**YOUR LOGO**

BUSINESS CONTINUITY PLAN

Last updated XX/XX/XXXX by FirstName LastName

Template provided by Inoni on behalf of NFU Mutual

\*\*\*Rename a copy of this document CompanyName BCP. All blue text can be deleted from the copy \*\*\*

**Introduction**

This document is supplied by Inoni ([www.inoni.co.uk](http://www.inoni.co.uk)) on behalf of NFU Mutual to provide small businesses in the service sector with an easy to complete Business Continuity Plan (BCP) template.

Please note the template is not recommended for organisations with over 50 staff, those operating from multiple sites, or to meet specialised regulatory requirements. For these more advanced needs please contact your local NFU Mutual agent.

**How to use the document**

The following provides a baseline BCP suitable for a small service sector business with example text that you can easily adapt or replace. To complete the template, simply work through the document in the order it is written, reviewing the supplied information, deleting, inserting, and editing, as necessary. Guidance is provided for each section indicated by  icons. Once you are comfortable with your supplied content, you can delete/replace the blue help text, although you may like to keep a copy of the original template for future reference.

**Things to consider for your service sector business**

Service sector organisations often derive value from business continuity as it helps them identify potential recovery bottlenecks that otherwise remain invisible. Most rely on ready access to skills, information systems, consumables suppliers, and for some specialist equipment. Having a pre-considered recovery strategy addressing the loss of these could ensure you satisfy expectation and deliver service continuity through major incidents.

Depending on the type of service you provide, your customers may on the one hand be tolerant to disruption, contracted and willing/obliged to wait for recovery; or on the other, they may revoke the agreement and switch to a competitor almost immediately. If this is the case, you may face challenges returning to pre-incident levels of revenue.

For planning purposes, your priority is to understand your critical customers’ own situations, the services they rely on from you, and their tolerance to delay in provision before they penalise you in some way, damage your reputation, or look elsewhere. Your insight into their tolerance to loss of service, and your own tolerance to the resulting loss of opportunity, reputation, income and so on, drives the required pace of your recovery. It means that all the recovery strategies you devise must deliver an acceptable level of service within these timeframes.

Having survived the effects of Covid-19 lockdowns you may already feel that you are in a good place to survive any major incident. Formalising your business continuity plan will help you provide further assurance to your stakeholders and ensures coverage for all major risks. The chances are your challenges are no longer so closely tied to physical infrastructure, but you may still need access to specialised equipment. Similarly, most of your staff can now work from home comfortably, meaning any office-related incident is unlikely to have a major impact on your business.

However, you can now expect to rely more heavily on IT infrastructure and suppliers, which brings other risks into play around information security and IT service continuity. Having a strong IT Disaster Recovery Plan in place, as well as well rehearsed Crisis Management capability should now be a core aspect of business continuity planning and resilience.

## **Impact tolerance**

|  |  |
| --- | --- |
| Information with solid fill | Define how much impact your organisation can tolerate following an incident before you consider it to be unacceptable. This provides you with your own unique definition of what continuity risk means to your organisation and prevents you from including minor operational risks in the plan which don’t require a continuity response.Unacceptable impact is any that would prevent your organisation from achieving its long-term objectives. An impact of this scale requires you to change the operation of your organisation to survive. We generally define it in terms of Financial, Reputation, Production, Human, Regulatory impact contribution. |

The below table defines the levels and equivalence for the types of loss the organisation can sustain.

|  |  |
| --- | --- |
| **Impact Type** | **An unacceptable impact is…** |
| Financial | e.g. a major uninsured incident that leads to a drop of over 50% in annual profits |
| Reputation | e.g. where relations with stakeholders are badly affected, major loss of trust with customers and/or significant barriers to resumption and growth |
| Production | e.g. disruption that delays production/service for over 1 week, or major and widespread quality issues |
| Human | e.g. a health and safety incident on site that leads to serious injury or fatalities, or major and widespread product safety issues |
| Regulatory | e.g. legal or regulatory imposition that prevents us from trading |

## **Product recovery timeframes**

|  |  |
| --- | --- |
| Information with solid fill | Identify your critical products and services and estimate the required recovery timeframe of each. Think about how quickly you would need to recover it at different times of the year, i.e. at Peak and Off-Peak. Only include your most critical products whereby its loss threatens the continuity of the business. In Column C, list the critical processes that the product relies on. |

Our business-critical products and services are listed in this table. A critical product is any that is essential in satisfying a critical stakeholder requirement.

|  |  |  |
| --- | --- | --- |
| **Product** | **Required recovery timeframe** | **Processes that it relies on** |
| Service A | 1 week | Process A, B, C, D |

## **What does this mean for my plan?**

Completing the tables above give you the understanding you need to:

* Identify coinciding periods of increasing and peak exposure
* Identify at-risk products and risk sources that could lead to unacceptable loss
* Identify preventive and defensive (resilience) measures to reduce the risks you identify
* Identify scenarios you may want to explore or plan for
* Provide a timeline for the strategies you devise to recover from each scenario

With this information, your plan will be focused on responding to the key risks and/or recovering in acceptable time.

## **Continuity risk assessment**

|  |  |
| --- | --- |
| Information with solid fill | Based on your definition of what an unacceptable impact is, review the risks below and remove any that you feel wouldn’t impact you enough should they materialise in the worst case. If you can identify any that aren’t included below, add them at the end and estimate what their effect would be. |

Based on the impact tolerance defined in the preceding sections, the following continuity risks have been identified.

|  |  |  |
| --- | --- | --- |
| **Risk** | **Description** | **Effect** |
| Loss of office access | Catch all for any risks that could lead to loss of office access (flood, fire, power, water, internet etc) | Loss of office access |
| Loss of access to critical IT system | Loss of server environment or system failure leading to loss of access to critical applications | Loss of IT service |
| Data disclosure  | Cyber-attack or sabotage leading to theft and disclosure of sensitive data | Non-operational Crisis |
| Sabotage (IT) | Sabotage of IT by disgruntled employee  | Data breach |
| Ransomware | Malware that holds company data for ransom | Loss of IT service |
| Cyber attack | Attack leading to disclosure of sensitive data | Data breach |
| Widespread staff illness | Temporary loss of over 50% of a critical team through viral contagion or accident | Widespread loss of staff |
| Team defection | Permanent loss of over 50% of a critical team to a competitor  | Widespread loss of staff |
| Non-operational crisis | Incident that does not require operational recovery | Strategic risk |
| Systemic risk (e.g. Covid-19, Brexit) | Widespread effect or restriction leading to supplier or partner failure and reduction in activity | Strategic risk |

## **Continuity scenarios**

|  |  |
| --- | --- |
| Information with solid fill | After completing the table above, you will notice that you have a concise list of potential effects on your organisation in the third column. It is these scenarios that we write our recovery strategies for, in the knowledge that they provide a recovery for all identified continuity risks. You can define them further in the table below, by providing a description/assumption of the scenario effect, and a recovery timeframe based on your product recovery timeframes. |

Assessment of the risks faced by the organisation has led us to propose the following 'worst case' scenarios as the basis for our Business Continuity Plan. It is intended that by demonstrably defending against these scenarios, we should be well-positioned to respond acceptably to any sub-worst-case disruptions that arise.

|  |  |  |
| --- | --- | --- |
| **Scenario** | **Description/Assumption** | **Recovery timeframe** |
| Loss of office access | Loss of access to the office for an estimated period of 2 weeks | 1 day |
| Loss of IT service | Loss of access to critical applications  | 1 day |
| Data breach | Disclosure of sensitive data | 1 week |
| Widespread loss of staff | Loss of over 50% of a critical team for over 1 month | 1 week |
| Non-operational crisis | Incident that does not require operational recovery | Strategic risk |

## **Activity tracker**

|  |  |
| --- | --- |
| Information with solid fill | Making sure staff are aware of your BCP, trained where necessary and is proven to be effective are important aspects of the programme. We recommend annual review, training and exercise to provide adequate assurance to your stakeholders. You can plan/manage these activities below. |

All significant planned BCP activities are listed below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Activity** | **Description** | **Status** | **Date planned/completed** |
| Production/Authorisation | Development and sign off of BCP by leadership team | Completed | July 2021 |
| Training 2021 | Training of all staff with a role in the BCP | Planned | August 2021 |
| Exercise 2021 | Desktop simulation of one of the scenarios to ensure effectiveness | Planned | September 2021 |
| Review 2022 | Review and update of BCP | Planned | July 2022 |
| Training 2022 | Training of all staff with a role in the BCP | Planned | August 2022 |
| Exercise 2022 | Desktop simulation of one of the scenarios to ensure effectiveness | Planned | September 2022 |

