operations.

Also refer to document CHK-004 Exiting/recovery Checklist.

10.2 Verification of Business and Service Operations

- Managers confirm that all services are functioning within agreed service levels.
- Any ongoing issues or temporary workarounds are documented and monitored until fully resolved.
- Verification ensures compliance with:
 - Aged Care Quality Standards (client care and safety)
 - NDIS Practice Standards (service delivery and participant support)
 - Mental Health Standards (clinical governance)
 - Human Services Quality Standards (risk management and governance)
 - Child Safe Standards (policies and procedures)
 - Internal organisational policies and contractual obligations

10.3 Post-Incident Review and Lessons Learned

- A post-incident review (PIR) is conducted by the EMT within 14 days of incident resolution.
- The review focuses on:
 - Incident timeline and sequence of events
 - Effectiveness of response and continuity procedures
 - Staff and client feedback
 - Communication effectiveness internally and externally
 - Resource allocation and usage
 - ICT recovery performance
- Key findings are documented and shared with the Board.

10.4 Corrective Actions and Continuous Improvement

Recommendations from the PIR are incorporated into:

- Updates to the BCRP
- Service-level continuity procedures
- ICT disaster recovery protocols
- Staff training and exercises
- Supplier or partner agreements, if applicable

Continuous improvement ensures that future incidents are managed more efficiently, and organisational resilience is strengthened over time.

10.5 Wellbeing and Support for Staff and Clients Post-Incident

Footprints recognises the potential psychological impact of disruptions on staff and clients. Support measures may include:

- Debrief sessions for staff
- Access to Employee Assistance Programs (EAP)
- Additional support for clients experiencing distress or disruption to their care

Wellbeing initiatives are documented and monitored as part of the post-incident review.

10.6 Formal Closure

- The CEO formally closes the incident following review and corrective action planning.
- All documentation, logs, and communication records are stored securely for audit, regulatory compliance, and future reference.
- Lessons learned are incorporated into annual training, drills, and continuity plan updates.

11. Testing, Training, and Maintenance

11.1 Testing Program

Regular testing of the BCRP ensures that procedures are effective, staff are prepared, and critical functions can be maintained during disruptions.

Types of Tests:

1. **Tabletop Exercises** – Discussion-based scenarios for leadership and staff to review procedures and decision-making.
2. **Functional Exercises** – Simulated activation of specific business continuity or ICT procedures, testing response and recovery steps.

Frequency:

- Tabletop exercises: Annually
- Functional exercises: Annually

Documentation:

Exercise results, identified gaps, and corrective actions are recorded and reported to the Executive Management Team.

11.2 Roles in Testing

- **Executive Management Team (EMT):** Oversight, authorisation, and participation in exercises.
- **Continuity Coordinator:** Plans and coordinates testing, monitors results, and reports outcomes.
- **Managers:** Ensure staff participation and simulate continuity procedures for their programs/regions.
- **ICT Lead:** Tests IT recovery procedures, system restorations, and backup functionality.
- **Staff and Volunteers:** Actively participate in exercises and training, providing feedback for improvements.

11.3 Staff Training and Awareness

All staff and volunteers receive training on:

- Their roles and responsibilities during disruptions.
- Activation of the BCRP.
- Communication protocols and escalation procedures.
- Use of manual workarounds or alternative service delivery methods.

Training is provided at induction and reinforced through annual refresher sessions. Specialised training for ICT recovery, clinical emergency response, and regulatory compliance is provided as required.

11.4 Plan Review and Update Cycle

The BCRP is reviewed at least annually, or after:

- A major service change
- An incident or activation of the plan
- Changes to regulatory or legislative requirements

Reviews ensure that contact lists, systems, procedures, and risk assessments are current.

Updates are documented in the document register, including author, date, version, and nature of changes.

Appendices

Appendix 1 – Implementation/Activation Checklist (CHK-001)

Task	Responsible	Completed (✓)	Notes
Confirm incident meets activation criteria (critical service disruption, ICT outage, facility loss, regulatory breach)	CEO / EMT / Continuity Coordinator		
Activate BCDRP	CEO/EMT		
Assign roles & responsibilities	Continuity Coordinator/Managers		
Ensure staff and volunteers are informed of activation	Service Managers / Communications Officer		
Implement initial response steps (safety, assessment, temporary workarounds)	Managers		
Notify external stakeholders if required (clients, families, regulators, suppliers)	Communications Officer		
Mobilise alternate service delivery methods (telehealth, temporary sites, mobile units)	Managers		
Activate ICT disaster recovery if systems or data are compromised	ICT Disaster Recovery Lead		
Record all actions, decisions, and communications	Continuity Coordinator		

Instructions for Use

1. Complete each item in real time during activation stage.
2. Include dates, names, and notes for accountability.
3. Use completed checklist as part of audit/review.

Appendix 2 – Communication templates

IT Outage/Cyber Incident

Email

Subject: Business Continuity Alert – IT Systems Disruption

Dear Team,

Our IT systems have experienced a disruption as of [time/date]. The Business Continuity and Recovery Plan has been activated.

Please follow these instructions:

- Avoid using affected systems until notified.
- Use [alternate communication method, e.g., phone or Teams] for urgent messages.
- Contact [IT Support Contact Name / Role] at [phone/email] if you need immediate assistance.

Updates will be provided every [x hours] via [email/SMS/Teams].

Thank you for your cooperation.

Kind regards

SMS

Footprints BCRP activated – IT outage. Avoid using affected systems. Check email for instructions or contact [IT contact] at [number].

Phone Script – for afterhours contact as needed

Hi [Name], this is [Your Name] from Footprints. Our IT systems are down, and the Business Continuity Plan has been activated. Please avoid using affected systems and follow instructions sent via email. For urgent support, contact [IT contact] at [number]. Can you confirm you received this?

Site Emergency

Email

Subject: Business Continuity Alert – Site Emergency

Dear Team,

There has been a [type of emergency, e.g., flood/fire/earthquake] at [site/location] as of [time/date]. The Business Continuity and Recovery Plan is in effect.

Actions to take:

- [Evacuate / work from home / report to alternate site at [location]]
- Avoid the affected area until further notice.
- Contact [Emergency Contact Name / Role] at [phone/email] if you require assistance.

Updates will be provided via [email/SMS/Teams].

Please prioritise your safety.

Kind regards

SMS

Footprints: BCRP activated – [flood/fire/earthquake] at [location]. Follow instructions in email. Contact [name] at [number] for urgent help.

Phone Script

Hi [Name], this is [Your Name] from Footprints. There's a [type of emergency] at [location], and the Business Continuity and Recovery Plan is active. Please [evacuate/work from home/report to alternate site]. Contact [Emergency Contact Name] at [number] for help. Are you safe and able to follow these instructions?

Utility Failure

Email

Subject: Business Continuity Alert – Utility Disruption

Dear Team,

A [type of utility failure, e.g., power outage, water interruption, internet outage] has occurred at [location] as of [time/date]. The Business Continuity and Recovery Plan has been activated.

Instructions:

- [Work from home / suspend client-facing operations / use alternate site]
- Keep devices charged and maintain communication via [phone/Teams].
- For urgent assistance, contact [Contact Name / Role] at [phone/email].

Updates will be provided every [x hours].

Thank you for your cooperation.

Kind regards,

SMS

Footprints: BCRP activated – [power/internet/water] outage at [location]. Follow email instructions. Contact [name] at [number] for urgent help.

Phone Script

Hi [Name], this is [Your Name] from Footprints. A [utility failure] has occurred at [location], and the Business Continuity Plan is active. Please [action – work from home / relocate / suspend operations]. Contact [Contact Name] at [number] if you need help. Can you confirm you received this message?

Pandemic/Health Emergency

Email

Subject: Business Continuity Alert – Health Emergency / Pandemic Measures

Dear Team,

Due to [pandemic/health emergency], the BCRP has been activated as of [time/date]. Please

follow the instructions below to ensure your safety and business continuity:

Actions:

- Work from home where possible.
- Avoid non-essential travel or gatherings.
- Maintain health and hygiene protocols.
- Report any symptoms or exposure to [Health/HR Contact Name] at [phone/email].

