The Highland Council
Business Continuity Management Policy

Version 1.0
Date: 2023

(For review 2025)

1. Introduction

1.1.

This policy provides the framework within which The Highland Council will ensure compliance regarding its duties in relation to Business Continuity, in accordance with statute and relevant guidance.

The Civil Contingencies Act 2004 established a legislative framework for civil protection in the UK and places clear duties on organisations preparing for and responding to emergencies.

Local authorities have a number of duties placed on them by the Civil Contingencies Act 2004 (Contingency Planning) (Scotland) Regulations 2005.

The Civil Contingencies Act is a framework that places several duties on local authorities to:

- Assess the risks of an emergency occurring and publish a Community Risk Register
- Prepare and maintain contingency plans to make sure we can respond effectively to an emergency
- Co-operate with other agencies to develop multi-agency emergency response
- Warn and inform the public
- Provide advice to the public

- Prepare and maintain plans to ensure continuity of our services during emergencies
- Promote business continuity to local businesses

The Act lays a duty upon Scottish Category 1 responders, including The Highland Council, to "maintain plans which relate to more than one emergency or more than one kind of emergency". This includes maintaining plans to ensure business continuity and to promote business continuity to local businesses and voluntary agencies. Planning focuses on key risks within the Community Risk Register which reflects nationally and regionally identified risks. Advice and guidance can be found on our website here: https://www.highland.gov.uk/info/1226/emergencies/72/resilience

1.2.

The Council's General Emergency Plans and topic specific emergency plans can be found here https://www.highland.gov.uk/info/1226/emergencies/72/resilience

The Corporate Risk Register identifies key risks for the Council and both mitigation and business continuity action plans sit beneath this. https://www.highland.gov.uk/info/20009/performance/795/corporate_risk_management

In addition to the Corporate Risk Register, recent Cyber workshops have identified a number (but not exhaustive list) of key critical services or functions which require a detailed Business Continuity Plan (BCP).
Critical corporate functions include those functions which, if interrupted for a period of 0-10 days, could have significant human health or financial or legal consequences.
See appendix 1

1.3.

The Business Continuity Institute has developed global guidelines on development of business continuity management to build organisational resilience. As part of those guidelines, they promote the formulation of a Business Continuity Management Policy.

The policy provides the framework for maintaining arrangements to ensure compliance with statute. It requires Executive Officers and Heads of Service to ensure that all functions within the service areas they lead are within the scope of a service area recovery plan and business continuity arrangements which must be reviewed and exercised regularly.

Guidance on developing business continuity plans can be found at **appendix 2**

2. Definition of Business Continuity

For the purpose of this policy, business continuity is defined as: **the capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident.**

In terms of Section 2 of the Civil Contingencies Act 2004 the Council must maintain plans for the purpose of ensuring, so far as is reasonably practicable, that if an emergency occurs the Council is able to continue to perform its critical functions.

Having well documented risk management and business continuity arrangements can contribute to savings in the Council's insurance premiums. Effective Business Continuity Management helps the Council to minimise the impact of any interruption to service delivery.

The policy should be reviewed every two years and updated to reflect best practice and changes to job titles, and any updates from the Business Continuity Institute.

The policy applies to all critical activities and functions across all services of the Council.

3. Policy Statement

The Council will maintain Business Continuity Planning which will:

- Have regard to:
  - The Business Continuity Institute Good Practice Guidelines.
  - Preparing Scotland – Having and Promoting Business Resilience.
- Ensure all services maintain plans and regularly test them, to minimise the impact to Council critical services and routine functions whilst responding to any emergency.
- Form part of corporate governance and performance arrangements within the Council.
  - Business continuity plans will be maintained and monitored as part of the Council's Performance Review and Management System (PRMS) and Risk Registers
- Ensure that all Council Staff and elected Members are:
  - Aware of this policy at a level of detail appropriate to their role and the requirement to comply with it.
  - Through the provision of appropriate resources (including management induction, training, guidance and support), enabled to fulfil any role they are assigned in connection with business continuity management.
- Where products or services are outsourced, ensure that conditions relating to the business continuity arrangements of providers are included in such a contract and such arrangements are included within the scope of the Council's business continuity plans.
- Ensure the capture of learning through testing of plans and from disruptive events through debrief and that this will inform revised plans.
- Ensure that BCPs are held centrally in Sharepoint, and in hard copy by Services

4. Benefits

This policy provides a clear commitment to business continuity management. During normal business and at times of heightened activity, effective business continuity will enable the Council to:

- Continue to provide critical services in times of disruption.
- Make best use of personnel and other resources at times when both may be scarce.
- Reduce the period of disruption to the Council and our communities.
- Resume normal working more efficiently and effectively after a period of disruption.
- Comply with standards of corporate governance.
- Improve the resilience of the Council's infrastructure to reduce the likelihood of disruption.
- Reduce the operational and financial impact of any disruption.
- Comply with its legal duties.
- Ensure learning from disruption informs review and updates to BCPs and any training

By promoting business continuity planning to the business community of the Highlands, overall resilience and effective recovery from emergencies will be improved.

5. Roles and Responsibilities

5.1.

The **Chief Executive** will retain overall responsibility for ensuring an appropriate and a proportionate response to emergencies. They will ensure that adequate resources are available to provide planning, advice, guidance, training and support to the management of all Council Services in discharging their responsibilities to Business Continuity.

5.2.

All Chief Officers will ensure:

- Business Continuity Plans are in place across their service areas and these are stored centrally, as well as held in hard copy within services https://highlandcouncil1.sharepoint.com/sites/GoldGroup/Business%20Continuity%20Plans/Forms/AllItems.aspx
- Adequate resources are made available within their respective service areas to maintain business continuity arrangements.
- Identification of a lead to coordinate business continuity arrangements within the service.
- Identification and review of critical corporate functions
- Business Continuity Plans are reviewed and updated every two years or as and when key circumstances change.
- Business Continuity Plans are exercised annually with a focus on key risks.
- All service staff are aware of and, where appropriate, trained in their role in any business continuity arrangements.
- Where products or services are outsourced, any contract is subject to considerations relating to the business continuity arrangements of the Council and the ability of the supplier to meet these conditions.
- Risks are appropriately identified in service risk registers and corporate risks are escalated to the Corporate Risk Register.
- A Business Impact Analysis is carried out in respect of their respective service areas. These analyses will be reviewed biennially or following a significant change:
    - To products or services relative to that service.
    - Outsourcing activity providing that product or service.
    - Service or Council priorities.
    - Legal or Regulatory requirement.

5.3.
The Communications and Resilience Manager will:

- Ensure that advice and guidance is promoted to local businesses and voluntary agencies through appropriate channels.
- Ensure that multi-agency emergency and resilience training and exercising and business continuity guidance is promoted to services.
- Ensure that emerging risks at national or regional risk register level are highlighted to the Corporate Risk Group.
- Ensure that a log of Resilience Training is maintained.
- The review of this policy biennially or following a significant change to its content.

5.4.
Strategic Lead (Corporate Audit & Performance) will:

- Ensure that any identified risks are reflected where appropriate on the Corporate Risk Register.
- Ensure that business continuity planning activities are subject to regular audit reviews.

Document control Sheet

Review/Approval Date	Version	Name	Position
September 2023	**V. 1.0**	**Kate Lackie**	**Interim Depute CEO**
September 2025			

File location: https://highlandcouncil1.sharepoint.com/sites/GoldGroup/Business%20Continuity%20Plans/Forms/AllItems.aspx
Author Ruth Rountree Provan, Communications and Resilience Manager

Appendix 1

Critical corporate functions identified through workshops and feedback (2021):

Critical functions	Lead Service	Link to BCP	Date exercised
ICT services/support	ICT		
Paying staff/Payroll	HR		
Communicating with key staff (and Admin)	All		
Communicating with all staff and members	Communications/Governance		
Children's Home/LAC Child Protection/referrals	H&SC		
Homelessness referrals	H&P		
Social work/client protection	H&SC		
Communicating with public	C&R		
Providing response to major emergencies	C&R		

File location: https://highlandcouncil1.sharepoint.com/sites/GoldGroup/Business%20Continuity%20Plans/Forms/AllItems.aspx
Author Ruth Rountree Provan, Communications and Resilience Manager

Providing out of hours emergency response **Roads** **Housing** **Social work** **ELGs**	 **E&I** **H&P** **H&SC** **C&P**		
Communicating with key partners	**All**		
Issuing Welfare Payments	**Revenues and Business Support**		
Revenue Collection	**Revenues and Business Support**		
Service centre telephony	**C&P**		
Education continuation/exams	**Education**		
Governance arrangements	**P&G**		
Burials/Cremations	**C&P**		
Website	**Digital Services**		
Elections	**P&G**		
Waste collection	**C&P**		

File location: https://highlandcouncil1.sharepoint.com/sites/GoldGroup/Business%20Continuity%20Plans/Forms/AllItems.aspx
Author Ruth Rountree Provan, Communications and Resilience Manager

Environmental Health functions	**C&P**		

Appendix 2

Guidance for developing Business Continuity Plans

Business continuity plans (BCPs), templates and guidance are stored in Sharepoint here:

https://highlandcouncil1.sharepoint.com/sites/GoldGroup/Business%20Continuity%20Plans/Forms/AllItems.aspx

Introduction

The purpose of a Business Continuity Plan (BCP) is to identify your priority functions and activities and consider how you would continue to provide these in the event the loss of:

- Significant Staffing shortages
- Key roles
- ICT
- Utilities (Power, water, phone lines etc) or “NETS failure”
- Infrastructure/buildings

A significant emergency could result in the loss of more than one of these for a period of time.

Templates are available for a detailed BCP and a simplified BCP. What is important is that all priority or critical functions are identified, impacts are considered and plans are drawn up to reduce risk and mitigate any potential impacts during disruption.

Cyber BCP

A Cyber attack would likely mean you would lose ICT – email, network, applications, and possibly phones/mobile access. It is possible you may only be able to use work mobiles to make and receive calls and SMS texts.

There will be considerable uncertainty in the timescales of loss of ICT and the extent. You need to plan for anything between 1 day and **many months** duration.

Your BCPs and supporting documents should be held in a printed copy and /or held on USB kept in a secure place in the event you are unable to access online files.

Priority Functions

All services must consider and identify their priority functions and any interdependencies and develop plans to mitigate the potential impacts.

A list of corporate priority functions has been identified and there must be BCPs for each of these as a minimum.

Cyber incident: Consider and identify your priority functions which require any element of ICT.

Consider what ICT applications you need to support these priority functions – including email, accessing passwords, contact details, logging in to applications and ICT your clients or staff use.

Priority functions should always include the following and details for how this will be done:

- Contacting your staff
- Contacting your service clients
- Contacting your key stakeholders/partners/external organisations
- Any functions which would have a serious impact on the welfare of clients or staff if interrupted for any length of time

Statutory/legal duties

Consider any statutory functions and what key personnel or ICT and contact details you need to carry these out. Consider whether there may be any derogation of these legal duties in the event of an emergency or Cyber attack. You could find this out in advance. Statutory bodies may have their own emergency or Cyber plans which take account of these arrangements. This should be stated in your BCPs.

Detail and impact

The likelihood and potential impact of the disruption will help to identify the level of risk.

Staffing: Consider the impact of losing a large number of staffing through illness or strike; and also the impact of any key staff with specific skills who may be a “single point of failure” in providing a service.

ICT: Explain what you use ICT to do and what impact losing ICT would have on your ability to carry out the functions and the impact on service users/others/staff and partners.

Consider timeframes and how this would affect or alter the impact. For example – an outage for 3 days may cause significant disruption or be simply inconvenient. A longer outage could have a financial impact and or welfare implications. A detailed business continuity plan asks you to consider ranking functions on the basis of those critical business areas which;

- Must be kept functioning 24/7 if immediate serious consequences are to be avoided (such as ICT)
- Could accept a business interruption of up to 3 days before having serious consequences, and
- Could accept a business interruption of up to 7 days before having serious consequences.

Focus your plans and mitigation on impacts which have greater risk of harm.

Consider what you or other staff should **stop** doing to focus on the highest priorities.

Consider which applications should be prioritised for bringing back first or for complete rebuild during a recovery phase.

Mitigation and Contingency

Staffing: What can you stop doing? What aspects could you prioritise and can you widen training to others?

Buildings and infrastructure: Detail what other buildings can be made available to carry out the function. For example; Loss of a school building in a fire – can you co-locate in another school or use a community centre? What assessments can you make in advance for space and equipment?

ICT: Can the function be provided alternatively without ICT? If not, how do you communicate that and who are your stakeholders. What are your messages?

Consider what you can do in advance to mitigate the impacts or to have alternative arrangements which can be put in place. Are there any possible “workarounds”? Who do you need to liaise with in advance to discuss arrangements.

Consider what interdependencies you have with other services or stakeholders (eg digital services, service centre, communications team, Finance, the Bank). Discuss these and ensure they know they are part of your BCP.

Consider what mitigations or contingency measures you can put in place. This may include the need to keep information stored elsewhere. It may include training of staff or use of alternative premises or resources.

Consider what passwords you need to access applications remotely – often to change a password you need access to your email and you may not have this. Do not use the BCP to list passwords – detail these separately and where they are stored.

Action Plans

Your action plan should detail **what** you need to do now to put these contingencies in place; a **timescale** for the actions to be completed; **who** is responsible for the actions; and **where** you intend to keep alternative resources such as contact lists.

An action plan should also detail what immediate actions are required in event of a cyber attack, for example – change passwords, contact staff, inform partners.

Also consider what non-urgent activities can be stopped, the impact of this and how staff can be diverted to other tasks; and what training or instruction manuals could you provide in advance?

Regular review and exercising is essential and can help to fine-tune your plans and ensure your staff know their roles and what to do.

Appendix 3

Further reading and research:

- Ready Scotland – Business continuity: https://ready.scot/prepare/business-continuity

- The Business Continuity Institute: The Business Continuity Institute (BCI) was established in 1994 to enable individual members to obtain guidance and support from fellow business continuity practitioners
- The Business Continuity Institute: Good Practice Guidelines - Guidelines that aim to provide a generic framework for BCM.
- Business Gateway - This website provides practical help, advice and support for new and growing businesses in Scotland, including guidelines and templates on Business Continuity planning.
- HM Government: Preparing for Emergencies - Practical, common sense advice on what businesses can do.
- A Guide to Business Continuity Planning for business and voluntary organisations

Short Cleveland and Redcar Video from 22 November training session:

https://web.microsoftstream.com/video/7d8d2a60-b36c-4f1a-a84c-b9b4a1e02e5a

Full Cleveland and Redcar Cyber Attack Lessons Learned video:

https://web.microsoftstream.com/video/a6cc007d-5689-4ed8-a29e-6ae483d01a04

SEPA Cyber Attack Lessons Learned – Dr David Pirie, Incident Manager (from yesterday):

https://web.microsoftstream.com/video/35ae83bc-41dc-4ce1-a119-51ad4b77abcd

SEPA Cyber Attack Lessons Learned – Terry A'herne, Chief Executive

File location: https://highlandcouncil1.sharepoint.com/sites/GoldGroup/Business%20Continuity%20Plans/Forms/AllItems.aspx
Author Ruth Rountree Provan, Communications and Resilience Manager

https://web.microsoftstream.com/video/b6fccdd2-3ae9-4053-a816-317edfae7c69

Cybercrime – Ready, Resilient and Responsive - https://web.microsoftstream.com/video/82ddf93d-c620-4b6d-bdf9-9f0a38a0dcb7