## **Resilience improvements tracker**

|  |  |
| --- | --- |
| Information with solid fill | Having completed your plan, you should begin to think about how you can strengthen your organisation, addressing every risk you’ve identified and applying best-practice controls against it to reduce either the likelihood of the risk materialising, or the impact should it materialise. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **Improvement measure** | **Status** | **Date planned/completed** |
| Flood | Install bunding | Completed | July 2021 |
| Flood | Raise critical equipment off the floor  | Completed | July 2021 |
| Flood | Sign up to EA flood service | Completed | July 2021 |
| Flood | Develop flood response plan | Not started | December 2021 |

# Business Continuity Plan Structure

|  |  |
| --- | --- |
| EMERGENCY RESPONSE | Purpose is to SAVE LIVES and contain damage to business. Emphasis on practised capability |
| CRISIS MANAGEMENT | Purpose is to provide TOP-LEVEL DIRECTION and MAINTAIN CONFIDENCE in the business |
| BUSINESS RECOVERY  | Purpose is to resume ACCEPTABLE LEVELS of business operation by preparing and adapting |
| CONTACTS | Essential internal and external PEOPLE and ORGANISATIONS whose support may be required |
| ANNEX | Supporting DETAILED PLAN INFORMATION referenced from main plan sections |

# Role Definitions and Assignees

|  |  |
| --- | --- |
| Information with solid fill | Assign the following roles to available competent and qualified personnel |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Competencies required** | **Goals** | **Primary** | **Deputy** |
| INCIDENT MANAGER | Site knowledgePractical experienceDecisive and communicative | Managing the incident to closure Assessing the damage Escalating the response to Crisis Management and Recovery Managers if required Communicating all relevant developments to Crisis Management and Recovery Managers if required Liaising with the Emergency Services Ensuring governance and record-keeping Returning site to normal |  |  |
| CRISIS LEADER | Business knowledgeCustomer-facingDecisive and communicative | Leading the external crisis responseAnalysing the situation and positioning the business Upholding brand and reputation, creating confidence and certainty Providing a media figurehead and primary spokesperson Selecting, adapting and directing communications strategy Returning to normal |  |  |
| RECOVERY MANAGER | Production knowledgeOperational expertiseBusiness continuity trained | Directing the business operational response Deploying recovery strategyDeploying IT recovery strategy Delegating key tasksReturning to normal operation  |  |  |

# Emergency Response

## Flowchart

Immediately apply the following flowchart if in any doubt about an incident-related threat to safety or normal business activity

|  |  |
| --- | --- |
| Information with solid fill | Review the flowchart below and amend/adapt if necessary |

**INCIDENT**

**ARE YOU SAFE?**

**WHERE IS THE THREAT LOCATED?**

**FIND A SAFE PLACE INSIDE**

**GO TO PRIMARY EVACUATION POINT**

**ARE OTHER LIVES AT RISK?**

**EMERGENCY SERVICES CALLED?**

**DIAL 999 EMERGENCY SERVICES**

**IS THERE A THREAT TO BUSINESS?**

**ESCALATE USING THE PROCEDURE BELOW**

**CARRY ON AS NORMAL**

YES

NO

OUTSIDE

INSIDE

YES

NO

NO

NO

YES

**GO TO SECONDARY EVAC POINT**

**IS THE PRIMARY EVACUATION POINT SAFE?**

NO

YES

YES

## Staff checklist

Take the following steps to ensure your safety

|  |  |
| --- | --- |
| Information with solid fill | Review the checklist below and amend/adapt if necessary |

Raising the Alarm

* Your personal welfare is the absolute top priority. **Stay safe**; take no unnecessary risks
* In the event of an incident or accident, which requires the attendance of the emergency services ANYONE should immediately contact the relevant Emergency Services
* Dial 999 and respond to the questions being asked
* Immediately notify your Line Manager. If they are not available, notify the next available manager

If you are on-site and the alarm sounds

* Follow your manager’s instructions to evacuate the affected area to a designated muster point or go indoors as appropriate

If you are off-site e.g. at home and are made aware of an incident

* Remain contactable and stay near your normal phone number e.g. mobile / home
* For major incidents, listen to radio and TV for advice
* If you’ve heard of a disruption that you know is being dealt with, wait to be contacted
* ONLY when instructed by your manager, go to the site he/she identifies.
* Contact or meet with your manager and act on instructions

