**YOUR LOGO**

[CENTRE NAME] Business Continuity Plan

DATE: XXX-202X

Version: X.X

Author(s)

|  |  |
| --- | --- |
| Name | Title |
|  |  |
|  |  |
|  |  |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Revision Date** | **Revised By** | **Summary of Changes** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Introduction to the Template 2](#_Toc112224451)

[1. Overview 2](#_Toc112224452)

[2. Chain of Command 3](#_Toc112224453)

[3. Risk Assessment and Response 3](#_Toc112224454)

[4. Core Business Systems 3](#_Toc112224455)

[5. Crisis Management Group 3](#_Toc112224456)

[6. Key Contacts 4](#_Toc112224457)

[7. Staff Contact Details 4](#_Toc112224458)

[8. Recording Incidents 4](#_Toc112224459)

[9. Training 4](#_Toc112224460)

[10. Review and Test of Business Continuity Plan 4](#_Toc112224461)

[11. Documentation and Location(s) 5](#_Toc112224462)

[Appendix A: Core Business Systems 6](#_Toc112224463)

[Appendix B: Crisis Management Group 7](#_Toc112224464)

[Appendix C: Key Contacts 8](#_Toc112224465)

[Appendix D: Staff Contacts 9](#_Toc112224466)

# Introduction to the Template

Each Centre can use this template to create their own Business Continuity Plan (BCP). Each heading has some exemplar content that must be tailored to and modelled by the Centre to reflect the Centre’s plans and strategy. Guidance for each section is given in upper case within square brackets e.g. [CENTRE GUIDANCE]. *Replace the words in the brackets with your own content as appropriate.* If parts of the plan and/or wording are not relevant to your business, please delete or adjust the wording as necessary.

# 1. Overview

[THIS SECTION IS GENERIC AND YOU MAY ONLY NEED TO INSERT YOUR CENTRE NAME WHERE INDICATED.]

Business continuity management is a holistic management process that identifies potential impacts that pose a threat to business and provides a framework for building resilience against them. It constitutes an effective response that safeguards the interest of its key stakeholders, reputation and revenue-generating activities.

These impacts - or ‘crises’ - include:

* Building or site incidents: for example, flood, fire and terrorist threats that affect access to or from buildings and sites
* Infrastructure incidents: for example, loss of power and communications (computer / telephone systems)
* Staff / operational incidents: for example, loss of key staff or critical documents
* Widespread environmental factors: for example a flu pandemic or fuel shortages
* Prevention and mitigation of Adverse Effects in order to protect Learners interests.

The primary objective of a BCP is to identify risks and outline how [CENTRE NAME] would manage operations under specific adverse circumstances. It will help [CENTRE NAME] to:

* To minimise interruption of normal operations
* To limit disruption and damage
* To minimise any financial impact
* To establish alternative means of operation

To train personnel in emergency procedures

* To provide smooth and rapid service restoration

# 2. Chain of Command

[THIS SECTION IS AN OVERVIEW OF WHO HAS EXECUTIVE AUTHORITY AND WHAT THE STAFF HIERARCHY OF YOUR CENTRE…WHO HAS AUTHORITY?]

Overall responsibility for business continuity in [CENTRE NAME] is held by [DIRECTORS, OWNER(S), ETC.] and, in their absence, operational managers and key service personnel. See Appendices B, C and D.

# 3. Risk Assessment and Response

Please see the [CENTRE NAME] ***Risk Register***, which is reviewed and updated monthly by the [DIRECTORS, OWNER(S), MANAGER, ETC.]

[CENTRE NAME] will outsource IT systems to ensure that major or catastrophic risks are mitigated as far as possible.

The chosen supplier will securely backup [CENTRE NAME] data to a UK location at least 25 miles from the primary site. Data will be backed up incrementally every day of the week and a full back up taken weekly by the supplier and all backups will be stored offsite. In this way, any major or catastrophic service outage will result in a maximum of 24 hours of data loss (restore full weekly back and then restore all incremental backups to that point).

# 4. Core Business Systems

Some areas are so critical that [CENTRE NAME] would not be able to function without them. We have assessed each of our core business processes and systems in terms of their criticality to [CENTRE NAME].

Please see Appendix A: Core Business Systems Table.

# 5. Crisis Management Group

If a major disaster occurs then [CENTRE NAME]’s Crisis Management Group (CMG) is mobilised to coordinate the business continuity plan. This team oversees invocation thresholds - when certain elements of the plan are enabled - and manages the relocation of business functions if necessary.

Designated CMG members are responsible for certain business systems and operations. They identify parties responsible for customer communications, internal communications, and supplier/vendor relations. Others may have responsibilities to communicate with the emergency services, utilities providers and, if necessary, the company’s insurers.

The **Chief Operating Officer** is responsible for convening the Crisis Management Group.

Please see Appendix B: Crisis Management Group Table.

# 6. Key Contacts

In the event of a disaster, we hold details of certain key contacts outside of [CENTRE NAME] who need to be alerted. These can vary according the type of disaster.

Please see Appendix C: Key Contacts Table.

# 7. Staff Contact Details

In the event of a disaster, we have a current record of all employees contact information so we can communicate with them. [CENTRE NAME] currently has [XX] staff.

Please see Appendix D: Staff Contact Details Table.

# 8. Recording Incidents

All major incidents and actions are recorded for future reference and in case there is a need for further investigation. These records also inform future business continuity planning and further risk mitigation actions.

# 9. Training

All staff and key personnel are made aware of their roles and responsibilities within the business continuity plan. (This is done as part of their induction, supervision or performance review). Their responsibilities include awareness of key policies and procedures, including the content of the business continuity plan itself. Staff and key personnel are encouraged to take personal responsibility to ensure they are familiar with the contents of the plan. They know who to contact in case of an incident, and how they can contribute to the plan’s implementation.

#  10. Review and Test of Business Continuity Plan

The [CENTRE NAME] Board conduct a comprehensive risk review annually. They submit their revised plans to the CMG for incorporation within the [CENTRE NAME] BCP.

After any major revision (such as supplier changes/hardware upgrades/etc.) the BCP is tested. There is a regular program of testing incorporated into the Regular Review Checklist, at 6 monthly intervals..

11. Documentation and Location(s)

Key Documentation is backed up remotely as well as backed up within the Cloud. This is a list of all key documents which are backed up by [CENTRE NAME] [MONTHLY/WEEKLY/DAILY/ETC.]

[ADD/DELETE/AMEND THE LIST BELOW AS APPROPRIATE TO YOUR CENTRE]

|  |  |
| --- | --- |
| Name of key document | Location |
| Business Continuity Plan including AppendicesOrganisational ChartAll [CENTRE NAME] PoliciesCentres HandbookLearner HandbookRisk RegisterLearner Records (inc. portfolios, etc.)Centres Contact ListFinancial Records |  |

# Appendix A: Core Business Systems

The following table identifies some of the main applications and line of business systems, their likely level of impact on operations and the planned responses to those risks. [THESE ARE EXAMPLES AND MUST BE REPLACED WITH YOUR SYSTEMS]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Priority** | **Service name** | **Service/product supported** | **Disaster Impact** | **Short Term Solution** | **Long Term Solution**  |
| High | Centre Admin System | RegistrationAdministration | Impair Centre communication with [CENTRE NAME][CENTRE NAME] cannot update admin requirements | Alert centres to alternative contact plansRevert to manual recording  | Restore systems on backup servers at alternate data centre within 72 hours. Update centres. Isolate issues, fix and restore systems to primary site when possible.Isolate issues, fix and migrate manual records back to cloud servers |
| Medium | Complaint & Appeals System | Administration | [CENTRE NAME] cannot update admin requirements | Revert to manual recording | Isolate issues, fix and migrate manual records back to cloud servers |
| Low | Back office systems | Finance / Marketing / IT | [CENTRE NAME] cannot update admin requirements | Revert to manual recording | Isolate issues, fix and migrate manual records back to cloud servers |
| High | Communication Systems | Phones / Website / Social Media | [CENTRE NAME] communication systems impaired | Contact Answering Service and alert them to issues | Isolate issues, fix and return calls |
| High | Quality Assurance Systems | Assessment, IQA, moderation. | Unable to assess qualifications in the agreed timescale | Revert to manual system. | Isolate issues, fix and migrate manual records back to cloud servers |
| High | Timely issue of Results and Certification | Administration | Unable to issue results and certificates in agreed timescales | Revert to manual system. | Isolate issues, fix and migrate manual records back to cloud servers |
|  |  |  |  |  |  |

# Appendix B: Crisis Management Group

Personnel should be listed in order of succession and include their primary role during a disaster.

[EXAMPLES LISTED BELOW. ADD YOUR STAFF NAMES AND RELEVANT DETAILS IN EACH COLUMN]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Position** | **CMG role** | **Contact numbers** | **Email Address** |
|  | Managing Director | Emergency Co-ordinator |  |  |
|  | Head of IT | IT and Data Recovery |  |  |
|  | Marketing Director | Internal / External Communications |  |  |
|  |  |  |  |  |

# Appendix C: Key Contacts

[FOR EXAMPLE: STAKEHOLDERS, LANDLORD, UTILITY COMPANIES, SERVICE USERS, SUPPLIERS AND INSURERS]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Company** | **Role** | **Contact Number** | **Email** |
|  | Company Insurance | [CENTRE NAME] Insurance | TBC | TBC |
|  | NLPQ | Awarding Organisation |  |  |
|  |  | Accountant |  |  |
|  |  | Legal Contact |  |  |
|  |  | Cloud Service Provider |  |  |

# Appendix D: Staff Contacts

Staff contact information and any roles they have.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Role** | **Contact Number** | **Mobile Number** | **Line Manager** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |