**Business Continuity Plan**

**Document Details**

|  |  |
| --- | --- |
| **Document Title:**  | **Business Continuity Plan** |
| **Version Number:** | **1.0** |
| **Issue date:** | **15.01.24** |
| **Author:** | **Cristina Vannini-Goodchild** |

**Document Authorisation**

This document is issued under the authority of:

|  |  |
| --- | --- |
| **Name** | **Position and Organisation** |
|  |  |
|  |  |

1. **Introduction**

**1.1 Purpose and Objectives**

The aim of this business continuity plan is to ensure that key activities that are essential to the business with regards to the provision of goods and services to its customers and its personnel can continue to be delivered such as IT, Finance, HR, Data Protection and H&S in the face of disruption. Outlining the responsibility of the Managing Director/CEO and other senior staff and partners in the event of a crisis to maintain critical functions as practically possible.

The key objectives of the plan are to:

* Engage the response team as soon as disruptions are present
* Provide an overview and prioritisation of essential activities
* Outline and analyse known risks to ensure continuous delivery of these activities, including reduction of risks where possible
* Provide a framework for responding to any disruptive incident the business faces

**1.2. Overview of the function and activities delivered:**

**Head Office Location:** <add business address>

**Key Service:** <add key internal and external services>

Overall accountability for the effective day to day running of these services lies with <add responsible role>

In the event of an incident related to any of the key services listed above the following individuals should be contacted in ascending order:

**Incident Response Team**

|  |  |  |  |
| --- | --- | --- | --- |
| **Priority Order** | **Name** | **Role** | **Contact Details** |
| **1** |  |  |  |
| **2** |  |  |  |
| **3** |  |  |  |
| **4** |  |  |  |
| **5** |  |  |  |

In response to any incident the Incident Response Team must consider and action the following steps:

* Identification
* Assessment
* Planning
* Communication
* Implementation
* Assessment
* Review

**1.3. Staff Notification**

In the event of an incident or disruption to any of the key services the Incident Response Team must ensure all management staff and key partners are notified, this applies both in and out of hours.

Management staff, once notified, should ensure that all staff within their department are communicated to about the incident or disruption including any implications to their working environment.

**1.4. Communication**

In the event of incident or disruption the Incident Response Team will ensure that all stakeholders to include field staff, volunteers and self-employed are notified of any changes. The organisation appreciates the potential knock-on effect to other organisations and our clients and therefore would ensure that all affected stakeholders be included in this communication, if appropriate.

The Incident Response Team will ensure all stakeholders are contacted by the appropriate means, this will include an initial communication via email, calling where necessary, and providing information on the company intranet.

**1.5. Risk Assessments**

Organisational and security risks are assessed regularly on a quarterly basis as part of our risk management and escalation procedures. The likelihood and potential impact is assessed against each risk and an appropriate risk strategy is put in place to effectively mitigate and prepare possible impacts in advance.

In accordance with the organisation’s internal governance procedures annual reviews are conducted for all services.

**1.6. Infectious Diseases and Pandemics**

In response to a spread of infectious disease we have implement a RAG status system (Red, Amber, Green), in accordance with Government guidance. Each person entering the premises is to be assessed individually via a rapid lateral flow test and temperature gauge to ensure the well being of staff.

All staff are routinely exposed to a self-administered lateral flow rapid test twice a week. The appropriate precautions and measures are in place in terms of Personal Protective Equipment (PPE) and Disclaimers following the guidance from the Local Authority, Public Health and the NHS.

Wherever possible staff are encouraged to work from home and access the organisation system via a secure VPN.

To assist our staff to better cope with the effects of isolation and other restriction that might have been imposed by the authorities to safeguard the well being of its citizen the organisation has engaged with Health Assured which provides an Employee Assistance Programme and wellbeing services and includes a comprehensive telephone service and access to structured therapy. We will continue to evaluate the benefits of this service and the provider to ensure that we respond to our staff needs.

1. **Continuing Essential Activity in the Event of a Disruption**

**2.1. Failure of IT Systems**

<add the company name>, like many organisations, relies upon a number of IT systems for their day-to-day operations. A disaster that prevents the organisation from accessing these systems whether caused by the failure of the systems themselves or being due to an incident such as fire or flooding will potentially have an impact on the continuation of the organisation.

IT system failures may include:

* Loss of email/internet
* Loss of access to stored documents (shared server)
* Loss of individual IT systems/applications such as Sage and HubSpot
* Major IT network outage.

All IT system failure will be managed via the Incident Response Team who is responsible for managing the relationship with the various providers. The IT Provider will lead on all technology, systems, and telephony failures. Any IT system failures must also be reported to the internal Data Protection Office (<add email address>) due to the risk of a data breach.

The development of telecommunications that are reliant upon the IT network makes it likely that telephone failure will also result from any IT network failure. The priority in which restoration is required will depend on the tasks at hand.

If there is a loss of hardware or software through theft or damage, then advice should be sought from the IT provider and the incident reported in the Company’s Incident Record Log and reported to the Data Protection Office (<add email address>) as a data breach.

**2.2. Failure of Telecommunications**

The telephone lines at <add company name> are provided under a telecommunications contract with the IT Provider. Should the telephone systems (including mobile telephony) be inactive across the entire organisation then the IT Provider must be contacted. The priority in which restoration of phone lines are required will depend on the service area however it is likely that telephone communication can be reinstated via mobile phone.

If electricity has failed, then prior consideration needs to be given to the ability to recharge mobile phone batteries. All senior management office staff are equipped with a company issued mobile phone which should always remain charged and in their person.

**2.3. Loss of Records**

Where there has been a loss of records (electronic or paper), the Data Protection Office will be informed immediately, and the incident will be treated as a data breach the relevant processes defined within the Information Governance Policy and GDPR Regulations will be followed.

**2.4. Staff Shortages**

The absence of staff will undoubtedly have varying effects depending on their role. In some cases, roles can be covered by other staff members, but others may be highly specialised, and necessary arrangements need to be explored. It is the responsibility of the Managing Director/CEO to ensure that a cross-section of staff are trained and/or have the relevant empowerment to step in when necessary.

Potential threats related to staff shortages include:

* <add role name> unavailability during critical steps of the payroll and finance process
* <add role name> unavailability for the online approvals
* <add role name> unavailability to carry out the critical functions of the finance process to include the required approvals and authorisations.
* <add as necessary>

The Managing Director/CEO is responsible to put in place an Operational Manager who has been granted the relevant empowerment including the online approvals to step in in the absence of the CEO. In the absence of the Finance Officer approvals and authorisations activities will be assigned to the CEO/Ops Manager while the delivery of financial outputs will be outsourced to an accounting service provider. Non-critical functions will either be cancelled or postponed.

**2.5. IT Supply Chain**

It is the responsibility of the Managind Director/CEO to ensure effective backups are in place with the relevant providers. These includes:

* MS Office 365
* Sage
* HubSpot
* SharePoint

MS Office 365, SharePoint and HubSpot are cloud-based systems with regular backups in place via our IT support provider; in case of a loss of data either permanent or temporary the organisation will be able to re-install it via the cloud solutions.

Sage is backed up locally from the local server on disks which are then safely locked in the safe. We are in the process of exploring alternative solutions.

**2.6. Other**

Other areas that could potentially affect the service and its activity may include the following: this list is not exhaustive:

* Terrorist attack or threat affecting the transport network or community locations
* Theft or criminal damage of equipment
* Chemical contamination
* Fraud, sabotage, or other malicious acts
* Severe weather

**2.7. Insurance and Incident Costs**

The insurance arrangements in place which may apply to incidents are Employers and Public Liability Insurance. All insurance policies are to be reviewed bi-annually with the company’s insurance providers.

**2.8. Mutual Aid and Interim Redeployment**

It is the responsibility of the Managing Director/CEO to assess where shortfalls in staffing in critical areas of the business may occur because of high levels of staff absence.

Consideration will have to be given to the viability of redeploying staff away from activities deemed to be non-essential to cover critical areas across the organisation.

It is essential that staff should always wear their ID badges; this will ensure that all stakeholders can check the authenticity of staff transferring between business areas.

1. **Conclusion**

<add name of company> is committed to ensuring a continuous provision of the critical activities to its employees, volunteers, trustees, partners and associates. The organisation is proactive in assessing potential disruption and highly reactive to minimising any impact on essential support functions.

We ensure that we maintain robust and proactive processes and audits in order to ensure continuity of service.

**Month/year**

Next Review month/year

To Be Reviewed Annually