If you are approached by the media or any third party regarding an incident

* Obtain and formally verify the identity of the enquirer and log the interaction
* Politely but firmly decline to comment on the situation
* Refer the enquirer to the Crisis Leader
* DO NOT speculate or offer opinion
* Immediately notify the Crisis Leader of the enquiry

## Where to Go

If the alarm sounds, go to the first safely accessible Emergency Assembly Point for the location.

|  |  |
| --- | --- |
| Information with solid fill | Add assembly points for all sites in scope. Assembly Point A should be near to the site, with adequate space for all staff. Assembly Point B should be away from the site (preferably 400m), in case it is not safe to use Assembly Point A. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Location** | **Primary Assembly Point A** | **Map Reference A** | **Alternate Assembly Point B** | **Map Reference B** |
| e.g. High Street Office  | e.g. Front Car Park | Use <https://what3words.com/> and add location link here | e.g. Hotel Car Park | Use <https://what3words.com/> and add location link here |
| Add all sites in scope |  |  |  |  |

## Who to Call

Escalate to one of the management team below.

|  |  |
| --- | --- |
| Information with solid fill | Add contacts details for the management team |

|  |  |  |
| --- | --- | --- |
| **Role** | **Name** | **Contact Number** |
| e.g. Managing Director  |  |  |
| etc |  |  |

Decide whether to contact and mobilise the following suppliers (if material to the current response)

|  |  |
| --- | --- |
| Information with solid fill | Add any suppliers that might support you in containing an incident. Consider electricity, water, gas, internet, equipment maintenance, insurer, landlord, lawyers, IT managed service provider etc |

|  |  |  |  |
| --- | --- | --- | --- |
| **Type of supply** | **Company name** | **Contact name** | **Emergency Contact Number** |
| e.g. Electricity provider  | e.g. SSE |  |  |
| e.g. IT provider | e.g. Managed IT Limited |  |  |
| etc |  |  |  |

## Detection and Escalation

Immediately apply the following if you detect an incident or are notified that an incident may have occurred.

|  |  |
| --- | --- |
| Information with solid fill | Review the procedure below and amend/adapt if necessary |

**Incident Manager**



**Any staff member detects incident**

**Crisis
Leader**



**Recovery Manager**



**2. ESCALATE**

Notify Incident Manager or any manager

**3B. MOBILISE** if customers affected

**3A. MOBILISE** if operations disrupted

**1. DETECT**

Life or property at risk? Raise the alarm

**DIAL 999**

* **Detect** Any member of staff may raise the alarm if an incident has occurred or is imminent. If lives are at risk, **Dial 999** and notify Emergency Services
* **Escalate** You must notify the Incident Manager or any manager.
* **Mobilise** The Incident Manager mobilises the Recovery Manager and/or Crisis Leader. Apply guidance for each role

## How to contain specific incidents

Some incidents require a specific immediate response to contain their effects and may have associated detailed procedures. In any incident check the list below to determine how to respond. Use it as a guide to interpret the general response. If in doubt, refer to the Incident Manager.

Note the below provide initial responses only, you must refer to the Recovery Strategies as well for complete response.

|  |  |
| --- | --- |
| Information with solid fill | Refer to your [Risk Assessment](#_Continuity_risk_assessment) and consider whether any require specific incident responses procedures. We have provided some examples to help you |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Incident** | **Immediate Response** | **Preparatory measures**  | **Resulting Scenario** |
| Fire | * Sound the alarm
* Evacuate, and get staff to safe assembly point
* Advise staff not at site of the situation and advise not to come to site
* Make sure all staff are accounted for, if not advise Fire Services
* **Use Recovery Strategy in Section 3 for longer term response**
 | * Fire detection and suppression
* Regular cleaning and removal of clutter
* Complete a Fire Risk Assessment
* Fire safety training and fire drills
 | Destructive loss of site |
| Flood | * Receive flood warning
* Establish severity of flood, and adjust response accordingly
* Evacuate, and get staff to safe assembly point
* Advise staff not at site of the situation and advise not to come to site
* Make sure all staff are accounted for, if not advise Fire Services
* Safely shut down any equipment and isolate electrical equipment
* Raise or relocate key equipment and materials
* Prevent water from entering key areas and/or entire building
* Wait for flood to subside, or use water pumps
* Clean up and conduct a damage assessment
* Assess disruption timeframe
* **Use Recovery Strategy in Section 3 for longer term response**
 | * Bunding is in place
* Raised critical equipment off the floor
* Signed up to EA flood service
 | Denial of access to site |
| Power Failure | * Escalate to Incident Manager and maintenance manager
* Establish if outage is internal or external
* Evacuate, and get staff to safe assembly point
* Advise staff not at site of the situation and advise not to come to site
* Fail over to generator
* **Use Recovery Strategy in Section 3 for longer term response**
 | * Generator installed
* UPS for all critical IT hardware
 | Denial of access to site |
| Transport failure | * Escalate to Incident Manager
* Provide access to the site from another side if possible
* **If failure leads to denial of access use Recovery Strategy in Section 3 for longer term response**
 | * Multiple points of access identified
 | Denial of access to site |
| Widespread staff illness | * **Use Recovery Strategy in Section 3**
 | * Regular handwashing
* Hand sanitisers
* Regular surface cleaning
* Flu jabs
* Cross training
* Periodically inspect water systems for legionella
 | Widespread loss of staff |
| Cyber-attack / Ransomware  | * Confirm incident has occurred
* Establish severity of attack, and adjust response accordingly
* Identify the origin of the threat and gather intelligence about the activities being conducted during the incident
* Ring-fence and protect confidential information
* Resume service as quickly as possible
* Check integrity of the affected systems
* Preserve evidential integrity, where criminal activity is suspected
* **Use Section 3 for longer term response**
 | * Limit access to most valuable data.
* Employee education
* Cyber breach response plan in place
* Strong credentials and multi-factor authentication enforced where possible
* Sensitive data is encrypted
 | Loss of IT service |

# Crisis Management

## Command Centre Locations

|  |  |
| --- | --- |
| Information with solid fill | Add at least two options for command centres below. The Crisis Management Leader should gather their relevant team here to direct the external response.  |
|  |  |

Immediately adopt one of the following as the Crisis Command Centre.

|  |  |  |
| --- | --- | --- |
| **Option**  | **Address** | **Switchboard** |
| Microsoft Teams | Online | Add link to meeting here |
| High Street Hotel | 1 High Street | 01000 100 100 |

## Stakeholder Priorities

|  |  |
| --- | --- |
| Information with solid fill | Refer to the table in the Stakeholder Dependencies section at the beginning of this template. Add in any additional stakeholders who you might need to manage through an incident. |
|  |  |

Use the table below to inform and manage stakeholder and customer expectation

|  |  |
| --- | --- |
| **Stakeholder** | **What do they rely on from us?** |
| Customers | Service A |
| Staff | Health and Safety, Payroll |
| Investors | Return on Investment |

## Crisis Checklist

Adapt and apply the checklist. Gather all relevant decision information. Decide if a crisis response is required

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PRINCIPLES*** Protect and ensure the safety and welfare of staff and those affected
* Protect organisational assets, liquidity, reputation and environment
* Continue to supply products and services to customers
* Comply with relevant laws and regulations
 |  **RESPONSE SUMMARY**

|  |  |
| --- | --- |
| **DetectionActivation****Initial Meeting**  | Incident notification by any member of staff. Contact Incident Manager. Contact the Crisis Management Leader. Act to ensure staff safety and welfare Face-to-face OR telcon |

* Organise. Assign roles, responsibilities. Deputise where primary is absent
* Adapt the plan and agree a response strategy. Minute all Crisis meetings
* Assess damage and analyse impact. Agree timeframes and priorities
* Establish communications strategy. Notify key staff and management
* Mobilise business recovery teams. Invoke work area recovery if required
* Communicate with key stakeholder groups (customers, suppliers, agencies). Buy time
* Engage professional support for legal, media, insurance, financial response
* Agree timing and format for update meetings

|  |  |
| --- | --- |
| **Meetings****Stand Down**  | Observe the principles and follow the agenda Communicate the stand-down when incident is contained or ended |

 |
|  **AGENDA*** Situation report. Damage assessment and impact analysis
* Review the plan and confirm actions
* Review the strategy prioritisation and timeframes
* Communications
* Next meeting
 |
|  **INFORMATION and COMMUNICATION*** Where are we getting our internal/external information? How often is it updated?
* How current and reliable is it? Can key facts be corroborated? Do we believe it?
* Are we sharing information effectively? Is our decision-making consistent?
* What information do we need and how where can we get it?
* Who is coordinating the information process?
 |
| **ASSESSMENT*** What happened? When? How?
* Rate and direction of situation change?
* What parts of business are affected?
* What steps taken to contain the damage?
* Who is in charge? Incident Coordinator?
 |  **ANALYSIS*** What are the threats to business?
* What are our immediate priorities?
* What seasonal cyclic issues do we face?
* What is the worst-case outcome?
* How fast must we respond?
 |  **MOBILISATION*** What parts of the BCP do we activate?
* Who should be mobilised? On standby?
* CMT need to meet? When? Where?
* What is the core message?
* Who must we notify? Suppliers Clients?
 |  **RECOVERY** * Which recovery teams do we activate?
* What is the strategy?
* Have key roles been assigned?
* How is recovery funded resourced?
* Who owns this activity?
 |
|  **MEDIA*** Will there be media interest?
* Who will front the press conference?
* What are the messages to stakeholders?
* Do we need to engage media experts?
* Who owns this activity? Trained?
 |  **HUMAN WELFARE*** Are people affected? Who? How badly?
* Are they being cared-for? By whom?
* Can we account for all our people?
* What are we communicating to staff?
* Who owns this activity?
 |  **STAKEHOLDERS*** Which clients are will be affected?
* What service reduction will they tolerate?
* How what when will we communicate?
* Who owns this activity?
 |  **INSURANCE and LEGAL*** Will there be legal challenge?
* Do we need to act now or instruct staff?
* Insurers / legal counsel informed?
* Are we following their instructions?
* Who owns this activity?
 |

## Crisis Guidance

|  |  |
| --- | --- |
| Work at the speed of the crisis  | You cannot control external factors and risk being overtaken by events if you over-plan or wait for meetings or to observe protocol. Social media is near-instantaneous, and you must be on top of it at all times e.g. monitor Twitter |
|  Prepare for judgement calls | YES, you need the best possible decision information BUT the full information may not be available SO you need to compromise. Apply 80:20 but CONSIDER THE FULL RANGE OF OUTCOMES AND CONSEQUENCES |
|  Share high-grade information | MONITOR all forms of media constantly. BE AWARE OF the quality reliability age and relevance of the information at your disposal. Ensure essential others SHARE the same consistent decision information |
|  Respond early | You can BUY TIME by notifying third parties allowing them to prepare and invoke their own continuity plans. Involvement early reduces the likelihood of later shock and embarrassment |
|  Get external support | Crises are familiar to those who specialise in handling them. Engage experts to advise on critical decision areas including PR, Welfare Agencies, legal Counsel, Insurers, Loss Adjusters, Forensics. They may be able to provide additional resource. |
|  Keep focused | Focus on organisational position and perception. Take a strategic forward-looking view and provide direction BUT stay detached from internal operational recovery  |
|  Delegate  | Be prepared to hive off specific issues and problems and delegate to teams formed specifically for the task. Establish terms of reference, provide command and control, receive information via frequent reports |
|  Keep records | You MUST keep detailed records of all decisions and actions taken. These may be needed to support investigations, challenge lawsuits and evolve the crisis response. |

# Business Recovery

Apply the following steps to recover the business post-disruption

* Assess the situation and select the best-fit scenario. Check which if any of the assumptions are valid and related implications.
* Read the corresponding strategy from the list below. Adapt these to fit the situation.
* Modify the instructions to staff and reflect changes in the corresponding strategy diagram (below).
* Communicate to all involved staff. Mobilise and review as the situation develops.

## Recovery Strategies

|  |  |
| --- | --- |
| Information with solid fill | Referring to your list of Continuity scenarios completed in the introduction, take each one and populate them in the tables below. Copy the assumption, add all of the risks that are associated from the Risk Assessment and add the recovery timeframe. Then work with your team to develop your response to each scenario. Remember, you need to be able to recover an acceptable level of production to your customers within the set timeframe. |
|  |  |

The following record how we have decided to deal with each major scenario identified. Select the best fit strategy and systematically adapt it for circumstances. Communicate it fully.

