Business Continuity Management Policy

Purpose of this policy

This Business Continuity Management (BCM) policy outlines the requirements for the management of business continuity in the NSW Department of Planning and Environment (department).

The department is committed to implementing appropriate levels of business continuity preparedness to safeguard its people, stakeholders, office infrastructure, information technology, reputation and critical activities from the impact of incidents and disruptive events.

The policy complements the department's incident and emergency management procedures and associated plans, and its wider obligations under functional areas and sub / supporting plans of the NSW State Emergency Management Plan.

This policy defines the:

- commitment of senior executives to providing effective governance and leadership for BCM
- principles that underpin the approach to BCM
- scope of BCM in the department and across the Planning and Environment cluster
- roles and responsibilities of key positions to embed and maintain an effective BCM capability.

To whom this policy applies

This policy applies to all departmental employees, consultants, contractors and volunteers. It also applies to the employees, consultants and contractors of all entities that make up the Planning and Environment cluster who have employees employed in or through the department.

Policy statement

This policy requires the department to develop, implement and maintain a BCM Framework that covers its identified critical activities. Critical activities with a maximum tolerable period of disruption of up to 3 days are within the scope of the framework.

The related BCM Framework document defines how the department will implement BCM and the process to be used.

The principles of the department's BCM process:

- establish robust governance arrangements aligned with related business activities and the requirements of NSW Cyber Security Policy to enhance organisational resilience
- develop, implement and maintain a BCM Framework based on *ISO 22301:2019 Security and Resilience - Business Continuity Management Systems - Requirements*
- ensure that employees are trained in their preparation and response roles and responsibilities and have the necessary level of competence, authority and resources required

© State of New South Wales through Department of Planning and Environment 2022. Information contained in this publication is based on knowledge and understanding at the time of writing and is subject to change. For more information, please visit dpie.nsw.gov.au/copyright
DOC19/852470

- foster effective relationships with stakeholders to coordinate the response to a disruptive incident and support the continuity of critical activities.

Failure to comply with this policy

Ethical and behavioural standards are set out in the Code of Ethics and Conduct that you are expected to demonstrate while working with the department. If you fail to meet those standards, corrective action may be taken in accordance with the Code of Ethics and Conduct.

Review timeframe

Governance Division will review this policy no later than 3 years from the date the document is approved. The document may be reviewed earlier in response to post-implementation feedback, changes to legislation, or as necessary.

Related documents

Other related policies and documents that should be read in conjunction with this policy:

- Business Continuity Management Framework

Policy metadata

Table 1. Policy metadata

Category	Description
Status	Final
Date of approval	16 December 2021
Approver	General Counsel
Division	Governance
Policy owner	Executive Director Governance
Branch	Risk and Resilience
Document location	DPE Intranet and Internet
Next review date	December 2024
Associated procedure	Business Continuity Management Framework
Any additional applicability	Nil
Superseded document	DPIE BCM Policy V1.0 (March 2020) DFSI Business Continuity Management Framework FACS Business Continuity Management Policy and Framework SOPA Business Continuity Plan other legacy BCM documentation relating to in-scope DPIE cluster entities
Further information	business.continuity@dpie.nsw.gov.au
Document Reference	DOC19/852470

Version control

Table 2. Version Control

Version	Date issued	Change
1.0	March 2020	New document
1.1	December 2021	Minor factual changes to maintain currency and reflect DPIE policy template requirements
1.2	3 May 2022	Updated to reflect new branding and name change

Appendices

Appendix 1 – Roles and responsibilities

Table 3: Roles and responsibilities

Role	Responsibilities
Secretary	Provide leadership, commitment and resources to build BCM capability within the department
Group Deputy Secretary (or equivalent level)	Establish and maintain BCM capability within groups that identifies and safeguards critical activities and supports the response to disruptive events
Group Deputy Secretary, Corporate Services Group Deputy Secretary, People, Culture and Communications	Joint leads of the department's Crisis Management Team, activating and overseeing the response to crisis events on behalf of the Secretary Oversight of situation reports to, and liaison with, senior executives as part of the crisis management response
General Counsel	Senior executive sponsor for BCM policy in the department
Executive Director, Governance	Senior executive champion for BCM in the department Report to and advise senior executive managers on BCM issues
Director Risk and Resilience	Develop, manage and maintain the BCM Policy and Framework documents Report to the Audit and Risk Committee and other departmental committees as appropriate
Audit and Risk Committee	Ensure that an effective approach has been followed in establishing the department's BCM process in line with Internal Audit and Risk Management Policy for the General Government Sector – Treasury Policy and Guidelines Paper (TPP 20-08)
Manager, Business Continuity	Day to day coordination of BCM work across the department and support to groups, divisions and the Crisis Management Team (when activated)
Chief Digital and Information Officer	Maintain an ISO27001:2013 certified Information Security Management System, and the minimum controls and mandatory reporting requirements in the NSW Cyber Security policy Maintain Information Technology business continuity, IT service continuity and cyber incident response plans

Role	Responsibilities
Deputy secretaries, executive directors, directors, managers or business unit heads	Follow the instructions of the department's Crisis Management Team to undertake actions to support the response to and recovery from disruptive events
All employees	To be aware of and understand the components of the BCM process, including roles and responsibilities in the event of disruption

Appendix 2 - Definitions

Table 4: Definitions

Term	Definition
Activities	One or more tasks undertaken by, or for an organisation, that produces or supports the delivery of one or more products and services
Business continuity	The capability of the organisation to continue delivery of products or services at acceptable pre-defined levels following disruptive incidents
Business Continuity Management (BCM)	A holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its people, stakeholders, office infrastructure, technology, critical activities and reputation
BCM Framework	The ongoing management and governance process supported by an organisation and appropriately resourced to implement and maintain BCM
Business Continuity Plan	Documented procedures that guide the response and recovery of identified critical activities to a pre-defined level of operation following disruption
Business impact assessment	The process of analysing activities and the effect that a business disruption might have upon them
Crisis	A situation with a high level of uncertainty that disrupts the core activities and/or credibility of an organisation and requires urgent action
Critical activities	The activities identified in the business impact assessment process as critical to which priority must be given following an incident in order to mitigate impacts
Incident	A situation that might be, or could lead to, a disruption, loss, emergency or crisis
Maximum tolerable period of disruption	The time it would take for adverse impacts, which might arise as a result of not providing a product or service or performing an activity, to become unacceptable
Organisational resilience	The ability to anticipate, prepare for, respond to and adapt to incremental change and sudden disruptions, so as to continue to perform critical activities and the delivery of services to meet customer and stakeholder expectations
Senior executives	The Secretary, Group Deputy Secretary, Deputy Secretary, Executive Director and Director bands under the Government Sector Employment (Senior Executive Bands) Determination 2014

Term	Definition
Threat	A potential cause of an unwanted incident, which can result in harm to individuals, the environment or the community