[Service Letterhead]

Disclaimer

Please be advised that this resource has been prepared by the Aboriginal Health and Medical Research Council of NSW (AH&MRC) to broadly meet the needs of AH&MRC's Member Organisations. This resource is a general guide and will need to be amended to suit your particular organisation.

AH&MRC cannot guarantee that this resource will meet all the requirements of your individual organisation and may not be relevant to particular patients or their circumstances. AH&MRC strongly recommends that you undertake your own independent skill or judgement or seek appropriate professional advice relevant to their own particular circumstances when so doing.

Intellectual Property and Copyright

Unless otherwise expressly stated, the copyright of this resource is owned by AH&MRC. This resource may only be used by AH&MRC's Member organisations and cannot be used for any other purpose or by any other organisation or group.

This resource must not be published or replicated without AH&MRC's written permission. All other rights are reserved.

Limitation of liability

AH&MRC takes reasonable steps to maintain the accuracy of information available in this resource, however, some or all of the information is current at the date of the first publication, and may, from time to time, be amended, or become superseded or otherwise inaccurate. AH&MRC is not responsible for ensuring that the information contained within this resource is accurate, current, suitable or complete, and offers no guarantee that this resource will meet your organisation's or particular patients needs.

Accordingly, where conditions and warranties implied by law cannot be excluded, the AH&MRC limits its liability where it is entitled to do so. Otherwise, AH&MRC, its employees and agents are not liable for any loss or damage (including consequential loss or damage) to any users of this resource, however caused, which may arise directly or indirectly from this resource.

Governance and Implementation

This resource should be reviewed and endorsed in accordance with the organisation's governance and document control processes prior to implementation.

[Organisation Name]

Organisational Emergency Management and Business Continuity Policy

Document Control

Policy Title	Organisational Emergency Management and Business Continuity Policy
Policy Number	P-XXX
Approval Date	DD/MM/YYYY
Amended Date	DD/MM/YYYY
Next Review Date	DD/MM/YYYY
Version Number	1.0
Responsible Officer	Chief Executive Officer
Accreditation Mapping Code	RACGP – Clinical Governance; Emergency Preparedness and Response; Business Continuity; Risk Management; Information Security; Workforce; Patient Safety; Access and Continuity of Care; Quality Improvement NSQHS – Standard 1 Clinical Governance; Standard 2 Partnering with Consumers; Standard 5 Comprehensive Care; Standard 6 Communicating for Safety NSQPH – Clinical Governance; Partnering with Consumers; Clinical Safety; Communicating for Safety QIC – Governance; Risk Management; Emergency and Disaster Management; Business Continuity; Workforce; Service Delivery; Information Management; Quality Improvement

1. Purpose

The purpose of this policy is to establish the overarching governance, preparedness, response, business continuity, resilience and recovery requirements for emergencies, disasters, critical incidents and significant disruptions that may affect [Organisation Name], its people, communities, facilities, systems, information, resources or ability to deliver services.

[Organisation Name] recognises that emergencies may occur with little or no warning and may arise from natural hazards, public health events, security incidents, infrastructure or technology failure, cyber incidents,

workforce disruption, supply-chain failure or other circumstances. Effective emergency management requires coordinated arrangements that protect life and safety, maintain critical healthcare and organisational functions, safeguard assets and information, support affected communities and enable timely and sustainable recovery.

[Organisation Name] will apply the principles of prevention and mitigation, preparedness, response and recovery and will ensure that emergency arrangements are proportionate, adaptable, culturally safe, risk based and capable of operating alongside external emergency-management and health-system arrangements.

This policy is intended to ensure that [Organisation Name]:

- maintains an organisation-wide emergency management and business continuity system;
- identifies, assesses and manages foreseeable emergency, disaster and continuity risks;
- prioritises the protection of life, health and safety;
- maintains essential healthcare and critical organisational functions wherever reasonably practicable;
- establishes clear emergency authority, leadership, command, coordination, communication and accountability;
- maintains effective emergency preparedness across all service locations and models of care;
- identifies critical services, systems, infrastructure, information, suppliers, dependencies and single points of failure;
- establishes acceptable service levels and recovery priorities for critical functions;
- maintains effective evacuation, lockdown, shelter-in-place and emergency response arrangements;
- maintains contingency arrangements for loss of facilities, utilities, telecommunications, ICT systems, critical equipment, workforce, suppliers and other dependencies;
- provides for continuity, prioritisation, reduction, relocation, suspension and restoration of services where normal operations are disrupted;
- maintains appropriate emergency communication with workers, patients, communities, emergency services, partner organisations and authorities;
- supports interoperability and cooperation with external emergency, health and community organisations;
- protects critical records, information and organisational assets;
- considers the needs of Aboriginal and Torres Strait Islander people and communities and people who may experience disproportionate impacts during emergencies;
- provides for operational, clinical, workforce and community recovery;
- identifies and addresses healthcare that has been delayed, interrupted or missed because of an emergency;
- periodically tests emergency, continuity and disaster recovery arrangements;
- provides governance assurance regarding organisational preparedness; and
- learns from emergencies, disruptions, exercises and near misses.

Emergency management and business continuity form part of [Organisation Name]'s broader organisational governance, clinical governance, work health and safety, risk management, information governance and continuous quality improvement systems.