|  |  |
| --- | --- |
| **Scenario** | **Loss of office access** |
| Assumption | Loss of access to site for estimated period of 2 weeks. |
| Identified risks | Fire, Flood, Power failure, Water failure, Internet failure, Regulatory breach, Transport failure, Neighbouring site incident, Fatality on site, Pandemic lockdown |
| Strategy | **Day 1**Identify and escalate using the procedures found in Section 1Contain using specific incident response (see Section 1)Damage assessment provided to Crisis Management and Business Recovery Manager by Incident ManagerEstimate length of outage and adapt response accordinglyInstruct all staff to work from homeStaff to advise Recovery Manager of any critical PC hardware or application access issuesNotify insurersDeploy crisis management plan and manage all affected stakeholders and customersClose and secure site**Week 1**Regular crisis meetings to manage any evolving situationsRecovery Manager to monitor operational levels, identify and escalate bottlenecks or delays in processRegain access |
| Recovery timeframe | 1 day |

|  |  |
| --- | --- |
| **Scenario** | **Loss of IT service** |
| Assumption | Loss of access to warehouse management system |
| Identified risks | Loss of access to critical IT system, Ransomware |
| Strategy | **Day 1**Identify and escalate using the procedures found in Section 1Damage assessment provided to Crisis Management and Business Recovery Manager by Incident ManagerContain and recover using specific incident response found Section 1 and IT Service Recovery procedures found in Section 3Deploy crisis management plan found in Section 2 and manage all affected stakeholders and customersUse manual workarounds for critical processes where possibleCommunicate outage to all staffRegain access to systemsCalibrate systems and validate before going back onlineStop manual workarounds |
| Recovery timeframe | 1 day |

|  |  |
| --- | --- |
| **Scenario** | **Widespread loss of staff** |
| Assumption | Loss of over 50% of a critical team for over 1 month |
| Identified risks | Widespread staff illness |
| Strategy | **Day 1**Contain spread by testing workforce and applying safety measures on siteIf permanent loss, recover through temporary agencies initially, then rehire permanent staffDamage assessment provided to Crisis Management and Business Recovery Manager by Incident ManagerNotify insurersDeploy crisis management plan found in Section 2 and manage all affected stakeholders and customersUse unaffected staff from other parts of the business for any critical processesProvide training if necessary**Week 1**Reduce service levels and communicate any delays with affected customersWait for recovery of staff |
| Recovery timeframe | 1 week at reduced service levels |

|  |  |
| --- | --- |
| **Scenario** | **Data breach** |
| Assumption | Disclosure of sensitive data |
| Identified risks | Sabotage, Cyber-attack, Human error |
| Strategy | **Day 1**Identify and escalate using the procedures found in Section 1Triage, validation and investigationLiaise with third-party suppliers as required for supportAdvise ICO of breachOrganise crisis responseNotify insurersPrepare legal response |
| Recovery timeframe | 1 week |

|  |  |
| --- | --- |
| **Scenario** | **Non-operational crisis** |
| Assumption | Reputation threatening incident that does not require operational recovery |
| Identified risks | Reputation related |
| Strategy | Use Section 2 of the BCP to organise your response. |
| Recovery timeframe | N/A |

## IT Service Continuity

The following provides a breakdown of critical IT systems and their recovery processes.

|  |  |
| --- | --- |
| Information with solid fill | Identify the IT systems that your critical services rely on. For each, detail how it is hosted and who relies on it. Work with the relevant teams to establish any manual workarounds to reduce impact should access be denied. Then detail the recovery process. |
|  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **System/application** | **How is it hosted?** | **Who relies on it?** | **Workarounds** | **Recovery process** | **Recovery time** | **Tested** |
| Finance system | Private cloud | Finance, Suppliers | Extend payment terms temporarily | Failover serverValidate | 1 day | Yes |
| Microsoft 365 | By supplier (SaaS) | All staff | Mobile phones for communication | Wait for supplier recovery | 1 day | Yes |
| HR System | By supplier (SaaS) | HR | Run payroll based on previous month | Wait for supplier recovery | 1 day | Yes |
| File storage | On-premise server | All staff | Offline files | Advise staff to keep manual records of files changesRebuild server Recover backupsRecover data backlogs | 1 day | Yes |

# Contacts

|  |  |
| --- | --- |
| Information with solid fill | Add critical contacts in the below sections. |
|  |  |

## Stakeholder Contacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Organisation** | **Contact Name** | **Role** | **Office** | **Out-of-Hours** | **Comment** |
|  |  |  |  |  |  |

## Supplier Contacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Organisation** | **Contact Name** | **Role** | **Office** | **Out-of-Hours** | **Comment** |
|  |  |  |  |  |  |

## Staff Contacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Location** | **Name** | **Business Role** | **Mobile** | **Relevant Competencies** | **Location** |
|  |  |  |  |  |  |

## **Supporting information and procedures**