Business Continuity Management Policy

Purpose

The purpose of this policy is to demonstrate NSW Trustee & Guardian's (NSWTG) commitment to Business Continuity Management (BCM). This approach supports proactive planning and provides information to staff on how NSWTG's manages business disruptions through:

- the development of business continuity plans through defining critical business functions,
- performance of business impact analysis, and
- establishment of roles and responsibilities.

This policy should be read in conjunction with the BCM Procedure.

Policy statement

NSWTG's commitment

NSWTG is committed to implementing management strategies and processes that will manage possible crisis events that will impact all our business activities.

For this purpose, NSWTG is committed to:

- developing, implementing and maintaining the BCM policy and procedure by reviewing at defined intervals and when significant change occurs.
- managing risks and impacts following a disruptive event.
- developing, maintaining and exercising business continuity plans that address the organisational requirements.
- conducting business impact analysis inclusive of a risk assessment on an annual basis and when significant change occurs to critical business functions.
- complying with all applicable regulatory requirements.
- taking a risk-based approach to business continuity planning and prioritising activities that address the worst-feasible scenarios for NSWTG and its customers.
- effectively communicating information relating to incidents, disruptions or disasters to relevant NSWTG stakeholders.
- managing and responding to disruptions and incidents in a coordinated, consistent and sustainable manner.
- testing and reviewing the key inputs of the business continuity plans on an annual basis and when significant change occurs. This includes reporting the outcomes of the review to the Executive Leadership Team and the Audit and Risk Committee.

Objectives

NSWTG's response to a business continuity event is to maintain the key services for our customers by minimising the impact that a major disruption could have on the viability of the organisation. This includes:

- ensuring the welfare and safety of staff and customers.
- maintaining an appropriate level and minimising impacts to service levels.
- protecting the organisation's image and reputation.

- enhancing organisational stability.
- reducing risk exposures and potential economic losses.
- addressing legal responsibilities.

Requirements

The BCM policy and procedure is underpinned by the BCM plans outlined in Table 1 which enable NSWTG to plan for, respond to and recover from different aspects of a disruption or incident. Depending on the nature of the disruption, other specific plans may be developed such as for pandemics. The overall BCM structure and relevant documents are outlined in Figure 1.

Figure 1: **BCM Structure**

```
                        BCM Policy & Procedure
         ┌──────────────────┬──────────────────┬──────────────────┐
 Business Continuity    IT Disaster         Pandemic        Other specific plans
    Plan (BCP)         Recovery Plan      Management Plan
```

Table 1: **BCM Plans**

Plans	What is it?
Business Continuity Plan (BCP)	The BCP provides guidance and information to help teams respond and recover from a disruption affecting the property or staff at the Justice Precinct Offices, O'Connell Street offices or the Wentworth Avenue Client Specialist Centre. Branches currently operate under local arrangements and will be guided by the Business Continuity Team (BCT) during a disruption.
IT Disaster Recovery Plan (ITDRP)	The ITDRP serves as the guide for NSWTG IT staff to maintain IT services in the event of an interruption or restore IT systems and infrastructure in the event of a disaster or similar scenario.
Pandemic Management Plan	The pandemic management plan is developed to supplement NSWTG's business continuity by minimising potential pandemic impacts on customers and business operations.
Other specific plans	Depending on the nature of the threat or disruption, a specific plan may be developed to respond to the impacts on the organisation and its stakeholders such as a data breach.

Roles and Responsibilities

All NSWTG staff (including contingent labour) are responsible for contributing and participating in the identification, escalation to the relevant BCT member and management of business continuity related risks and incidents. Some staff also have specific responsibilities and accountabilities as set out below.

Chief Executive Officer (CEO)

The **CEO** is responsible for:

- overall accountability for NSWTG's BCM approach.
- approval of BCM policy and procedure as part of the corporate governance role.
- providing visible support and endorsement for the BCM procedure by communicating the importance of effective planning and promoting continual improvement.
- ensuring that appropriate financial and human resources are available to establish and deliver an effective BCM approach.

Executive Leadership Team (ELT)

The **ELT** is responsible for:

- overseeing the assessment and management of the risks of disruption to critical business functions for the division they are accountable.
- overseeing the development, maintenance and testing of BCPs at least on an annual basis to ensure that essential services can be maintained at an acceptable level during a major disruptive event and restored to full functionality within an acceptable timeframe. This includes review of the business impact analysis to ensure all relevant critical business functions are captured in BCPs.
- collectively reviewing and endorsing significant enterprise and operational changes as required.
- nominating a primary and alternative BCT member for their respective divisions and locations.
- integration of the BCM policy and procedure into the organisation's business processes.

Director Strategy & Governance

The **Director Strategy & Governance** is responsible for:

- approving the draft content of, and any subsequent amendments to, the BCM policy and procedure and distribute to the ELT for endorsement.
- overseeing regular reviews and testing of the validity, integrity and practicality of implementing the BCP, Pandemic Management Plan and any other specific plans as needed.
- providing updates on significant changes and report on the performance of BCP to the CEO, ELT and the Audit and Risk Committee.
- overseeing the regular review and assessment of the strategies outlined in the BCP including confirmation that adequate financial and human resources are available to implement the strategies.

Director Information & Technology

The **Director Information & Technology** is responsible for:

- overseeing regular reviews and testing of the validity, integrity and practicality of implementing the ITDRP.
- providing updates on significant changes and report on the performance of the ITDRP to the CEO, ELT and the Audit and Risk Committee.
- overseeing the regular review and assessment of the strategies outlined in the ITDRP including confirmation that adequate financial and human resources are available to implement the strategies.

Business Continuity Team (BCT)

The **BCT**, including the team leader are responsible for:

- understanding their BCT role and responsibilities and undertaking necessary training.
- responding to a crisis or business continuity event that may have the potential to impact on the organisation.
- participating in the regular reviews and testing of the validity, integrity and practicality of implementing the BCP and Pandemic Management Plan
- undertaking their business continuity functions in accordance with this policy and the BCM procedure.

BCT members

In addition to their BCT responsibilities, **BCT members** are responsible for assessing and notifying the BCT leader if a reported incident or potential disruption is identified at their location or division, depending on the nature of the incident.

Scope

The scope of business continuity covered by this policy includes all NSWTG business areas. It includes all staff (including contingent labour) within these business areas that:

- have designated responsibilities for business continuity planning and management activities.
- are affected by any major disruption.
- are responsible for undertaking actions or response to, a disruption.

Related resources

- Business Continuity Management Procedure
- Business Continuity Plan
- Pandemic Management Plan
- IT Disaster Recovery Plan
- Risk Management Policy
- Risk Management Procedure
- ISO 31000:2018, Risk Management Standard
- ISO 22301:2019, Security and resilience - Business continuity management systems requirements.

Definitions

Business Continuity Management: is an overall framework which focuses on the recovery of critical business processes to minimise the service delivery and financial impacts caused during a business disruption. It includes policies, plans, forms, and other processes.

Business Impact Analysis (BIA): is documented consideration of possible impacts on different business functions, including each function's priority, recovery time objective and the resources needed for recovery.

Crisis: an intense, unexpected and unstable state that disrupts normal operations, has highly undesirable outcomes and requires out-of-the-ordinary measures to restore order and normality.

Critical Business Functions: key business activities and processes that must be restored in the event of a disruption to ensure the ability to protect the organisation's assets, meet organisational needs, and satisfy regulations. These are business activities and information that should not be disrupted such that they impact the ability of the organisation to achieve its minimum business continuity objective.

Disruption: an event that interrupts normal business functions, operations, or processes, whether anticipated (e.g. hurricane, political unrest) or unanticipated (e.g. security breaches, blackout, terror attack, earthquake).

Incident: an adverse event that might cause disruption, loss or emergency, or lead to a crisis.

Risk: the effect of uncertainty on objectives. It is usually expressed as a combination of risk sources, potential events, their consequences and their likelihood.

Threat: a potential cause of an unwanted incident, which can result in disruption to business processes, harm to individuals, the environment or the community.

Document information

Title:	Business Continuity Management Policy
Owner:	Director Strategy & Governance
Approver:	Chief Executive Officer
Date of Effect:	24 May 2021