Updates will be provided via [email/SMS/Teams].

Thank you for your cooperation.

SMS

Footprints: BCRP activated – Health emergency. Work from home if possible. Follow hygiene protocols. Contact [Health/HR contact] at [number] for guidance.

Phone

Hi [Name], this is [Your Name] from Footprints. Due to a health emergency/pandemic, the BCRP is active. Please work from home if possible and follow health guidelines. Contact [Health/HR contact] at [number] for support. Are you able to comply with these instructions safely?

Client & Family Communication Templates

Service Disruption Notification

Email Template

Subject: Important: Temporary Service Disruption – [Service Name / Location]

Dear [Client/Family Name],

We are writing to inform you that due to [incident type – e.g., power outage, site emergency, pandemic], our services at [location] will be temporarily disrupted as of [date/time].

We understand this may cause inconvenience and we are working to minimise the impact.

Updates will be provided regularly via [email/SMS/phone].

For urgent concerns, please contact [Contact Name / Role] at [phone/email].

Thank you for your understanding and cooperation.

Kind regards,

SMS Template

Footprints: Service disruption at [location] due to [incident]. Updates via email/phone. Contact [name] at [number] for urgent matters.

Phone Script

Hi [Client/Family Name], this is [Your Name] from Footprints. We are experiencing a [type of incident] at [location], which will temporarily affect services. We are working to manage the situation and will provide updates via [email/SMS]. If you have urgent questions, you can reach [Contact Name] at [number].

Alternate arrangements Notification

Email Template

Subject: Service Update – Alternate Arrangements in Place

Dear [Client/Family Name],

To ensure continuity of care during the [incident], we have implemented the following alternate arrangements:

- [Example: Services will be delivered at [alternate location]]
- [Example: Staff will provide services at home/virtually]
- [Example: Temporary schedule changes – specify if needed]

These arrangements are in place from [start date/time] until [end date/time or “further notice”].

Please contact [Contact Name / Role] at [phone/email] if you have questions or concerns regarding these arrangements.

Thank you for your cooperation and understanding.

Kind regards,

SMS Template

Footprints: Alternate arrangements for [service] are in place due to [incident]. Contact [name] at [number] for details.

Phone Script

Hi [Client/Family Name], this is [Your Name] from Footprints. Due to [incident], we have put alternate arrangements in place for [service], including [briefly describe arrangements]. These will remain in place until [date/further notice]. For questions, please contact [Contact Name] at [number].

Safety Guidance/Health Instructions

Email Template

Subject: Important Safety Guidance – [Service Name / Location]

Dear [Client/Family Name],

In light of [incident/pandemic/health emergency], we request that you follow the below safety guidance to protect yourself and others:

- [Example: Maintain social distancing / wear masks / hand hygiene / avoid non-essential visits]

- [Example: Follow any isolation or quarantine guidance if symptomatic]
- [Example: Report any health concerns to [Contact Name / Role]]

Your safety and wellbeing remain our priority. Please contact [Contact Name] at [phone/email] if you need further advice or support.

Thank you for your cooperation.

Kind regards,

SMS Template

Footprints: Please follow safety guidance due to [incident]. Wash hands, maintain distancing, and contact [name] at [number] if unwell.

Phone Script

Hi [Client/Family Name], this is [Your Name] from Footprints. Due to [incident], we ask that you follow safety guidance: [briefly outline key points]. If you feel unwell or have concerns, contact [Contact Name] at [number]. Are you able to follow these guidelines safely?

Regulatory Incident Notification Templates

Email Template

Subject: Urgent Notification of [Incident Type] – Footprints

To: [Regulator Contact / Email]

Cc: [Internal Compliance / Risk Team]

Dear [Regulator Name/Title],

We wish to notify you of an incident/compliance breach that occurred on [Date] at [Location/Department].

