**DISASTER RECOVERY**

**AND**

**BUSINESS CONTINUITY PLAN**

**ABC Financial Planning Ltd**

**202X**

Contents:

[1. Purpose of the Disaster Recovery and Business Continuity Plan 3](#_Toc109912779)

[2. Responsibility for delivery of the Disaster Recovery and Business Continuity Plan 3](#_Toc109912780)

[3. Location of the Disaster Recovery and Business Continuity Plan 4](#_Toc109912781)

[4. Review of the Disaster Recovery and Business Continuity Plan 4](#_Toc109912782)

[5. Testing of the Disaster Recovery and Business Continuity Plan 4](#_Toc109912783)

[6. Details of business and premises 5](#_Toc109912784)

[7. Personnel 6](#_Toc109912785)

[8. Records and data 7](#_Toc109912786)

[9. Systems 7](#_Toc109912787)

[10. Identification and Mitigation of Risks 9](#_Toc109912788)

[11. Action plans 12](#_Toc109912789)

[11.1 Loss of Key Personnel Resources 12](#_Toc109912790)

[11.2 Telecommunications Infrastructure Failure 12](#_Toc109912791)

[11.3 Denial of Workplace Access - Short Term 12](#_Toc109912792)

[11.5 Loss of data 12](#_Toc109912793)

[12. Impact assessment 13](#_Toc109912794)

[13. Evacuation of Premises and Safeguarding of Staff 14](#_Toc109912795)

[14. Communications 14](#_Toc109912796)

[15. Recovery 15](#_Toc109912797)

[16. Plan Sign Off 15](#_Toc109912798)

### 1. Purpose of the Disaster Recovery and Business Continuity Plan

This plan is designed to ensure ABC Financial Planning Ltd (ABC) is capable of continued service delivery in the event of a disruptive incident.

FCA Requirements:

SYSC (3.2.19) Business Continuity

*A firm should have in place appropriate arrangements, having regard to the nature, scale and complexity of its business, to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption. These arrangements should be regularly updated and tested to ensure their effectiveness.*

This plan is designed to ensure that, where there is any potential for loss of business, disruption to performance of business functions or potential inability to comply with FCA requirements, a series of defined actions will be undertaken and enforced to enable ABC to manage the impacts of operational disruption.

# Through this plan ABC will seek to:

* Define and prioritise the critical functions of the business
* Analyse the emergency risks to the business
* Detail the agreed response to an emergency
* Identify key contacts and a communication pathway

### 2. Responsibility for delivery of the Disaster Recovery and Business Continuity Plan

The main point of contact within ABC for co-ordinating and implementing this plan is/are:

Name: Moneypenny

Position: Director

In the event of Moneypenny being on holiday / off sick, implementation will be the responsibility of Smith.

Upon notification or awareness of an event Moneypenny would initially co-ordinate the logistical arrangements; these could vary depending on the type of disaster, which may occur. In the first instance he will contact the staff, brief them on the situation and instruct them of the mitigation arrangements relevant to the incident.

A copy of this plan will be issued to all existing and new staff, all of whom have a responsibility to familiarise themselves with the content and their responsibilities therein.

Identification of any other risks by members of staff should be referred to Moneypenny in order that they can be included in the next review of the plan.

### 3. Location of the Disaster Recovery and Business Continuity Plan

Electronic copies of this Plan are stored:

### 4. Review of the Disaster Recovery and Business Continuity Plan

This plan will be formally reviewed by Moneypenny on a tri-annual basis or updated when there is a material change to normal operations.

Reviews of the plan are designed to:

* Identify any shortfalls within the implementation of the scheme
* Suggest corrective action regarding the above
* Ensure that the standards maintained within the plan meet those expected by the Regulator

Last review date: 20\*\*

Next review due: 20\*\*

### 5. Testing of the Disaster Recovery and Business Continuity Plan

This plan was successfully tested on …….. and amendments made where necessary.

### 

### 6. Details of business and premises

Business address:

The firm’s registered office address is the same as the firm’s principal place of business.

There are no other connected companies at other addresses.

The following functions are carried out at the principal place of business:

* Administration
* Client Meetings
* Business management
* Staff training

### 7. Personnel

Emergency contact details for personnel

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Business Role** | Contact Details | Role within this plan | Alternate if unavailable |
| Moneypenny | Director & Compliance Officer |  | Co-ordinator |  |
| 007 | Director & Financial Planner |  |  |  |
| Smith |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Authorised key holders.

First aiders

### 8. Records and data

All documents are held electronically on local desktops which are continuously synced with our online cloud-based service (Cloud Service). Any hard copy documents received into the office are scanned to Cloud Service on date of receipt.

Our IT consultants are …. who can be contacted at:

Moneypenny and 007 have remote access to all files and resources from their laptops

Staff are required to have their laptops and mobile phones passworded. Online access to *Cloud Service* is through 2 Factor Authentication.

### 9. Systems

The firm uses the following programmes:

| **IT System** | **Name** | **Supplier** | **Contact Details** |
| --- | --- | --- | --- |
| Operating System | Windows | Microsoft |  |
| Email | Microsoft Outlook | Microsoft |  |
| Word Processor | Microsoft Office | Microsoft |  |
| File Hosting | Cloud Service | Cloud Service |  |
| Back Office |  |  |  |
| Client Platform |  |  |  |
| Client Platform |  |  |  |
| Client Platform |  |  |  |
| DFM |  |  |  |
| Client Platform |  |  |  |
| Cashflow Software / Financial Modelling |  |  |  |
| Research software |  |  |  |
| Client Risk Profiling |  |  |  |
| Anti-Money Laundering |  |  |  |
| Telephones |  |  |  |
| Broadband |  |  |  |
| Client Portal |  |  |  |

### 10. Identification and Mitigation of Risks

| **Potential Disaster** | **Impact** | **Mitigation** | **Initial Response** | | | | | **Additional Procedures** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Loss of internet access and systems (including email)** | Critically dependent upon email and internet access for business | Immediate response required to threats to prevent loss of service or long-term system un availability | Contact suppliers. Access Server Room if safe | Assess impact and duration on systems availability. Ensure integrity of power supply and shutdown if necessary | Communicate impact to Board | Invoke IT Recovery Plan for individual systems if able and as required | If part of wider system failure, invoke Business Continuity Plan | IT Recovery Plan |
| **Loss of Telephones** | Telephone communication critical to business | Use of back up phone line provided by DTX | Immediate divert of phones to alternative/ home office and send staff there | Activate divert procedure | Investigate fault with service providers and re-establish connectivity asap | Invoke Telecoms Recovery Plan for individual systems if able and as required | If part of wider system failure, invoke Business Continuity Plan | Use mobiles |
| May require temporary use of mobiles | IT Recovery Plan |
| **Loss of Cloud Access** | Critical access to databases, client documents and internet | HP servers used. Servers backed up daily. Service contract in place | Investigate fault with service partners and re-establish access to server asap | Invoke IT Recovery Plan |  |  |  | Consider secondary cloud service for additional back up |
| **Power/Utilities Failure** | Critical because of impact on voice and data communication, and operability of office through heating and water supply | Annual review of infrastructure. | Investigate and assess situation Call out service contractors. Liaise with utilities providers if appropriate | Consider impact and duration on hygiene. | If prolonged investigate buying in water | Prepare engineering solution and if appropriate hire temporary equipment and plug into building systems | Invoke Business Continuity Plan |  |
| Alternative/ home office available in event of long terms failure. | Hire boilers and temporary heaters if necessary |
|  |  |
|  |
|  |
| **Fire/Smoke** | Fire can damage systems. | Buildings have automatic detection. Tested once a week/month | Treat small and large fires the same way. | Activate fire alarm if not automatically activated. | Use extinguishers if safe to do so and trained to do so | Evacuate premises using the nearest and safest exit path | Only re-enter the premises when informed it is safe to do so | Fire Evacuation Procedure |  |
| Smoke damage can render premises unsuitable | Key staff trained in and supplied with fire extinguishers | Exercise extreme caution | Conduct head count and assist visitors and contractors | Follow advice of Fire Services if involved. |  |
| Possible injury/death to staff |  | If safe to do so attempt to locate source of fire |  |  |  |
| **Prolonged Denied Access to Premises** | Catch all category to include major safety incident, environmental, civil unrest | Remote/ home offices available with full recovery process in place. | Decide safest course of action in consultation with emergency services at remote muster point or other place as advised by emergency services. | Liaise with directors, emergency services etc to assess situation. | Agree on whether to implement Business Continuity Plan and advise staff on plan of action. | Invoke Business Continuity Plan |  | Business Continuity Plan |  |
| Denial of access to critical systems |  |  |
| **Loss of key staff** | Dependent upon key skills in specialist areas. | Some protection from Terms of Employment | Resignations/employment issues to be reported immediately to directors. | Directors to assess scale of problem. | Advise insurers/PI insurers if claim to be made. |  |  | HR & grievance procedures/staff handbook |  |
| Possible loss of business/ clients | Regular staff reviews. | Liaise with staff member if appropriate. | Instruct solicitors. |  |  |
| . | Succession planning and deputies in place |  |  |  |
|  | Key man/ |  |  |
| shareholder protection |  |  |
| **Loss of Outsourced Services** | Dependent on hardware and software support in event of failure | Alternative supplier sourced | Assess duration and impact of problem | Fast tract approval of alternative suppliers for additional supplies | Prioritise client services if some unavailable | Invoke IT Recovery Plan |  | See Significant Outsource Register |  |
| **Burglary/**  **Break in/**  **Vandalism/**  **Sabotage/**  **Fraud** | Critical to protect property which could be rendered unusable, confidential client and management data, and equipment | Building alarmed and serviced by alarm company  Full inventory of assets maintenance.  All computers password protected  Data backed up off site.  Insurance policy with ABC PLC covers office and contents for £0000, Employers liability for £yym and public liability for £zm. | Involve police at earliest opportunity | Investigate and assess situation. Call out contractors to secure premises (e.g. broken windows) if necessary | Determine extent of damage, theft and impact on business | Engage contractors to repair and replace damaged, stolen assets | Recommend action to Board.  Invoke IT Recovery Plan | IT Recovery Plan |  |
| If party still on premises do not enter  Exercise extreme caution and preserve any available evidence | Notify insurers |  |
|  |
|  |
|  |

### 11. Action plans

#### 11.1 Loss of Key Personnel Resources

This action plan identifies procedures to be followed or steps to be taken in the event of key individuals, or a critical percentage of staff being absent long term, or permanently.

|  |  |
| --- | --- |
| **Staff Member** | **Alternate Staff Member** |
| Non-Executive Advisers: ???? | 007 or Moneypenny |
| Executive Adviser: 007 | ???? or Moneypenny |
| Senior Manager with Significant Regulatory Functions: Moneypenny | 007 and The Compliance Department (Mark Dennison) |
| Senior Administrator: ???? | ?? |

#### 

#### 11.2 Telecommunications Infrastructure Failure

The broadband is supplied and managed by *Broadband supplier* in the event of any issues contact *Broadband supplier on 123456789*. If this fails, we will work from home using private broadband with VPN on.

#### 11.3 Denial of Workplace Access - Short Term

In the event we would work from home.

#### 11.5 Loss of data

In the event we would use alternate cloud-based servers. Request redundancy process from *Cloud Supplier* in the event of data loss.

### 12. Impact assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type of impact and its effects | Impact descriptors and event categorisation | | | |
| Catastrophic | High | Medium | Low |
| FINANCIAL | | | | |
| Event | Loss of 007, Moneypenny | Temporary Loss of 007, Moneypenny | Failure of Platform | Loss of Access to Premises |
| Loss of revenue | Short Term Minimal | Short Term Minimal | £0 (temporary) | £0 |
| Loss of shareholder value | 50% reduction in potential sale value | £0 | £0 | £0 |
| Penalties | £0 | £0 | £0 | £0 |
| Bad debts | £0 | £0 | £0 | £0 |
| Additional operating cost(s) | £200,000 | £100,000 | £0 | £10,000 |
| NON-FINANCIAL | | | | |
| Reputational loss | Low as Diane and Eleanor could temporarily fill in. | Possible loss of confidence in service to clients as of not working with 007. | Loss of confidence in service to clients as a result in platform failure. | Adverse comment in local media only and/or confined to a limited number of localised customers. |
| Loss of operational capacity | Yes | Yes | Yes | Yes |
| Customer service | Yes | Yes | Yes | Yes |

### 13. Evacuation of Premises and Safeguarding of Staff

As per the premises plan details on site.

### 14. Communications

In the event of an incident and this plan being activated, the following people may need to be contacted. Nature of contact will depend on the incident type and time it has occurred.

**Always Contact**

* Staff
* Clients to reschedule or relocate appointments

**Contact Depending on Incident**

|  |  |  |
| --- | --- | --- |
| **Name** | **Supplier** | **Contact Details** |
| Regulator | FCA | 02070661000 |
| PI Provider |  |  |
| IT Consultants |  |  |
| Bank |  |  |
| Compliance Provider | The Compliance Department | 01270-303179 |
| Office and Contents Insurance |  |  |

### 15. Recovery

The purpose of the recovery phase is to resume normal working practises for the firm. Where the impact of the incident is prolonged, normal operations may need to be delivered under new circumstances e.g., from a different building.

|  |  |
| --- | --- |
| **Action** | **Further Info / Details** |
| Agree and plan the actions required to enable recovery and resumption of normal working practises. | Agreed actions will be detailed in an action plan and set against timescales with responsibility for completion clearly indicated. |
| Respond to any long-term support needs of staff. | Depending on the nature of the incident, the Firm may need to consider the use of appropriate External Agencies. |
| Carry out a ‘debrief’ of the incident | This should be reviewed by Moneypenny to ensure key actions resulting from the incident are implemented within designated timescales. |
| Review this Continuity Plan in light of lessons learned from incident and the response to it. | Implement recommendations for improvement and update this Plan. Ensure a revised version of the Plan is read by all members of staff. |

**Sect**

**ion 14:**

### 16. Plan Sign Off

Moneypenny Wall acknowledges responsibility for ensuring that this plan is maintained, exercised, and updated in accordance with internal requirements for business continuity.

Signed:

Name: Moneypenny

Position: Director

Date: