****

|  |
| --- |
| **(Example) Business Continuity Strategy** |
|  |
| **Version:** Business Continuity Strategy **Date of Board sign off:** **Date for Review:**  |
| **Responsible Lead:**  |

**Aim of this Strategy**

The aims of this strategy are to provide XXXXXX (name of organisation) with the ability to effectively respond to scenarios and situations which place the organisation at risk or threaten its core functions. It intends to outline the planning, preparatory and recovery activities XXXXXX (name of organisation) will take to ensure that the critical business functions will either continue to operate despite serious incidents or disasters or will be recovered to an operational state within a reasonably short period. For XXXXXX (name of organisation) effective Business Continuity requires three key elements to be considered:

1. **Resilience**:

That the Critical Business Functions and the supporting infrastructure are designed and engineered in such a way that they are materially unaffected by most disruptions.

1. **Recovery**:

That arrangements are identified and enacted to recover or restore Critical and less Critical Business Functions that fail for some reason (whether through error, infrastructure failure, natural disaster or deliberate malice).

1. **Contingency**:

 XXXXXX (name of organisation) establishes a capability and readiness to cope effectively with whatever major incidents and disasters occur, including those that were not, and perhaps could not have been, foreseen. Contingency preparations constitute a last-resort response if resilience and recovery arrangements should prove inadequate in practice.

This strategy will therefore identify the mechanisms by which XXXXXX (name of organisation) will be resilient to, recover and/or identify contingency should situations occur which disrupt Business Critical Functions (BCF’s).

The XXXXXX (name of organisation) Crisis Management Plan is linked to this strategy – reference should be made to this plan where there is a need for reactionary or mitigatory activity to effectively respond to a situation or time of intense difficulty or danger where important decisions need to be made. The XXXXXX (name of organisation) Crisis Management Plan defines the Crisis Management Team (CMT)

**Our Vision**

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

**Our Mission**

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

**Our Corporate Goals**

**Goal One:**

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

**Goal Two:**

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

**Goal Three:**

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

**Goal Four:**

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

**Business Continuity Plan (BCP) Objectives**

1. **Resilience**
	1. To define and prioritise the **Critical Business Functions (CBFs) of XXXXXX (name of organisation) and evaluate the emergency risk to business**
		1. Identify Emergency Response Coordinator (ERC)

*Glossary of Terms for Organisation Contacts (Examples)*

|  |  |
| --- | --- |
| **ERC** | Emergency Response Coordinator (Designated by Organisation) |
| **CHR** | Chair to Board |
| **ARC** | Audit and Risk Chair (or similar e.g., Business and Risk, Finance etc |
| **FD** | Finance Director  |
| **BSM** | Business Support Manager (or similar) |
| **CEO** | Chief Executive Officer ( or General Manager) |
| **HR** | HR Director ( or partner) |
| **SGL** | Safeguarding Lead |
| **PerfM** | Performance Manager |
| **PartM** | Participation Manager |
| **EL** | Education Lead |
| **CL** | Communications Lead |
| **EQL** | Equality Lead |
| **LA** | Legal Advisor |
| **EM** | Event Manager |

1. **Recovery**
	1. To document the **procedure for** **responding to an emergency**
2. **Contingency**
	1. To ensure that all **staff are trained** annually and understand how:
		1. to **deliver the required response to an emergency** and to continue their Critical Business Functions outside of normal operating procedures.
3. **Objective 1: Resilience**

There are 5 categories of scenarios/situations which may have negative impact on XXXXXX (name of organisation) capacity to perform Critical Business Functions. Each situation has been rated High (H), Medium (M), or Low (L) for risk (likelihood of the situation occurring) and impact (criticality of event).

* 1. **Critical Business Functions of XXXXXX (name of organisation) , evaluation of risk and identification of Emergency Response Coordinator (ERC)**
		1. **Category 1: Business**

An incident which adversely impacts on XXXXXX (name of organisation) position, reputation, brand, or reduces workforce morale or productivity.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Impact** | **Rag** | **Scenario/Situation** | **ERC** |
| M | H |  | Loss of Exchequer Funding | CHR/CEO/FD |
| H | M |  | Loss of Commercial investment | CHR/CEO/FD |
| L | H |  | Fraud or unethical behaviour by an individual | ARC/CEO |
| L | H |  | Financial mismanagement | CHR/CEO/FD |
| M | H |  | Serious legal issue i.e., litigation, criminal activity, discrimination | CHR/CEO/LA |
| M | M |  | Significant negative media and/or internet coverage | CEO/CHR/CL |
| M | M |  | Regional currency or political crisis | CEO/CHR |
| M | H |  | Staff redundancies | CEO/FD/HR/CHR |

* + 1. **Category 2: Information**

The unauthorised disclosure or compromise of confidential information or personal data that would likely have a negative impact on the company’s reputation, brand, or cause them to breach Data Protection legislation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Impact** | **Rag** | **Scenario/Situation** | **ERC** |
| M | H |  | Personal data compromised  | CEO/BSM |
| L | H |  | Financial information compromised | CEO/BSM |
| M | H |  | Loss of Hardware containing personal, HR and/or financial information | CEO/BSM |
| L | H |  | Partner Data breach e.g., payroll provider | CEO/BSM |

* + 1. **Category 3: Information Systems**

An incident or threat which affects information systems confidentiality, integrity or availability.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Impact** | **Rag** | **Scenario/Situation** | **ERC** |
| H | H |  | Virus or other malicious code attack | CEO/BSM/ |
| M | H |  | Denial of Service attack | CEO/BSM/ |
| M | H |  | Compromise of system confidentiality through hack | CEO/BSM/ |
| L | M |  | Password loss for key systems and files | CEO/BSM |
| M | M |  | Computer crime e.g., clone of website | CEO/BSM/CHR |
| L | L |  | IT centre failure i.e., fire, power failure | CEO/BSM |
| M | H |  | Risk of catastrophic system failure | CEO/BSM |

* + 1. **Category 4: People**

A situation which impacts on the safety, security or productivity of XXXXXX (name of organisation) employees.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Impact** | **Rag** | **Scenario/Situation** | **ERC** |
| L | H |  | Death or serious injury that is work-related | CEO/CHR |
| L | M |  | All staff sickness | CEO/BSM |
| L | M |  | Workplace violence | CEO/CHR |
| L | H |  | Bomb threat | See *Table 1* |
| L | H |  | Mass departure | CEO/CHR |
| L | H |  | Abuse allegation or charge | CEO/CHR |
| L | H |  | Multiple death or serious injury at event (athletes, coaches, volunteers) | CEO/CHR |
| L | H |  | Terrorism effecting a XXXXXX (name of organisation) location | See *Table 1* |
| L | H |  | Terrorist attack at an event  | See Table 1 |
| M | M |  | Breach of privacy | CEO/ARC |

* + 1. **Category 5: Property**

A natural or human-caused event which affects the facilities or operational continuity of XXXXXX (name of organisation)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Impact** | **Rag** | **Scenario/Situation** | **ERC** |
| L | M |  | Natural disaster i.e., floods, hurricane, earthquake | See *Table 1* |
| M | M |  | Fire or explosion |
| L | H |  | Eviction from office locations | CHR/CEO |
| M | M |  | Vehicle accident  | CEO/BSM |
| L | L |  | Severe weather i.e., thunderstorm, heavy snow | CEO/BSM |

*Table 1:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Location** | **Bomb Threat** | **Terrorism** | **Natural Disaster**  | **Fire or explosion** | **Eviction** |
| **ERC** | **ERC** | **ERC** | **ERC** | **ERC** |
| **Location A e.g., Offices** | CEO/BSM | CEO/BSM | CEO/BSM | CEO/BSM | CEO/CHR/FD |
| **Location B****e.g., Performance Site**  | CEO/BSM/PM | CEO/BSM/PM | CEO/BSM/PM | CEO/BSM/PM | CEO/CHR/FD |
| CHR TO BE MADE AWARE  |  |

