Report of Head of Decarbonisation

Subject: Business Continuity Plan, IT Disaster Recovery

Purpose of Report

To provide the committee with an update on the recent testing and review activities undertaken in relation to the organisation's Business Continuity Plan (BCP) and IT Disaster Recovery Plan (IT DRP) and creation of a new Cyber Incident Management Plan.

The report summarises the scope of testing, outcomes and recommendation to ensure ongoing resilience and compliance with organisational and the latest Business Continuity Plan (BCP).

Background

The BCP provides overall guidance for National Park staff in responding to any significant incident which interrupts normal business operations.

The Plan outlines the strategies and procedures to be implemented by the National Park Authority (PCNPA) in the event of a disruptive incident and aims to ensure the continued operation of essential functions and services, protect the well-being of staff and stakeholders, and mitigate potential risks.

Alongside the BCP sits the IT Disaster Recovery (ITDR) plan. Due to a significant amount of business activity relying on IT systems the ICT DR plan is also reviewed annually (or sooner because of identified changes) and sits alongside the BCP.

In line with policy requirements and good practice, both plans are subject to periodic testing and review to confirm their effectiveness, accuracy, and alignment with current operational arrangements.

Alongside these 2 documents a new Cyber Security Incident Management Plan (CIMP) has been created, which sets out how the Authority prepares for, detects, responds to, and recovers from cyber security incidents such as data breaches, ransomware, system compromises, or service outages. It is explicitly recommended by the National Cyber Security Centre that all public sector organisations should have a CIMP.

Testing and review

The recent testing and review activities included:

- A structured review of the BCP and IT DRP documentation to ensure accuracy, completeness, and alignment with current organisational structures, roles, and dependencies.
- Update of Emergency contacts
- Review of Communications plan
- Additional Cyber Incident Management Plan

A scenario based testing of the BCP, focused on the organisation's response to a major operational disruption – in this case a power outage.

Summary and outcomes

- The BCP was generally found to be fit for purpose and aligned with current business priorities.
- The Emergency Response Team demonstrated a clear understanding of their roles and responsibilities during the test scenario.
- Communication and escalation processes worked however could be further tested.
- Minor gaps were noted and have been actioned, led by the internal Business Continuity group. None of the issues identified are considered to pose an immediate or material risk; however, addressing them will further strengthen organisational resilience.

Revisions of the plan included addition of critical function prioritisation.
Updated IT DR plan to reflect key infrastructure upgrade and key contacts.
Addition of the cyber incident management plan.

Conclusion

The testing and review of the BCP and IT DRP provide assurance that the organisation is broadly well-prepared to respond to and recover from significant disruptions. Continuous improvement actions have been identified and will be implemented to enhance the effectiveness and robustness of the arrangements.

Recommendation
Members are asked to note the contents of the report and Plan.

Author: Jessica Morgan Head of Decarbonisation

Pembrokeshire Coast National Park Authority

Business Continuity Plan

Version: 2.0

Date: April 2026

Prepared By: Head of Decarbonisation

Approved By: Chief Executive Officer

Last Updated: October 2025

Table of Contents

Reviews
October 2023
October 2024
October 2025

1. Executive Summary

This Business Continuity Plan (BCP) outlines the strategies and procedures to be implemented by Pembrokeshire Coast National Park Authority (PCNPA) in the event of a disruptive incident. The BCP aims to ensure the continued operation of essential functions and services, protect the well-being of staff and stakeholders, and mitigate potential risks.

This document is distributed to and retained on encrypted USB by the Chief Executive, and Directors. A version is also retained within the fire safe at Llanion and Oriel y Parc.

2. Introduction

The PCNPA has many policies and procedures in place to minimise the possibility of an event or incident causing an interruption to the usual day-to-day operations. It is impossible to predict every possible type of business interruption, but usually the impact on the business, and the continuity procedures, will be similar regardless of the cause. In dealing with any incident, the health and safety of staff and members of the public is always paramount.

The likely events include loss of a key building, loss of power, loss of IT and communications, loss of staff, an event impacting on our ability to deliver our work or a need to respond to a national emergency. These incidents may be short lived or cause interruption over an extended period.

3. Objectives

The primary objectives of this BCP are:

- Ensure the safety and well-being of staff, stakeholders and public during emergencies
- Protect the Authority's assets and minimise any environmental damage
- Facilitate a swift recovery and return to normal operations
- Be clear about roles and responsibilities in:
    - Handling a disruption or emergency
    - Keeping up to date key supporting documents relating to IT, emergency contacts
    - Communicating the arrangements in place

This Business Continuity Plan provides overall guidance for PCNPA staff in responding to any significant incident which interrupts normal business operations. The intention is for the plan to be embedded in our day-to-day working practices, so

that a cycle of continual improvement involving analysis, planning, training, exercising and review of our approach is created.

This plan does not address how we respond to emergencies in the National Park, e.g., wildfires and outbreaks of animal or plant diseases as there are other processes, involving partners, in place for this type of emergency.

This plan aims to provide a framework to structure our response during an emergency and to provide guidance to an Emergency Response Team regarding the areas they will need to consider. It is not intended to act as a step-by-step guide covering all possible scenarios, but instead to provide the information required to form a plan of action relevant to a specific situation should an emergency occur.

By implementing the Business Continuity Plan, the Authority will be better prepared for disruptive incidents. Officers will examine the possible impacts of service disruption and make plans to respond to incidents.

The Management Team will review the plan annually. Interim updates will be issued if there are any significant disruptive events, changes to the organisation's structure/priorities, or alterations to the working environment. The business continuity plan is subject to periodical inspection by the Authority's internal auditors.

The plan considers potential risks that could impact the Authority and lays down steps for activation, management and co-ordination and responses. Some specific incidents are identified. This document should also be read in conjunction with the IT Disaster Recovery plan which outlines in-depth arrangements to maintain an IT system.

4. Risk Assessment

The services provided by the Authority are not considered as life threatening if not delivered, and an interruption of a few hours or even a few days, while inconvenient, should be acceptable in the event of a significant incident. However, the Authority has a responsibility to restore its services as quickly as possible. Any significant incident is likely to have a knock-on effect one other offices and services within the Authority.

There are several possible incidents/scenarios that might activate this plan, e.g.:

- Civil emergency (e.g., major incident affecting transport/communications systems)
- Significant weather event
- Illness among staff – pandemic
- Infrastructure collapse (including power, water, IT/ digital systems)
- Damage or restricted access to assets (including fire, accident or sabotage)

- Emergencies affecting other organisations and impacting on the Authority
- Severe injury/sudden death of a member of staff/volunteers or several staff/ volunteers
- Severe injury/death of a of a public participant in PCNPA activities and events and/or on the premises of PCNPA
- National emergency impacting on the work of the Authority.

Although the possible risks are wide and varied, they can be summarised under the following table:

Risk	What key resources/ functions / services would be impacted?	List arrangements already in place to reduce the likelihood or impact	Risk score
Loss of utilities, e.g., water, gas or electricity for periods of longer than 4 hours	All	• Home working for those who are able • Use of alternative Authority property in NP with internet connectivity • 365 accessed remotely (emails, sharepoint, Teams), 3CX telephones accessible remotely.	Low 2
Loss of systems (IT or telecommunications) and information	All	• IT Disaster Recovery Plan including infrastructure, business systems and electronic data backed up as well as hosted on the cloud • The Authority's legal interests in land, i.e freeholds and leaseholds are registered electronically with the Land Registry and saved in a fire resistant safe at Llanion • Emails can be accessed remotely. Telephones – 3CX can be accessed remotely and reception calls diverted.	High 6 / Medium 3
Majority of staff unable to work due to exceptional weather conditions, or widespread illness	All	• Cross training of skills across several individuals • Process mapping and documentation – to allow staff to undertake roles with which they are unfamiliar.	Medium 4

Loss of access to building(s)	All those operating from the premises lost	• Homeworking where possible • Copies of all legal agreements in fire resistant safe. All Authority land holdings registered electronically at the Land Registry • Use of alternative Authority properties within the National Park with IT connectivity • Capability of updating web and uploading committee papers off site • If longer than a short-term period, lease arrangements sought to cover interim.	Low 2
Severe injury or loss of life due to accident/incident	Any, plus impact on reputation	• Trained designated first aiders on sites • Major accident reporting and investigation procedure in place • HSE advice and support available. • Emergency communications plan in place • Emergency Services.	Medium 3
Loss of vehicles	All but generally Wardens, Rangers, RoW team	• Insurance • Use of pool cars • Hire vehicles.	Low 1

The risk score is based upon the following scale:

Likelihood of occurrence	**Severity**		
	(1)Acceptable (Little to no effect)	**(2) Tolerable** (Effects are felt but not critical to outcome	**(3) Undesirable / Intolerable** (Serious impact could result in disaster)
(1) Low - Improbable Risk is unlikely to occur	**Low 1**	**Low 2**	**Medium 3**
(2) Medium - Possible Risk will likely occur	**Low 2**	**Medium 4**	**High 6**

(3) High - Probable Risk will occur	**Medium 3**	**High 6**	**High 9**

5. Response and Recovery Strategies

5.1 Activation, Management and Co-ordination

First responder – any member of staff.

Any member of staff may be the first to identify an emergency or a disruption trigger especially if it occurs outside normal office hours. This person is expected to:

- Liaise with emergency services if appropriate
- Establish as many facts as possible
- Contact a member of the Management Team, in call up sequence: Chief Executive, Director, Head of Service. Should any event cause an interruption to business, then the relevant sections of this plan can be activated by the Chief Executive, or in his/her absence, by the most senior member of staff present.

This plan will be activated in the following circumstances:

A sudden onset incident causing significant disruption to most services which is likely to last for at least one working day.

Initial Action:

- If necessary, evacuate relevant site or sites

- Once the situation has been reported, the Chief Executive will convene a meeting of Emergency Response Team (ERT) which will consist of the two Directors, Head of Communications and additional personal depending on the incident. This team will assess the situation and provide a statement of intended action. If the Chief Executive is unavailable or incapacitated, this meeting will be convened by one, or both, Directors.

A foreseen/slow onset incident causing significant disruption to many services and likely to last for at least one working day:

Initial Action:

- Planning and risk assessment – relevant Line Managers to convene and assess the impact and implement mitigation measures, as necessary. Consider alternative working arrangements and communications strategy.

- Line Manager to report concerns to Chief Executive / Directors and priorities for support identified.

- If strategic management is required, the Chief Executive will convene a meeting of Emergency Response Team (ERT) to assess the situation and provide a statement of intended action. If the Chief Executive is unavailable or incapacitated, this meeting will be convened by one, or both, Directors.

Notification

If face-to-face communication is not possible, key officers will be notified using the cascade call-out system using e-mail, Teams or by telephone. Partners should be notified if the disruption is to be prolonged and/or relocation is required.

Administration and Logging
During the response to and recovery from a significant disruptive event, all actions undertaken by ERT must be noted in the incident log.

Finance and Insurance
The Head of Finance will be responsible for monitoring emergency expenditure during the response to a major incident. During a disruptive event, the Authority should have the capability to undertake all financial transactions with contingent systems being available. All emergency expenditure must be logged, to provide detail for insurance claims where applicable.

Where appropriate the Head of Finance will notify the Authority's insurers at the earliest possible junction of the nature of the incident. They will also be responsible for ensuring there is appropriate available insurance in place to cover a major incident.

6. Command and Control

Emergency Response Team (Strategic Level)
The Chief Executive will decide whether to convene a meeting of Emergency Response Team (ERT). This team will consist of the Chief Executive, two Directors and Head of Communications initially, with additional officers included as necessary, depending on the incident.

In the preliminary stages, ERT will

- Agree the strategy for recovery based on initial reports of the disruptive event
- Confirm the decision to invoke the plan or parts of the plan
- Confirm and agree a meeting/coordination location
- Identify an incident manager and confirm the appropriate Incident Response Team
- Identify a record keeper
- Agree an initial plan of action

- Agree timeline of communication, key messages, priority audience and channels of communication.

This initial meeting may be held in person or virtually, depending on timing and circumstance of the incident.

Business Recovery Teams
ERT will decide whether to activate a Business Recovery Team for the tactical management of the recovery process. Members of the team will depend on incident. In many cases, recovery may be managed as an operational response by Head of Department by adopting their specific Business Continuity Plans.

7. Communication Plan

Internal Communications
ERT will require an initial situation report from relevant line managers regarding the impact of the disruptive event on their service and how they are responding**.** Regular bulletins for staff and Members will be issued by the ERT. These messages will be broadcast by the most appropriate channel and may include PCNPA Chat on Teams, intranet, email, phone call, staff notices and cascade briefings. Detailed briefings, including key messages, will be provided for customer-facing staff, as required.

External Communications
The Head of Communications will prepare an initial media statement (and media briefing, if necessary), in consultation with ERT members. The Authority will provide public information using the most appropriate channel for the incident and audience involved, and may include website news updates, social media posts, press releases/statements and interviews.

8. Time Critical Activities

Activities to be given priority

Business Unit	Priority	Critical Functions	Mitigation if disruption occurs	Recovery to commence within
IT	H	Recovery of IT systems, servers, data, and telecoms network to all services	Paper recording of data.	1 day
Estates	M	Providing safe and functional facilities for officers,	Generators for emergency power,	1 day

		contractors, members, and the public	alternative facilities, and equipment	
Finance and Payroll	H	Payment to customers and staff	Manual Payment system	5 days
HR	H	Staff support	Temporary Recruitment	5 days
Customer Service	M	Reception	Web information, alternative help-point	1 day
Communications	H	Web, social media and media enquiries		1 day
Planning	M	Planning applications Planning enforcement	APAS – hosted Back up tapes	1 day
Democratic Services	M	FOI requests Committee meetings	Use back up tapes with information if servers down. Communicate with requested if likely to be delayed in response If website down for extended period paper copies of committee papers could be made available at key locations	20 working day timeframe for FOI's 1 day – particularly if Development Management meeting or National Park Authority meeting
Warden Team, PROW Team and Rangers Team	L	Ensure safety of relevant area of National Park	Use relevant powers to close relevant areas	1 day

Stand-down

This plan will be stood down when all affected Business Units have confirmed that disruption is no longer being experienced and the Chief Executive (or Director in his absence) declares the incident closed.

9. Response and Recovery Considerations

The following items may need to be considered by the Emergency Response Team. The list is not intended to be exhaustive, but instead should provide a framework for the Emergency Response Team to plan their actions.

	Consideration / Action	**Further Information / Details**
1	Public and staff/ volunteer safety	Do any buildings need to be evacuated? • Use emergency evacuation procedures and ensure all visitors / contractors are accounted for • Ensure all staff and volunteers assemble, are accounted for and remain assembled at normal assembly points • Consider alternative locations to direct staff/ volunteers to, or if they are to be sent home consider how, when and where they should next return to work or contact the Authority • Do you require the emergency services? • Record the names and details of any staff, volunteers' visitors or contractors that have been injured or distressed in the incident, or that may have lost personal belongings.
2	Start a log of activities, decisions and expenditure	Ensure that one or more individuals are tasked with keeping a record of the incident as well as the Authority's response and actions: • Roles and hours worked of those present in the Emergency Response Team • Decisions and actions taken during the incident • Financial Expenditure during the incident.
3	Assess the impact of the incident	Consider the implications, affected services, assets, and personnel. Consider initial responses and first actions to make safe any situations and to attempt to prevent any situation degrading further, which may include: • Closing sites or services • Temporarily disabling IT services and systems, including social media sites • Sending staff/volunteers to alternative locations or home if no alternative is immediately available

		• Providing skeleton staff for key services • Recovering equipment (if safe to do so) to aid further response and return to service.
4	Contact additional staff	Use the emergency contact list (Appendix 2) to contact additional members of staff if further support and expertise is required to respond to and deal with the incident.
5	Form an Emergency Response Team and an Incident Response Team	Form an Emergency Response Team to provide decision making and coordination during the incident. Form an Incident Response Team (recording the details in the appropriate log) to act in response to the incident, utilising further business plans such as the IT Disaster Recovery Plan where appropriate.
6	Consider wider and public communications to alert and inform appropriate audiences to the incident	Dependent upon the nature of the incident and the availability of staff, may include: • The enactment of a Communications Plan or delegation of communications to a part of the Incident Response Team • Briefing Customer Service Team / Communications Team with key messages for incoming customer and/or public contact • Briefing other public-facing services as appropriate (Rangers, Wardens, Centre Managers etc.).
7	Consider planning actions to restore critical or priority services or to form a skeleton service provision for critical areas	Consider: • Resources and expertise required, and how to secure those resources and expertise • Locations for operations and where different services need to interact closely • IT services required to support operations. • Continued communication with staff, volunteers, the public and other interested parties • Changing the use or displacing staff at other locations to facilitate accommodation for critical services and staff • Provision of skeleton or basic levels of service as a temporary measure either initially, or throughout the incident (dependent upon the nature of the incident).
8	Seek advice from outside bodies	Consider informing and seeking support from: • Insurance companies • Other National Park Authorities • Other Local Authorities • Other partner organisations that may be able to offer support • Dyfed Powys Police.

9	Consider financial management and monitoring, as well as standing orders and any other policies that may apply (including exemptions for emergency situations)	The Head of Finance will give directions on what is required to maintain or recover the necessary financial administration and treasury management systems, within the scope of Standing Orders and existing policies. In the event of the Head of Finance being incapacitated and unavailable, this role will be undertaken by the Chief Executive.
10	Consider functions that become critical the longer the incident and disruption to normal services lasts for	Consider: • The time of the month and year during which the incident has occurred and the impact for cyclical activities such as payroll and financial reporting • Whether any meetings (committee or other public meetings) were scheduled and whether these need to be cancelled or arranged at an alternative location • Statutory deadlines or timeframes that impact our work, such as planning determinations etc. • The reputational impact on the PCNPA as an organisation and for key personnel.
11	Consider planning longer term response to incident and how to return following an incident	Consider: • Additional workloads and resource requirements that teams may have following a prolonged period of disruption • Financial implications of any expenditure during the incident and the knock-on effects for planned expenditure • Recovery and replacement of any temporary measures that may have been put in place during the incident (such as temporary computers with basic configurations etc.) • Repair reputation and/or re-engage with employees, the community, visitors, partners • Review and updates to this plan following any lessons learnt.

10. Training and Awareness

This Business Continuity Plan is a critical tool for Pembrokeshire Coast National Park Authority to prepare for and respond to disruptive incidents. It is essential that all staff members are familiar with the plan and their roles in its execution. Regular

training, testing, and maintenance are essential to ensure its effectiveness in safeguarding our organisation and serving our communities.

Provide staff with the necessary training and awareness programs to ensure they understand their roles and responsibilities during an emergency. Conduct regular drills and exercises to test the BCP's effectiveness.

Regularly test and evaluate the BCP through tabletop exercises, simulations, and live drills. Identify areas for improvement and update the plan accordingly.

11. Document Control

A centralised repository for all BCP-related documents will be kept with the Chief Executive Officer, including this plan, emergency contact lists, and recovery procedures. Ensure that all documents are accessible and up to date.

12. Plan Maintenance

The BCP will be reviewed and updated annually, or as needed, to reflect changes in the organisation's structure, processes, or risks. Ensure that staff are aware of any revisions to the plan.

13. Appendices

Document Section	Owner	Review Schedule
Business Continuity Plan	Head of Decarbonisation	12 months
Appendix 1 IT Disaster Recovery Plan	Head of Decarbonisation	12 months
Appendix 2 Emergency Contact Lists	Human Resources	3 months
Appendix 3 Communication Plan	Head of Communications and Marketing	12 months

Review and Revision

Written and Approved by Audit Committee	October 2023
Reviewed no change	November 2024
Reviewed updated included priority order of critical systems Audit Committee April 2026	March 2026