2. Scope

This policy applies to all persons undertaking work for or on behalf of [Organisation Name], including governance members, employees, healthcare practitioners, managers, contractors, consultants, students, trainees, volunteers, visiting practitioners and agency personnel.

It applies across all facilities, clinics, offices, outreach locations, mobile services, community programs, home-visiting activities, temporary service locations, events and other environments in which [Organisation Name] operates or provides services.

The policy applies to emergencies, disasters, critical incidents and significant disruptions that may affect people, communities, service delivery, facilities, infrastructure, technology, information, workforce, supply chains, community access or organisational operations.

Clinical emergencies involving individual patients are primarily governed by the Clinical Emergency Management Policy and associated clinical procedures. Where a broader organisational emergency creates clinical risks, service disruption or increased healthcare demand, both policies apply.

3. Definitions

Emergency – An actual or imminent event requiring coordinated action to protect people, property, services, information, the environment or organisational operations.

Disaster – A serious disruption causing significant human, material, economic, environmental, community or organisational impacts that may exceed normal operating capacity.

Critical Incident – An event or circumstance that causes, or has the potential to cause, serious harm, major operational disruption, significant organisational risk or substantial loss.

Emergency Management – The coordinated approach to prevention and mitigation, preparedness, response and recovery from emergencies and disasters.

Business Continuity – The capability of the organisation to continue delivering prioritised services and functions at acceptable predefined levels following disruption.

Business Continuity Plan (BCP) – Documented arrangements for maintaining, adapting, relocating, restoring or recovering critical functions and services following disruption.

Emergency Management Plan (EMP) – Documented arrangements for preparing for, responding to and recovering from emergencies affecting the organisation.

Critical Service / Function – A service, activity, system or function that must be maintained or restored within an identified timeframe to avoid unacceptable harm or organisational impact.

Minimum Acceptable Service Level – The minimum level at which a critical service or function can operate during disruption without creating unacceptable risk.

Maximum Tolerable Period of Disruption (MTPD) – The maximum period for which disruption to a critical function can be tolerated before consequences become unacceptable.

Recovery Time Objective (RTO) – The target timeframe for restoring a critical service, system or function following disruption.

Recovery Point Objective (RPO) – The maximum acceptable period of data loss, expressed in time, for a critical information system following disruption.

Single Point of Failure – A person, system, supplier, facility, resource or dependency whose failure could cause significant disruption because an effective alternative is not readily available.

Disaster Recovery – The coordinated restoration of ICT systems, data, infrastructure or other critical organisational resources following significant disruption.

Emergency Control Organisation (ECO) – Persons appointed to undertake designated emergency-control responsibilities for a facility or workplace.

Incident Management Team (IMT) – The designated group responsible for strategic and operational coordination of the organisational response to a significant emergency or disruption.

Incident Action Plan – A documented statement of current incident objectives, priorities, actions, responsibilities and resource requirements used to support coordinated management of a significant or prolonged event.

Situational Awareness – The timely collection, validation, analysis and sharing of information necessary to understand an emergency, its impacts, emerging risks, available resources and response priorities.

Mutual Aid / Reciprocal Arrangement – An arrangement between organisations to provide agreed support, resources, facilities, workforce or services during disruption or emergency.

Evacuation – The organised movement of people from an unsafe or potentially unsafe location to a safer location.

Shelter-in-Place – Remaining within, or moving to, a designated safe location within a facility when evacuation would create greater risk.

Lockdown – Restricting entry, exit or movement within a facility in response to an identified safety or security threat.

Recovery – The coordinated process of restoring services, systems, workforce capability, infrastructure, community access and organisational functioning following an emergency or disruption.

4. Policy Statement

[Organisation Name] is committed to maintaining an integrated, risk-based and culturally responsive emergency management and business continuity system that protects life and safety, maintains essential healthcare and supports organisational and community resilience.
Emergency management will be based on prevention and mitigation, preparedness, response and recovery.
The organisation's emergency arrangements will be guided by the following principles:

- protection of life, health and safety takes priority;
- essential healthcare and critical functions will be maintained wherever reasonably practicable;
- decisions will be proportionate to the nature, scale and consequences of the emergency;
- emergency authority and accountability will remain clear;

- decisions should be made at the most appropriate organisational level while enabling timely escalation;
- emergency arrangements will be adaptable to changing circumstances;
- services will cooperate and interoperate with external emergency, health and community systems where required;
- professional judgement and patient safety will remain central to clinical decisions;
- cultural safety, accessibility and equity will be considered throughout preparedness, response and recovery;
- reliable information and situational awareness will support decision-making; and
- emergency experience will be used to strengthen future organisational resilience.

[Organisation Name] will maintain arrangements that provide assurance that foreseeable risks are managed, workers understand their responsibilities, emergency plans remain current, critical services and dependencies are identified, continuity and recovery arrangements are effective, and emergency preparedness is periodically tested and improved.

5. Policy

5.1 Emergency Governance and Accountability

[Organisation Name] will maintain clear governance, accountability, delegations and reporting arrangements for emergency management and business continuity.

Emergency preparedness will be integrated with organisational governance, clinical governance, work health and safety, enterprise risk management, information governance, cybersecurity, asset management, workforce planning, financial management and continuous quality improvement.

The organisation will identify persons authorised to activate emergency and business continuity arrangements and establish appropriate succession arrangements where key decision-makers are unavailable.

Significant emergency risks, preparedness gaps, major disruptions and recovery issues will be escalated through appropriate governance structures.

The Board / Governing Body and Executive Management will receive appropriate assurance regarding organisational preparedness, continuity capability, testing outcomes and significant residual risks.

5.2 Continuity of Leadership, Authority and Delegations

Emergency arrangements will provide for continuity of organisational leadership and decision-making where the Chief Executive Officer, executives, managers or other key personnel are unavailable or unable to exercise their responsibilities.

Arrangements will establish appropriate:

- succession of authority;
- alternate authorised officers;
- emergency financial and operational delegations;
- clinical decision-making authority where relevant;
- governance escalation;

- authority to modify, relocate or suspend services; and
- arrangements for urgent decisions outside ordinary governance cycles.

Emergency decisions will be documented proportionate to their significance and retrospectively reported or ratified through normal governance processes where required.

5.3 Emergency Management Framework

[Organisation Name] will maintain a coordinated emergency management framework addressing prevention and mitigation, preparedness, response and recovery.

Arrangements will be proportionate to organisational size, service profile, geographic environment, community needs, operational complexity and risk exposure.

The framework will support scalable emergency response so that organisational arrangements can increase or reduce according to the severity, complexity, duration and consequences of an incident.

5.4 Emergency and Disaster Risk Assessment

Emergency and continuity risks will be identified, assessed, treated and monitored through the organisation's risk-management system.

Risk assessment will consider foreseeable hazards including:

- bushfire, grassfire and smoke;
- flood, storm, severe weather and environmental hazards;
- extreme heat;
- earthquake or structural damage;
- fire or explosion;
- hazardous substances, chemical spills or gas leaks;
- infectious disease outbreaks, epidemics and pandemics;
- electricity, water, sewerage and other utility failure;
- telecommunications or internet failure;
- ICT outages, cyber incidents and information-system failure;
- building, facility or critical-equipment failure;
- security threats, violence or civil disturbance;
- transport and access disruption;
- supply-chain interruption;
- medicine, vaccine, oxygen, fuel or other critical shortages;
- workforce shortages or widespread worker unavailability;
- loss of access to facilities;
- disruption to pathology, pharmacy, hospital, ambulance or other essential external services;
- emergencies affecting outreach, remote or mobile services; and
- concurrent, cascading or prolonged emergencies.

Risk assessments will identify interdependencies and circumstances in which failure in one area may create or compound disruption elsewhere.

5.5 Dependencies and Single Points of Failure

[Organisation Name] will identify critical internal and external dependencies and foreseeable single points of failure that could materially affect essential services.

These may include:

- key workers or specialist roles;
- buildings or service locations;
- clinical and business information systems;
- telecommunications and internet connectivity;
- electricity and water;
- pathology, pharmacy and hospital services;
- critical suppliers;
- vehicles and transport;
- medical equipment;
- refrigeration;
- payroll and financial systems; and
- other critical resources.

Where a material single point of failure is identified, reasonable alternative, redundancy, contingency or recovery arrangements will be established according to risk.

5.6 Emergency Management Plan

[Organisation Name] will maintain a current Emergency Management Plan appropriate to its risks and operating environment.

The plan will establish emergency activation and escalation arrangements, emergency roles and responsibilities, command and coordination, emergency contacts, communication and notification pathways, evacuation and protective actions, emergency-service access, critical resources, alternative operating arrangements and transition to recovery.

Site-specific emergency information will be maintained where facilities, risks or operating environments differ.

5.7 Emergency Activation Levels

The organisation will maintain defined arrangements for scaling emergency response according to the severity, complexity, duration and organisational impact of an event.

Activation arrangements will enable escalation from local operational management through to coordinated organisational emergency management where required.

Activation levels, triggers and operational arrangements will be defined within the Emergency Management Plan.

5.8 Incident Command and Coordination

For significant emergencies, [Organisation Name] will establish an Incident Management Team or equivalent coordination structure appropriate to the circumstances.

Authority, accountability and decision-making responsibility will remain clear throughout the response.

The incident structure may coordinate operations, clinical services, workforce, logistics, facilities, ICT, work health and safety, communications, stakeholder engagement, documentation and recovery.

Clinical leadership and emergency management leadership will remain appropriately coordinated where an organisational emergency affects clinical service delivery.

5.9 Situational Awareness and Incident Information

During significant or prolonged emergencies, [Organisation Name] will maintain reliable mechanisms for collecting, validating, analysing and communicating information necessary to support organisational decision-making.

Information may include:

- nature and extent of the emergency;
- affected locations and services;
- patient and community impacts;
- workforce availability;
- facility and infrastructure status;
- ICT and communication capability;
- critical supplies;
- emerging hazards;
- external emergency information;
- available resources;
- service demand;
- decisions and actions underway; and
- anticipated recovery requirements.

Information will be shared with those who require it to undertake their responsibilities while maintaining appropriate privacy and confidentiality.

5.10 Incident Action Planning and Decision Records

Significant or prolonged emergencies will be managed using documented priorities, objectives and actions proportionate to the event.

Major decisions, emergency directions, service changes, risk acceptances, resource priorities and significant external notifications will be appropriately recorded.

Where an Incident Action Plan is required, its form and operational use will be established through the Emergency Management Plan or supporting procedures.

5.11 External Coordination and Mutual Aid

[Organisation Name] will cooperate with emergency services, public health authorities, Local Health Districts, Primary Health Networks, government agencies, local councils, Aboriginal organisations and other relevant partners during emergencies.

Where beneficial and practicable, the organisation will establish reciprocal or mutual-aid arrangements with appropriate organisations to support temporary:

- service delivery;
- alternate facilities;
- workforce assistance;
- equipment or resource sharing;
- referral pathways;
- clinical support;
- communications; or
- other critical functions.

Reliance on reciprocal arrangements will be appropriately documented and periodically reviewed.

5.12 Emergency Warnings and Authoritative Information

[Organisation Name] will maintain arrangements to monitor authoritative emergency warnings, public health advice and relevant government directions where these may affect its people, communities or services.

Relevant information will be assessed and translated into timely organisational decisions, including changes to service delivery, workforce arrangements, travel, facility access or emergency activation.

Emergency decisions will not rely solely on informal or unverified information where authoritative information is reasonably available.

5.13 Emergency Preparedness and Response

Workers must be able to activate emergency assistance without unnecessary delay.

Emergency response will prioritise life safety, prevention of further harm, containment of immediate risk, timely communication and maintenance of critical services.

Emergency arrangements will recognise that circumstances may change rapidly and will support reassessment and escalation throughout an event.

5.14 Evacuation, Lockdown and Shelter-in-Place

Facilities will maintain arrangements for evacuation, lockdown, shelter-in-place and other protective actions appropriate to identified risks.

Planning will consider patients receiving care, children, older people, people with disability or reduced mobility, visitors unfamiliar with facilities, culturally and linguistically diverse persons and other people who may require assistance.

Emergency exits, evacuation routes, emergency equipment, assembly areas and emergency-service access will be maintained appropriately.

Re-entry following evacuation will occur only when authorised and considered safe.

5.15 Fire and Workplace Emergency Preparedness

[Organisation Name] will maintain fire and workplace emergency arrangements appropriate to each facility.

Fire protection and emergency systems will be maintained in accordance with applicable requirements.

Workers with designated emergency-control responsibilities will receive appropriate training.

Emergency planning and exercises will be undertaken consistent with work health and safety and applicable facility emergency-planning requirements.

5.16 Security, Violence and Serious Threats

Emergency arrangements will address foreseeable security incidents, including occupational violence, aggressive behaviour, serious threats, unauthorised access, armed threats, suspicious packages and other significant security events.

Workers must not place themselves or others at unreasonable risk.

Police or other emergency services will be contacted promptly where required.

Protective arrangements may include duress systems, lockdown, evacuation, restricted access and other proportionate controls.

5.17 Mass Casualty and Service Surge

[Organisation Name] will consider circumstances in which an emergency generates an unusual, sudden or sustained increase in demand for healthcare or community support.

Preparedness arrangements will consider:

- prioritisation of services;
- workforce surge;
- temporary redeployment;
- alternative models or locations of care;
- patient flow;
- clinical supplies and equipment;
- communication with the community;
- coordination with hospitals, ambulance, public health and other health services; and
- safe limits of organisational capacity.

The organisation will not undertake activities beyond available capability where this would create unacceptable risk.

5.18 Infectious Disease, Epidemic and Pandemic Emergencies

[Organisation Name] will maintain scalable arrangements for significant infectious disease outbreaks, epidemics and pandemics.

Arrangements will address, as applicable, infection prevention and control, public health reporting, patient flow, workforce exposure and illness, PPE, critical supplies, vaccination, testing, alternative service delivery, continuity of essential services and community communication.

Current public health requirements and authoritative guidance will be followed.

5.19 Outreach, Mobile, Home and Community-Based Services

Emergency arrangements will extend to services delivered away from permanent facilities.

Planning will consider location, travel, road access, communications, severe weather, worker safety, emergency equipment, vehicle failure, local emergency services, retrieval and transfer pathways and circumstances requiring cancellation or suspension of services.

Activities must not proceed where identified risks cannot be reasonably managed.

5.20 Rural, Remote and Isolated Service Considerations

Where services operate in rural, remote or geographically isolated environments, planning will recognise potentially prolonged emergency-service response times, transport limitations, telecommunications gaps, infrastructure vulnerability, supply-chain disruption and limited access to alternative healthcare.

Local emergency contacts, escalation pathways, alternative communications and appropriate contingency resources will be identified.

5.21 Emergency Communication

[Organisation Name] will maintain arrangements for timely, accurate, coordinated and authorised emergency communication.

Communication arrangements will address workers, patients, communities, emergency services, partner organisations, government agencies, regulators, governing bodies and media where applicable.

Alternative communication methods will be identified for foreseeable telecommunications, internet or power failure.

Only appropriately authorised persons may make official statements on behalf of [Organisation Name].

5.22 Patient and Community Communication

Where an emergency affects service access or delivery, patients and communities will be informed as soon as reasonably practicable of relevant closures, service changes, alternative arrangements, access to urgent care and restoration of services.

Communication will consider local community needs, literacy, language, digital access, cultural communication pathways and the reliability of communication infrastructure.

5.24 Business Continuity Planning

[Organisation Name] will maintain a Business Continuity Plan appropriate to its critical services and identified risks.

Continuity arrangements will establish how essential functions will be maintained, adapted, prioritised, relocated, reduced, suspended and restored following disruption.

Strategies may include alternative facilities, outreach or mobile services, telehealth, modified operating hours, workforce redeployment, alternative suppliers, manual processes, alternative communications, reciprocal arrangements and staged restoration.

Continuity arrangements must not expose patients, workers or communities to unacceptable risk.

5.25 Service Prioritisation and Minimum Service Levels

Where full service capacity cannot be maintained, [Organisation Name] will prioritise services according to patient safety, clinical risk, community need, statutory obligations, minimum acceptable service levels and available resources.

Particular consideration will be given to patients whose health or safety may be disproportionately affected by disruption.

Where multiple services or systems require restoration, recovery will be sequenced according to agreed criticality, dependencies and risk.

Significant decisions to reduce, relocate, defer or suspend services will be authorised and documented.

5.26 Workforce Continuity

Emergency and continuity planning will address significant reductions in workforce availability.

Arrangements may include succession, identification of critical roles, cross-training, workforce redeployment, alternative rostering, remote work, temporary workforce arrangements and access to wellbeing support.

Fatigue, workload and psychosocial risks will be monitored during prolonged emergency operations.

Professional scope, credentialing, competence and patient-safety requirements will continue to apply.

5.27 ICT, Cybersecurity and Disaster Recovery

[Organisation Name] will maintain contingency and disaster recovery arrangements for critical ICT systems, telecommunications, electronic health records and organisational information.

Arrangements will address system outages, cyber incidents, internet or telecommunications failure, backup and restoration, alternative communication, downtime processes, data integrity, privacy, cybersecurity and prioritised restoration.

Critical systems will have appropriate recovery objectives informed by the BIA.

Where systems are compromised or suspected of compromise, restoration of service must not override necessary cybersecurity containment, investigation or safe recovery requirements.

Continuity arrangements will support essential operations where affected systems must remain isolated or unavailable for an extended period.

5.28 Critical Information and Records

[Organisation Name] will identify information and records required to support emergency response, continuity and recovery.

These may include:

- emergency contacts;
- delegations and authorities;
- facility and evacuation information;
- critical supplier information;
- insurance details;
- licences and regulatory information;
- patient-critical information;
- critical contracts;
- asset and equipment information;
- medicine and vaccine information; and
- business continuity and disaster recovery documentation.

Critical information must remain reasonably accessible during foreseeable ICT, telecommunications or power failure while maintaining appropriate privacy and security.

5.29 Utilities, Facilities and Infrastructure Failure

Contingency arrangements will address foreseeable failure of electricity, water, sewerage, telecommunications, internet, heating, cooling, ventilation, refrigeration, medical gases, building access, security systems, clinical equipment and other critical infrastructure.

Where facilities are unsafe or essential operating requirements cannot be maintained, affected activities will be modified, relocated or suspended.

5.30 Medicines, Vaccines and Temperature-Sensitive Products

Emergency arrangements will address protection and management of medicines, vaccines and other temperature-sensitive products.

Power failure, refrigeration failure, evacuation or prolonged disruption must trigger appropriate assessment and management.

Products must not be used where their safety, integrity or storage conditions cannot be assured.

5.31 Critical Suppliers and Third-Party Services

[Organisation Name] will identify suppliers and third-party services whose disruption could materially affect critical operations.

Continuity risk will be considered in procurement, contracting and ongoing supplier management proportionate to criticality.

Where appropriate, arrangements will address:

- alternative suppliers;
- minimum or contingency stock;
- service-level expectations;
- supplier emergency contacts;
- substitute products or services;
- alternate technology providers;
- logistics and transport;
- escalation arrangements; and
- supplier business continuity capability.

Critical reliance on a single provider will be treated as an organisational risk where appropriate.

5.32 Financial Continuity and Insurance

Emergency and continuity planning will consider financial arrangements necessary to maintain critical operations and support recovery.

This may include:

- payroll continuity;
- emergency expenditure;
- revenue and billing disruption;
- access to financial systems;
- emergency procurement;
- financial delegations;
- insurance coverage;
- records required for insurance or disaster assistance;
- cashflow implications; and
- significant recovery expenditure.

Emergency expenditure will remain subject to reasonable accountability, probity and retrospective oversight.

5.33 Emergency Procurement

[Organisation Name] will maintain appropriate mechanisms to support urgent procurement during emergencies.

Emergency delegations will provide sufficient flexibility for timely response while retaining reasonable documentation, accountability and financial oversight.

Material emergency expenditure will be reviewed following the event.

5.34 Emergency Resources and Equipment

Emergency resources appropriate to identified risks will be maintained, accessible and periodically checked.

Resources may include emergency communication equipment, first aid resources, evacuation equipment, emergency lighting, backup power, torches, batteries, PPE, water and other locally identified resources.

5.35 Vulnerable and Higher-Risk Persons

Emergency planning will consider people who may require additional assistance or experience disproportionate impacts during disruption.

This may include people with disability or mobility limitations, children, older people, people with cognitive impairment, people requiring regular treatment or medicines, people without reliable transport, people with limited English proficiency, people with limited digital access and people living in remote or isolated locations.

Planning will consider individual needs and available community and family supports and avoid inappropriate assumptions about vulnerability.

5.36 Recovery and Restoration

Recovery planning will commence as early as reasonably practicable during emergency response.

Recovery will address restoration of clinical and operational services, facilities, ICT, workforce capability, supplies, finances, community access and normal governance arrangements.

Restoration priorities will reflect patient safety, clinical risk, community need, business impact, system dependencies and minimum service requirements.

Recovery will not be regarded as complete solely because facilities or systems have reopened.

5.37 Recovery of Interrupted Healthcare

Following significant service disruption, [Organisation Name] will assess whether patients have experienced delayed, interrupted or missed healthcare requiring active recovery.

This may include:

- missed or cancelled appointments;
- overdue recalls and follow-up;
- outstanding clinical results;
- interrupted medicines;
- delayed immunisation;
- chronic disease reviews;
- antenatal, maternal or child health care;
- delayed referrals;
- mental health and social and emotional wellbeing care;
- preventive healthcare;
- unresolved urgent care needs; and
- patients identified as being at higher clinical risk.

Recovery activities will be prioritised according to clinical risk and documented through appropriate service and clinical governance systems.

5.38 Community Recovery and Re-Engagement

Where an emergency significantly affects the community, recovery arrangements will consider broader health and service impacts rather than solely restoration of organisational operations.

[Organisation Name] will, within its role and capability:

- assess changing community health needs;
- restore accessible healthcare;
- communicate service recovery clearly;
- re-engage people whose care was interrupted;
- identify emerging health or wellbeing impacts;
- work with Aboriginal organisations, community leaders and health-system partners; and
- consider whether particular communities experienced disproportionate impacts.

Recovery activities will support restoration of trust, access and continuity of care.

5.39 Fatality and Serious Injury

Where an organisational emergency results in, or may have resulted in, death or serious injury, [Organisation Name] will ensure appropriate emergency-service involvement, scene preservation where required, statutory notification, documentation, privacy, family communication, cultural considerations and worker support.

Responsibilities of police, coronial authorities, SafeWork NSW or other authorities will be respected.

The organisation will not undertake actions that compromise a lawful investigation.

5.40 Worker Wellbeing and Psychosocial Recovery

[Organisation Name] recognises that emergencies and disasters may create significant psychological and psychosocial impacts.

Worker wellbeing, fatigue, workload, exposure to trauma, prolonged uncertainty and other psychosocial hazards will be considered during response and recovery.

Workers affected by serious or distressing events will have access to appropriate support.

5.41 Community-Led and Culturally Informed Preparedness

Where appropriate, emergency preparedness and recovery will draw on local Aboriginal community knowledge, relationships, leadership and trusted communication networks.

Community knowledge may inform understanding of local hazards, access barriers, community priorities, vulnerable locations, communication approaches and recovery needs.

Engagement will be undertaken respectfully and in a manner consistent with the principles of Aboriginal community control.

5.42 Debriefing, Review and Organisational Learning

Significant emergencies, disruptions, activations and exercises will be reviewed proportionate to their seriousness and learning potential.

Review will consider, where relevant:

- preparedness;
- timeliness of activation;
- leadership and decision-making;
- situational awareness;
- patient and worker safety;
- service continuity;
- communications;
- workforce capability;
- facilities and infrastructure;
- ICT and cyber response;
- suppliers and dependencies;
- external coordination;

- community impact;
- cultural safety;
- recovery;
- missed healthcare;
- delays and failures; and
- opportunities for improvement.

Corrective actions will be assigned, monitored and evaluated for effectiveness.

5.43 Legislative, Regulatory and External Notification

[Organisation Name] will comply with applicable emergency-related notification requirements arising under legislation, regulation, public health requirements, privacy and data-breach requirements, work health and safety obligations, funding agreements and accreditation standards.

Notifications to emergency services, SafeWork NSW, NSW Health, public health authorities, privacy regulators, insurers, funding bodies or other authorities will occur where required.

Emergency conditions do not remove statutory reporting obligations unless otherwise provided by law.

5.44 Annual Emergency Preparedness Assurance

Emergency preparedness and business continuity capability will be formally reviewed at least annually.

Assurance will consider, as applicable:

- emergency risk assessments;
- Emergency Management Plan currency;
- Business Continuity Plan currency;
- Business Impact Analysis;
- emergency contact information;
- critical dependencies;
- training and emergency-control arrangements;
- exercises and drills;
- disaster recovery and backup testing;
- continuity arrangements;
- mutual-aid arrangements;
- critical supplier arrangements;
- outstanding corrective actions;
- organisational or service changes; and
- significant emerging risks.

Material preparedness gaps will be reported through appropriate governance structures and addressed according to risk.

5.45 Plan Currency and Accessibility

Emergency and business continuity plans, contact lists and supporting resources will be reviewed periodically and following significant organisational change, emergency activation, exercise or identified failure.

Critical emergency information must remain accessible during foreseeable ICT or power outages

Superseded emergency documentation will be managed through organisational document-control systems.

6. Roles and Responsibilities

Role	**Responsibilities**
Board / Governing Body	Provides governance oversight of significant emergency, continuity and resilience risks and receives assurance regarding organisational preparedness and recovery capability.
Chief Executive Officer	Holds executive accountability for emergency management and business continuity and ensures appropriate authority, resources, delegations and governance arrangements are maintained.
Executive Management	Leads emergency preparedness and significant organisational responses within delegated responsibilities and ensures critical services, continuity and recovery requirements are appropriately managed.
Emergency / Incident Management Lead	Coordinates organisational emergency planning, response arrangements, exercises, incident coordination and improvement activities as designated.
Managers / Service Leads	Maintain local preparedness, worker awareness, critical-function arrangements, continuity requirements and implementation of emergency directions within their areas.
Work Health and Safety / Emergency Control Personnel	Support workplace emergency planning, evacuation, emergency-control arrangements, drills, safety monitoring and applicable compliance requirements.
ICT / Information Governance Personnel	Maintain ICT continuity, cybersecurity response, backups, disaster recovery, downtime and information-protection arrangements.
Clinical Leaders	Ensure emergency and continuity decisions affecting healthcare appropriately consider patient safety, clinical risk, service prioritisation and recovery of interrupted care.
Finance / Corporate Services	Support financial continuity, emergency procurement, insurance, critical suppliers, facilities and organisational resource requirements within delegated responsibilities.
Communications / Authorised Spokespersons	Coordinate authorised emergency, stakeholder, patient, community and media communications.
All Workers	Understand applicable emergency arrangements, follow lawful emergency directions, report risks promptly and undertake emergency responsibilities within their role and training.

7 . Cultural Considerations

[Organisation Name] recognises that emergency management within an Aboriginal Community Controlled Health Service must reflect the organisation's responsibilities and relationships with Aboriginal and Torres Strait Islander people, families and communities.

Emergencies and disasters may disproportionately affect Aboriginal communities because of geographic isolation, infrastructure limitations, existing health inequities, transport barriers, digital exclusion, housing circumstances, disruption to culturally important places and services and historical experiences with government and mainstream systems.

Emergency preparedness, response and recovery will therefore:

- support culturally safe and respectful communication;
- recognise Aboriginal leadership and community control;
- involve Aboriginal workers, community representatives and cultural knowledge where appropriate;
- recognise family, kinship, community and cultural responsibilities;
- consider local knowledge and community priorities;
- avoid unnecessary separation of people from family, community and Country;
- consider access barriers when alternative services are established;
- use trusted and locally appropriate communication pathways;
- ensure emergency decisions do not create avoidable inequity in access to essential healthcare;
- identify and respond to disproportionate health impacts arising from service disruption; and
- consider cultural safety and equity during post-emergency review.

Where practicable, emergency planning should occur with communities rather than solely for communities, recognising the value of community knowledge, existing resilience, relationships and local leadership.

Cultural safety principles will also be applied respectfully to people from other cultural, linguistic and diverse backgrounds.

8. Related Policies & Documents

- Clinical Emergency Management Policy
- Clinical Governance Policy
- Organisational Governance Policy
- Risk Management Policy / Framework
- Work Health and Safety Policy
- Incident Management Policy
- Quality Improvement Policy
- Health Information Management Policy
- Information Security / Cybersecurity Policy
- Infection Prevention and Control Policy
- Medication Management Policy
- Immunisation Management Policy
- ICT Disaster Recovery Plan
- Cyber Incident Response Plan
- Emergency Evacuation Procedure
- Fire and Emergency Response Procedure
- Lockdown Procedure
- Critical Incident Management Procedure
- Pandemic / Infectious Disease Emergency Plan
- ICT Downtime Procedure
- Emergency Communications Plan
- Site-Specific Emergency Plans and Evacuation Diagrams
- Emergency Contact Register

- Communications Policy
- Access and Continuity of Care Policy
- Cultural Safety Policy
- Patient Rights, Responsibilities and Person-Centred Care Policy
- Emergency Management Plan
- Business Continuity Plan
- Incident Management Team Activation Guide
- Critical Supplier / Dependency Register
- Risk Register
- Recovery / Post-Incident Action Plan
- Business Impact Analysis

9. Monitoring & Review

[Organisation Name] will monitor implementation and effectiveness of this policy through organisational governance, risk management, work health and safety, incident management, business continuity, information governance and continuous quality improvement systems.

Monitoring may include:

- emergency and continuity risk assessments;
- Business Impact Analysis currency;
- critical functions, dependencies and single points of failure;
- Emergency Management Plan and Business Continuity Plan currency;
- emergency contact information;
- evacuation and emergency exercises;
- business continuity exercises;
- ICT backup and disaster recovery testing;
- cybersecurity exercises;
- emergency equipment and resources;
- workforce emergency training;
- ECO / warden arrangements;
- emergency activations;
- service disruptions and downtime;
- response and recovery performance;
- critical suppliers and infrastructure;
- mutual-aid arrangements;
- emergency communications;
- incidents and near misses;
- regulatory notifications;
- patient and community impacts;
- missed or interrupted healthcare;
- cultural safety and equity impacts;
- post-incident reviews;
- corrective actions;
- accreditation findings; and
- annual emergency preparedness assurance.

Significant risks, recurring deficiencies and preparedness gaps will be escalated through appropriate governance structures.

Corrective actions will have assigned responsibility and timeframes and will be monitored through to completion and evaluated for effectiveness.

Emergency preparedness and business continuity capability will be formally reviewed at least annually.

This policy will be reviewed every two years, or earlier following a significant emergency or disaster, activation of business continuity arrangements, material organisational change, legislative or accreditation change, major exercise, external review or identified system failure.

10. Breach of Policy

Failure to comply with emergency management or business continuity requirements may expose patients, workers, visitors, communities and the organisation to preventable harm and compromise the organisation's ability to maintain essential services.

Actual or suspected breaches, preparedness deficiencies or failures of emergency systems must be reported and managed according to the nature and level of risk.

Where an immediate safety or continuity risk exists, appropriate action must occur without delay.

Significant failures will be investigated or reviewed and externally notified where required.

Breaches may result in corrective action, education, reassessment of emergency arrangements, risk treatment, performance management or disciplinary action where appropriate.

Emergency incidents, system failures and identified deficiencies will also be used to support organisational learning and continuous improvement.

11. Appendix

Referenced Documents and Resources

The following external and internal resources have informed the development of this policy and procedure:

Document Title	Type	Location / Access
Work Health and Safety Act 2011 (NSW)	External	NSW Legislation – Work Health and Safety Act 2011 (NSW Legislation)
Work Health and Safety Regulation 2025 (NSW)	External	NSW Legislation – Work Health and Safety Regulation 2025 (NSW Legislation)

[Service Letterhead]

Document Title	Type	Location / Access
State Emergency and Rescue Management Act 1989 (NSW)	External	NSW Legislation – State Emergency and Rescue Management Act 1989 (NSW Legislation)
Public Health Act 2010 (NSW)	External	NSW Legislation – Public Health Act 2010 (NSW Legislation)
Privacy Act 1988 (Cth)	External	Federal Register of Legislation – Privacy Act 1988 (Federal Register of Legislation)
Health Records and Information Privacy Act 2002 (NSW)	External	NSW Legislation – Health Records and Information Privacy Act 2002 (NSW Legislation)
AS 3745 – Planning for Emergencies in Facilities	External	Standards Australia – AS 3745 (Standards Australia)
ISO 22301 – Security and Resilience – Business Continuity Management Systems	External	ISO – ISO 22301 Business Continuity Management Systems (ISO)
NSW State Emergency Management Plan (EMPLAN)	External	NSW Government – State Emergency Management Plan (NSW Government)
NSW HEALTHPLAN – NSW Health Services Functional Area Supporting Plan	External	NSW Health – NSW HEALTHPLAN (Health NSW)
NSW Health Emergency Preparedness and Overarching Plans	External	NSW Health – Emergency Preparedness (NSW Health)
Australian Government National Emergency and Crisis Management Plans	External	National Emergency Management Agency – National Plans (NEMA)
Australian Disaster Recovery Framework	External	National Emergency Management Agency – Australian Disaster Recovery Framework (NEMA)
National Disaster Risk Reduction Framework	External	National Emergency Management Agency – Disaster Risk Reduction (NEMA)
Australian Disaster Resilience Handbook Collection	External	Australian Institute for Disaster Resilience – Handbook Collection (AIDR Knowledge Hub)

[Service Letterhead]

Document Title	Type	Location / Access
Australian Emergency Management Arrangements Handbook	External	Australian Institute for Disaster Resilience – Emergency Management Arrangements (AIDR Knowledge Hub)
Community Recovery Handbook	External	Australian Institute for Disaster Resilience – Community Recovery (AIDR Knowledge Hub)
SafeWork NSW – Emergency Plans	External	SafeWork NSW – Emergency Plans (SafeWork NSW)
National Safety and Quality Primary and Community Healthcare Standards	External	Australian Commission on Safety and Quality in Health Care – Primary and Community Healthcare Standards (Safety and Quality in Health Care)
RACGP Standards for General Practices – 6th Edition	External	RACGP – Standards for General Practices 6th Edition (RACGP)
Australian Charter of Healthcare Rights	External	Australian Commission on Safety and Quality in Health Care – Australian Charter of Healthcare Rights (Safety and Quality in Health Care)
Essential Eight	External	Australian Cyber Security Centre – Essential Eight (Cyber Security Australia)
Essential Eight Maturity Model	External	Australian Cyber Security Centre – Essential Eight Maturity Model (Cyber Security Australia)
Essential Eight Assessment Process Guide	External	Australian Cyber Security Centre – Essential Eight Assessment Process Guide (Cyber Security Australia)
Notifiable Data Breaches Scheme	External	Office of the Australian Information Commissioner – Notifiable Data Breaches (OAIC)
Clinical Emergency Management Policy	Internal	Internal Document
Organisational Governance Policy	Internal	Internal Document
Work Health and Safety Policy	Internal	Internal Document
Risk Management Policy / Framework	Internal	Internal Document

Document Title	Type	Location / Access
Incident Management Policy	Internal	Internal Document
Quality Improvement Policy	Internal	Internal Document
Health Information Management Policy	Internal	Internal Document
Information Security / Cybersecurity Policy	Internal	Internal Document
Infection Prevention and Control Policy	Internal	Internal Document
Communications Policy	Internal	Internal Document
Access and Continuity of Care Policy	Internal	Internal Document
Emergency Management Plan	Internal	Internal Document
Business Continuity Plan	Internal	Internal Document
ICT Disaster Recovery Plan	Internal	Internal Document
Emergency Evacuation Procedure	Internal	Internal Document
Fire and Emergency Response Procedure	Internal	Internal Document
Lockdown Procedure	Internal	Internal Document
Pandemic / Infectious Disease Emergency Plan	Internal	Internal Document

12. Version History

Version	Date	Author	Change Summary
1.0	DD/MM/YYYY	[Your Name]	Initial draft