1. **Objective 2: Recovery**
* Key Personnel required to lead the response to emergency situations (the Emergency Response Coordinator (ERC)) are identified in 1.1 a. – e.
* In the event of a situation occurring which is documented within this Plan, the ERC should be contacted immediately. If the ERC is not available, then the CEO (or in their absence the Chair of the Board) must be contacted immediately.
* Actions linked to the situations identified in 1.1 are in the Organisation’s **Action Matrix** (Appendix 1)
	1. **Procedure for Responding to an Emergency**
		1. For all emergency response situations please:
			1. Keep a log of immediate actions taken
			2. Contact the emergency services (if required and in line with common practise)
			3. Contact the Emergency Response Co-ordinator (ERC) identified for that situation (see 1.1. a. – e. above for ERC)
	2. **The ERC will then:**
		+ 1. Keep a log of actions taken (see **Appendix 2: Action Log**)
			2. Convene/contact the Emergency Response Team (ERT = CEO/Chair/ERC and (if applicable) appointed Legal Partner/Financial Consultant/Media Consultants as required by scenario/situation)
			3. Identify the functions disrupted
			4. **IF SAFE TO DO SO** identify damage
			5. Provide information to Board/staff
			6. ERC to agree a course of action (in consultation with additional partners/emergency services if required)
			7. Communicate decisions to staff and relevant partner organisations
			8. Provide information to the public to maintain reputation and business
			9. Arrange response review/debrief
			10. Post-emergency, review/amend Business Continuity Plan

|  |
| --- |
| **If an emergency occurs affecting any of the XXXXXX (name of organisation) premises, then please follow the building health and safety/evacuation procedures.**  |

1. **Objective 3: Contingency**

Scenario/Situation training will take place annually and may be conducted by XXXXXX (name of organisation) or by a partner organisation.

* 1. **All staff are trained to understand how to respond to scenario/situation and to continue critical business functions**

The XXXXXX (name of organisation) team will be trained according to the categories of Critical Business Function identified in Section 1.1:

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Training area** | **Provider** | **Training Opportunities** |
| 1. Business
 | * Vision, Mission, Values and Behaviours
* Staff Handbook
* Financial Procedures
* Equality Act 2010
 | * CEO
* CEO/HR
* CEO/FD
* CEO/HR/external partner
 | * Induction
* Discussion in team meetings
* Specific training sessions
* Awareness of Policy
 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Training area** | **Provider** | **Training Opportunities** |
| 1. Information
 | * Data Protection Act and GDPR
* Data Protection Policy
* Financial systems (for those who use them)
* Personal safety and security
 | * CEO/partner
* CEO/BSM````
* FD
* CEO/HR/external partner
 | * Discussion in team meetings
* Specific training sessions
* Awareness of relevant Policy
 |
| 1. Information Systems
 | * GDPR
* IT security
* Mobile Phone Policy
* Data Breach Policy and processes
 | * External partner
* Tech Solutions
* CEO
* CEO
 | * Discussion in team meetings
* One-to-one with Technology Solutions
* Awareness of relevant Policy
 |
| 1. People
 | * Welfare and Safeguarding Policy and Toolkit
* Equality/Equity Policy
* Diversity Strategy
* Facility Business Continuity and Crisis Management Plans
* Staff Handbook
 | * SGL/ External partner
* CEO/EQL
* CEO/BSM/Facility Partner/s
* CEO/HR
 | * Safeguarding Vulnerable Adults/Safeguarding Children & Young People
* Equity and Diversity workshops
* Emergency procedure training
* Discussions in team meetings
* Induction
* scenarios
 |
| 1. Property
 | * Business Continuity and Crisis Management Plan
* Health and Safety at work
* Drivers Policy
 | * CEO/BSM/Facility Partner/s
* CEO/HR/External Partner
 | * Discussions in team meetings
* Specific workshop
* scenarios
 |

The team will also receive training on the XXXXXX (name of organisation) **Action Matrix** identified in **Appendix 1**. All training will be followed up with scenario sessions to check understanding and support familiarity with processes.

**Appendix 1: XXXXXX (name of organisation) Action Matrix**

**Category 1: Business**

|  |  |  |
| --- | --- | --- |
| **Scenario/Situation** | **ERC** | **Action** |
| Loss of Exchequer Funding | CEO/FD | * Board approved Reserve policy to provide for redundancy payments
 |
| Loss of Commercial investment | CEO/FD | * Financial Contingency Plans identified annually to include loss of Commercial investment
 |
| Fraud or unethical behaviour by an individual | CEO/FD/LA | * All staff to be aware of Financial Procedures Policy

**Immediate Action*** When identified report to bank and (and potentially) police
* Follow Disciplinary Procedures
 |
| Financial mismanagement | CEO/FD/Chair | * Financial Contingency Plans identified annually
* Follow Financial Procedures Policy
* Include Financial update on all Audit & Risk/Finance and Board meeting agendas
* Follow appropriate Disciplinary Procedures where appropriate and report criminal activity if necessary
 |
| Serious legal issue i.e., litigation, criminal activity, discrimination | CEO/CHR/LA | * Ensure all staff are aware of relevant policies e.g., Bribery and corruption, Diversity Strategy and Equity, Whistleblowing policy
* Report suspected legal issues to the appropriate authorities (Police or Professional Bodies)
* Take legal advice from Company Solicitors
 |
| Significant negative media and/or internet coverage | CEO/CHR/CL | * Board Communications Lead or co-opted PR expert to mitigate against risk and respond to emergencies
* Staff who may need to liaise with media are supported by PR company
 |
| Staff redundancies | CEO/FC/HR | * Contingency for redundancies included within the Risk and Reserves Policy
 |

**Category 2: Information**

|  |  |  |
| --- | --- | --- |
| **Scenario/Situation** | **ERC** | **Action** |
| Personal data compromised  | CEO/CHR/ARC/LA | **Immediate Action*** Follow GDPR processes and complete Breach Report Form
* Report Breach to the ICO
* Report breach to all staff effected
 |
| Financial information compromised | CEO/CHR/ARC/LA | **Immediate Action*** Follow GDPR processes and complete Breach Report Form
* Report Breach to the ICO
* Report breach to all staff effected
 |
| Loss of Hardware containing personal, HR and/or financial information | CEO/CHR/ARC/LA | **Security measures in place.*** Check security protocols with Technology Solutions (Server provider, IT hardware and software), website provider and/or portal provider, Bank provider (internet banking).
* Utilise specialist advice and support where relevant (legals)
* No staff to make internet purchases without advising CEO first
 |
| Partner Data breach e.g., payroll provider | CEO/CHR/ARC/LA | **Immediate Action*** Contact partner and identify full extent of the breach
* Follow GDPR processes and complete Breach Report Form
* Report Breach to the ICO
* Report breach to all staff affected
 |

**Category 3: Information Systems**

|  |  |  |
| --- | --- | --- |
| **Scenario/Situation** | **ERC** | **Action** |
| Virus or other malicious code attack | CEO / BSM | * Risk of confidential materials being accessed contrary to Data Protection legislation

**Immediate Action*** Contact IT Provider and report attack
 |
| Denial of Service attack | CEO/BSM |
| Compromise of system confidentiality through hack | CEO/BSM |
| Password loss for key systems and files | CEO/BSM  | * Risk of confidential materials being accessed contrary to Data Protection legislation

**Immediate Action**Contact IT Provider and report attack |
| Computer crime e.g., clone of website | CEO/CHR/BSM | * Take legal advice regarding closing down clone website
* Identify clone website disclosure on organisation website
 |
| Loss of telecommunications | CEO/BSM | * All staff have access to mobile phones, emails and social media which should act as alternative communication methods for the duration of the failure.
 |
| Power failure | CEO/BSM | * Report failure to host of building in which failure has occurred
* Officers are mobile and can work from alternative premises
 |
| Risk of catastrophic system failure | CEO/BSM | * Server checked daily under contract – currently no back up to server, all cloud-based.
* Check all Financial information is held separately and updated weekly.
* All Staff carry laptops with information stored remotely from office.
 |

**Category 4: People**

|  |  |  |
| --- | --- | --- |
| **Scenario/Situation** | **ERC** | **Action** |
| Death or serious injury that is work-related | CEO/CHR/HR | * Impact on staff morale.
* Support all staff as appropriate through systems and partnerships
 |
| All staff sickness or threat (virus etc) | CEO/BSM/HR | * Inform Chair – communicate to key partners temporary disruption
 |
| Workplace violence | CEO/CHR/HR | * Staff to report any incidences of harm to CEO or if in immediate danger to emergency services.
* Policies in place to protect staff from harm.
 |
| Bomb threat | See *Table 1* | **Immediate response*** Staff to follow host building procedures and ensure familiarity with personal safety recommendations.
 |
| Mass departure | CEO/CHR/HR | * Managers conduct one-to-ones with their staff
* Performance Management system in place
* Board emergency meeting
* Conduct ‘exit’ interviews with all staff to identify reason. Apply relevant policy to address any issues identified.
 |
| Abuse allegation or charge | SGL  | * Ensure all staff engaging in regular and unsupervised activity (regulated activity) have a current safeguarding check.
* Ensure all staff have attended appropriate training and are familiar with reporting processes

**Immediate Action*** Follow organisation Safeguarding policies and apply Toolkit.
* . High impact on company/brand reputation.
 |
| Risk of harm/abuse at event/competition to athlete, coach or volunteer | SGL | * Ensure event / event partners have undertaken risk assessment undertaken to mitigate against risk. Company /brand reputation at risk.
 |

|  |  |  |
| --- | --- | --- |
| **Scenario/Situation** | **ERC** | **Action** |
| Catastrophic event incident | CEO/CHR/EM | * Ensure event manager/event partners have undertaken risk assessment to mitigate against risk.
* Ensure event has an appropriate Emergency Action Plan and Emergency Operating Procedures.
 |
| Terrorism effecting an Organisation location | See *Table 1* | **Immediate response*** Staff to follow host building procedures and ensure familiarity with personal safety recommendations.
 |
| Terrorist attack at an event  | CEO/CHR/EM | **Immediate response*** Staff to follow Events procedures and ensure familiarity with personal safety recommendations.
* ERC to ensure role call
 |
| Breach of privacy | CEO/ARC/LA | * Ensure Data Protection Policy is applied and all GDPR processes are followed.

**Immediate Action*** If there is a Data Breach – follow Data Breach Policy, record breach using a Breach Report Form and if it meets threshold report to the ICO
 |

**Category 5: Property**

|  |  |  |
| --- | --- | --- |
| **Scenario/Situation** | **ERC** | **Action** |
| Natural disaster i.e., floods, hurricane, earthquake | See *Table 1* | **Immediate evacuation*** Staff to follow building Health and Safety procedures for office base effected. ERC to check safety of all colleagues within office base.
* Staff to work from alternative premises
 |
| Fire or explosion | **Immediate evacuation*** Staff to follow building Health and Safety procedures for office base effected. ERC to check safety of all colleagues within office base.
* Staff to work from alternative premises
 |
| Eviction from office locations | * Staff to temporarily work remotely from home/offices
 |
| Theft from office locations | **Security measures in place.*** Never to leave doors unlocked.
* Risk surrounding out of hours access to offices for cleaners identified on Risk Register
* All personal belongings to be taken from the office at the end of each day by the owner
* Where personal belongings and corporate items of value are left in the office overnight, they should be kept out of sight and ideally in a locked cupboard or draw.
 |
| Vehicle accident  | CEO/BSM/HR | * Ensure all drivers are aware of the Driver Policy
* Ensure all Drivers are appropriately insured and have had their Drivers licence check

**Immediate Action*** Ensure driver and passengers are safe and report incident to emergency services if required
* Report accident to insurers
* Record accident with CEO
 |

|  |  |  |
| --- | --- | --- |
| **Scenario/Situation** | **ERC** | **Action** |
| Severe weather i.e., thunderstorm, heavy snow | CEO/BSM | * Staff all able to work remotely and access IT
 |
| Unable to access/leave building | See *Table 1* | * Await instructions from Building Managers
 |

**Appendix 2: Action Log**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name:** | ……………………………………………………………………………………………………………… | **Role:** | ……………………………………………………………………………….. |
|  |
| **Description of Crisis Situation:** |  |
|  |
| **Date Crisis identified:** | …………………………………………………….. | **Time Crisis Identified:** | ……………………………………………………….. |
|  |
| **Date** | **Start Time** | **Finish Time** | **Issue** | **Action taken** | **Key people** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Appendix 3: Key Personnel Contact information**

|  |  |  |  |
| --- | --- | --- | --- |
| **Organisation** | **Name** | **Contact numbers** | **E mail** |
| **Mobile** | **Landline** | **Alternate** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |