

Business Continuity Policy

Top things to takeaway



Service Continuity

Ensures critical services continue during disruptive incidents.



ISO 22301

BCMS is certified to ISO 22301.



Critical Services Identified

Business Impact Analysis defines priorities, RTOs and RPOs.



Risk-Based Planning

Plans are developed using assessed business continuity risks.



Clear Response and Recovery

Documented invocation, incident response and recovery plans.



Tested and Improved

Plans are tested annually and reviewed by management.

Proprietary Notice

Information contained in the document is accurate to the best of Node4's knowledge at the time of publication and is required to be treated as confidential at all times. Information presented herein may not be used, copied, disclosed, reproduced, or transferred to any other document by the recipient, in whole or in part, without the prior written authorisation from a Node4 authorised representative.

Version control and ownership

Policy owner: Jenny Cooper

Version no	Date	What changed	Changed by	Approver
0.1	20/05/2024	Initial draft	Eddie Adams	Kate Lincoln
1.0	24/05/2024	Final review	Eddie Adams	Kate Lincoln
1.1	12/03/2025	Scope updated in line with recertification	Eddie Adams	Kate Lincoln
2.0	10/04/2026	Rebrand and annual review	Jenny Cooper	Eddie Adams

What is this policy for?

This Business Continuity Policy sets out the framework for Node4 to manage and respond to disruptive incidents and ensure the continuity of critical business operations. In line with Node4's certification, this policy aligns with the ISO 22301 standard for Business Continuity Management Systems (BCMS).

Who is this policy for?

This policy applies to Node4 Limited and all activities within the scope of the Business Continuity Management System (BCMS), including delivery of cloud, network/connectivity, cyber security, data management, and IT managed services.

It covers all Node4-owned sites included within the BCMS scope:

- DC1, Derby
- DC2, Derby
- DC3, Wakefield
- DC4, Northampton

All employees and relevant third parties who deliver or support these services must comply with this policy.

Contents

Top things to takeaway	1
Proprietary Notice	2
Version control and ownership	2
What is this policy for?	2
Who is this policy for?	2
Contents	3
Business Continuity Management System (BCMS)	4
Business Impact Analysis (BIA)	5
Risk Assessment	5
Disaster Recovery Plans (DRP)	5
Incident Response	6
Testing and Exercising	6
Management Review	7
Roles and responsibilities	7
Training & Communication	8
Related Documents	8

Business Continuity Management System (BCMS)

Node4 establish, implement, maintain, and continually improve a BCMS in accordance with the requirements of ISO 22301.

The Plan-Do-Check-Act (PDCA) model is applied to the planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness Node4's BCMS.

- **Plan** – Establishing business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with Node4's objectives.
- **Do** - Implementing and operating the business continuity policy, controls, processes and procedures.
- **Check** – Monitor and review performance against business continuity policy and objectives, reporting the results to management for review, and determining and authorizing actions for remediation and improvement.
- **Act** – Maintaining and improving the BCMS by taking corrective action, based on the results of management review and reappraising the scope of the BCMS and business continuity policy and objectives.



Business Impact Analysis (BIA)

Node4 conduct a BIA to identify critical business functions and the resources supporting them in order to determine continuity and recovery priorities, objectives and targets. The BIA includes assessing the impacts of disrupting activities that support the organization's products and services.

A review of the BIA will be undertaken annually or when a change occurs to ensure that Node4's BCMS remains up to date. This assessment will be undertaken by the Quality & Compliance team with the relevant management team members.

The BIA will include the following:

- Identifying activities that support the provision of products and services;
- Assessing the impacts over time of not performing these activities;
- Setting prioritized timeframes for resuming these activities at a specified minimum acceptable level, taking into consideration the time within which the impacts of not resuming them would become unacceptable;
- Identifying risks that could affect the continuity of the products and services, informing the risk assessment process.

Risk Assessment

Based on the risks identified in the BIA, an assessment will be undertaken to analyse and evaluate the risk of disruptive incidents to the organization.

The risk assessment will:

- Identify risks of disruption to Node4's activities and the processes, systems, information, people, assets and suppliers that support them;
- Systematically analyse risk considering the threats, impact and likelihood;
- Determine which disruption related risks require treatment;
- Identify treatments in line with business continuity objectives.

Risks will be documented and assessed through Node4's Risk Management Procedure.

Disaster Recovery Plans (DRP)

Based on the results of the BIA and risk assessment, Node4 develop Disaster Recovery Plans to ensure the continuity of critical business functions during a disruption.

These plans are in place to manage a disruptive incident and continue our activities based on recovery objectives identified in the business impact analysis.

DRPs will be documented and subject to annual testing and exercising.

The plans include:

- **Purpose and Scope** – the purpose of the plan and its scope, including which parts of the organization it covers.

- **Objectives** – outlines the objectives of the disaster recovery plan, such as the recovery time objectives (RTOs) and recovery point objectives (RPOs) for critical activities.
- **Roles and Responsibilities** – defines the roles and responsibilities of individuals or teams during a disaster recovery situation.
- **Resource Requirements** – detail of the resources required (people, technical, financial etc.) in order to meet the objectives.
- **Activation and Deactivation Procedures** – describes when and how the disaster recovery plan should be activated and deactivated.
- **Incident Response** – outlines the steps to be taken immediately after a disaster has been declared, including safety procedures and communication plans.
- **Recovery Procedures** – the steps to be taken to recover each of the organization's critical activities within the defined RTOs and RPOs.
- **Restoration Procedures** – the steps to be taken to restore normal operations once the immediate disaster situation has been resolved.
- **Training and Testing** – the training to be provided to personnel and the testing to be carried out to ensure the disaster recovery plan is effective and up to date.
- **Appendices** – may include contact lists, equipment lists, floor plans, checklists, and any other information that supports the disaster recovery plan.

Incident Response

Node4 will establish an incident response structure and procedures to manage and respond to disruptive incidents in the form of an Invocation Plan.

This plan includes the procedures and management structure to respond to a disruptive incident using personnel with the necessary responsibility, authority, and competence to manage an incident.

The Invocation Plan is in place to:

- Identify impact thresholds that justify initiation of a business continuity response;
- Assess the nature and extent of a disruptive incident and its potential impact;
- Activate an appropriate business continuity response;
- Detail processes and procedures for the activation, operation, coordination, and communication of the response;
- Have resources available to support the processes and procedures to manage a disruptive incident to minimize impact;
- Communicate with interested parties and authorities.

Testing and Exercising

The BCMS and business continuity plan will be tested and exercised to ensure their effectiveness.

All Disaster Recovery Plans, along with the supporting Invocation plan will be tested annually, or when a significant change occurs.

A formal post-exercise report will be created that contain outcomes, recommendations and actions to implement improvements.

Results will be reported as part of the Business Continuity Management Review in order to ensure progression of improvement opportunities and treatment of risks.

Management Review

Node4 Management review the BCMS once per year to ensure its continuing suitability, adequacy and effectiveness.

Management reviews consider the performance of the organization, including:

- Actions from previous management reviews.
- The need for changes to the BCMS, including the policy and objectives.
- Opportunities for improvement.
- Results of BCMS audits and reviews.
- Techniques, products or procedures, which could be used to improve the BCMS’ performance and effectiveness.
- Status of corrective actions.
- Results of exercising and testing.
- Risks or issues not adequately addressed in any previous risk assessment.
- Any changes that could affect the BCMS.
- Adequacy of policy.
- Recommendations for improvement.
- Lessons learned and actions arising from disruptive incidents.
- Emerging good practice and guidance.

Roles and responsibilities

Task	HoG	COO	Q&C	SLT	Employees
Who is responsible for complying with this policy		R	R	R	
Who is accountable for compliance to this policy	A				
Who needs to be consulted on this policy	C	C	C		

Who needs to be informed of this policy

I

Training & Communication

This Business Continuity Policy is made available to employees N4 Hub based on SharePoint, stored under the Governance site.

This Business Continuity Policy is also published on our website for access by relevant interested parties such as our clients.

All employees involved in incident response will be trained on the relevant policies and procedures that make up Node4's BCMS.

Related Documents

The following documents are related to this policy:

- N4 BCDR Invocation Plan.
- N4 Contingencies Plans.
- N4 Emergency Action Plan.