Incident Details:

- **Type of Incident:** [e.g., Data Breach / Safety Incident / Service Interruption]
- **Description:** [Brief description of what happened]
- **Affected Parties:** [Number of individuals/clients/customers impacted]
- **Immediate Actions Taken:** [Containment, mitigation, or safety actions]
- **Potential Impact:** [Operational, financial, or regulatory impact]

We are conducting a full investigation and will provide a detailed report within [timeframe, e.g., 7 days].

Please advise if additional information or immediate actions are required.

Sincerely,

Formal Letter Template

Date: [DD/MM/YYYY]

To: [Regulator Name/Agency]

Address: [Regulator Address]

Subject: Regulatory Notification of [Incident Type]

Dear [Regulator Name/Title],

This letter serves as formal notification of an incident that occurred within Footprints on [Date].

Incident Summary:

- **Type of Incident:** [Describe]
- **Location/Department:** [Specify]
- **Description of Incident:** [Provide detailed description]
- **Immediate Response:** [Actions taken to manage the incident]
- **Impact Assessment:** [Estimate of affected individuals, financial, or operational impact]
- **Preventive Measures:** [Steps taken to prevent recurrence]

We are committed to full compliance and will provide an in-depth report as soon as our investigation is complete. Please advise if further information or immediate action is required.
Sincerely,

Media Statement Templates - For public-facing communications during major incidents

FOR IMMEDIATE RELEASE

Date: [DD/MM/YYYY]

Headline: [Brief, clear statement of incident]

Example: “Footprints Responds to Service Disruption Affecting Home Care Clients”

Subheadline (optional): [Optional brief context or reassurance]

Example: “Immediate measures implemented to ensure client safety and service continuity”

Body:

[City/Location] – Footprints confirms that [brief description of incident, e.g., “a disruption to our IT systems” / “a confirmed COVID-19 case among staff”] occurred on [Date].

Details of the Incident:

- **What Happened:** [Plain-language description of the incident]
- **Who is Affected:** [Clients, staff, community, etc.]
- **Immediate Actions Taken:** [Safety measures, mitigation, containment, notifications]
- **Next Steps / Ongoing Measures:** [Investigation, monitoring, alternative arrangements, collaboration with authorities]

Footprints is committed to transparency, safety, and minimising disruption. We are working closely with [regulatory bodies / health authorities] to ensure all requirements are met.

Contact for Media Inquiries:

[Name]

[Position]

[Phone]

[Email]

Optional Closing Statement / Quote:

Example: “The safety and wellbeing of our clients and staff remain our highest priority. We are taking every measure to address this incident promptly and effectively.” – [CEO / Director Name]

Appendix 3 – Continuous Improvement/Follow Up (CHK-002)

Task	Responsible	Frequency	Completed (✓)	Notes
Incorporate lessons learned into BCR Plan updates	Continuity Coordinator	After PIR		
Update staff training & exercises based on incident findings	HR / Training Lead	Post-incident		
Test corrective actions and improvements in next exercise	Continuity Coordinator /Managers	Next scheduled test		
Report findings to EMT & BCR Committee	Continuity Coordinator	Post-incident		
Review regulatory & contractual compliance post-incident	Compliance Officer	Post-incident		

Appendix 4 – Monitoring Checklist (CHK-003)

Task	Responsible	Frequency	Completed (✓)	Notes
Monitor client safety & service delivery	Managers	Daily		
Track staff availability & redeployment	Managers / HR	Daily		
Monitor ICT system recovery progress	ICT Lead	Ongoing		
Maintain communication logs (internal & external)	Communications Officer	Ongoing		
Track resource usage (supplies, vehicles, emergency kits)	Facilities / Logistics Coordinator	Daily		
Record incident developments & risk updates	Continuity Coordinator	Ongoing		
Escalate new or emerging issues to IMT / CEO	Continuity Coordinator	As required		
Liaise with external stakeholders for updates or support	Communications Officer / Managers	As required		
Review critical supplier availability and activate alternates if needed	Facilities / Procurement	Daily		
Document all changes to service delivery, ICT status, and client impact	Continuity Coordinator	Ongoing		

Instructions for Use

1. Complete each item in real time during monitoring
2. Include dates, names, and notes for accountability.
3. Use completed checklist as part of **audit, PIR, and regulatory reporting**.

Appendix 5 – Exiting/Recovery Checklist (CHK-004)

Task	Responsible	Completed (✓)	Notes
Confirm incident resolved and normal operations can resume	CEO / Continuity Coordinator		
Conduct handover from IMT to service managers	Continuity Coordinator		
Verify all services restored and functioning within agreed service levels	Managers		
Ensure ICT systems fully restored and tested	ICT Disaster Recovery Lead		
Notify all staff, clients, families, and external stakeholders of resumption	Communications Officer		
Conduct post-incident review (PIR)	Continuity Coordinator / IMT	Within 14 days	
Identify lessons learned and corrective actions	PIR Team		
Update BCDR Plan, procedures, and training materials	Continuity Coordinator		
Review supplier/contractor continuity performance	Facilities / Procurement		
Provide staff debriefs & wellbeing support	Managers / Safety Lead		
Archive all incident records, communications, and logs	Continuity Coordinator		
Formal closure of incident and sign-off by CEO	CEO		

Instructions for Use

1. Complete each item in real time during exit stage.
2. Include dates, names, and notes for accountability.
3. Use completed checklist as part of audit.

Key Contacts

Internal Contacts

Position	Name	Phone	Email
Chief Executive Officer	Dr Tanya Bell	0439 343 284	tanyab@footprintscommunity.org.au
GM Compliance and Reporting	Janine Seabrook	0449 662 328	janines@footprintscommunity.org.au
GM Sector Impact	Sharon Sweeney	0412 703 914	sharons@footprintscommunity.org.au
GM Service Operations	Ryan O'Leary	0422 846 067	ryano@footprintscommunity.org.au
GM Finance and Corporate Services	Scott Thompson	0476 231 909	scottt@footprintscommunity.org.au
Senior Manager People and Culture	Loku Priyantha	0414 768 367	lokup@footprintscommunity.org.au
RM Southern	Robert Kilpatrick	0492 950 853	robertk@footprintscommunity.org.au
RM Central	Jacqui Klenner	0426 242 063	jacquik@footprintscommunity.org.au
RM North	Jane Matsen	0481 601 899	janem@footprintscommunity.org.au
Ageing Well Lead	Kim Grady	0481 601 488	kimg@footprintscommunity.org.au
Mental Wellness Lead	Helen Doyle	0404 616 253	helend@footprintscommunity.org.au
Technology and Systems Lead	Anthony Cowdroy-Ling	0424 731 145	Anthonyc@footprintscommunity.org.au
Communications Officer	Antoinette Lloyd		antoinettel@footprintscommunity.org.au
Facilities and Logistics Coordinator	Jenny English	0402 675 090	jennifere@footprintscommunity.org.au

External Contacts

Company	Contact	Phone	Email
Emergency Services		000	
SES		132 500	
Aged Care Quality and Safety Commission		1800 951 822	info@agedcarequality.gov.au
NDIS Commission		1300 311 675	contactcentre@ndiscommission.gov.au
Australian Commission on Safety and Quality		(02) 9126 3600	mail@safetyandquality.gov.au
Brisbane South PHN		1300 467 265	contactus@bsphn.org.au
Brisbane North PHN		3630 7300	
Darling Downs and West Moreton PHN		4615 0900	info@ddwmphn.com.au
Gold Coast PHN		5635 2455	info@gcphn.com.au
Country to Coast Qld PHN (Sunshine Coast/Wide Bay)		5456 8100	info@c2coast.org.au
Northern Queensland PHN		4034 0300	support@nqphn.com.au
Western Queensland PHN		4573 1900	admin@wqphn.com.au
Hunter New England and Central Coast PHN		1300 859 028	info@hneccphn.com.au

Revision history

Version no	Date commenced	Change description	Review date	Plan owner		Authorised by (CEO or Board)
				Position title	Functional Area	
1	2 April 2026	- Initial version - Replaces the previous 'Disaster Recovery Plan'	2 April 2027	GM Compliance and Reporting	Compliance and Reporting	CEO
2						
3						