Business Continuity Management System

**Business Continuity Plan – Rev 017**

|  |
| --- |

**Relationship with other Business Continuity (and appropriate) documents**

| **Document** | **Description** |
| --- | --- |
| [Business Continuity Policy](https://yondrverse.com/intranet/security/business-continuity-policy-2) | Outlines why the organisation has Business Continuity in place, who is responsible and how it will be maintained, trained out and tested. |
| Business Impact Analysis (BIA) | Updates from WW and IMT info updated. |
| Triage Plan | High level decision making document for invocation of the appropriate Business Continuity Plans and teams. |
| Regional Business Continuity Plan  (Office BCP) | Localised Plan which contains the escalation and response procedures for incidents which occur at an office location. |
| Data Centre Business Continuity Plan (DC BCP) | Localised Plan which contains the escalation and response procedures for incidents which occur at a data centre (stored onsite). |
| Emergency Operating Procedures (EOPs) | Set of incident specific emergency procedures which are stored at the DC Network Operations Centre (NOC). |

# Executive Summary







**Contents**

[Executive Summary 3](#_30j0zll)

[1.](#_3rdcrjn) Purpose, Scope and Objectives 6

[1.1.](#_32hioqz) Purpose 6

[1.2.](#_46r0co2) Maintenance 6

[1.3.](#_2lwamvv) Scope and Risks 6

[1.4.](#_206ipza) Objectives 7

[1.5.](#_2nusc19) Triggers for Invocation 7

[2.](#_1302m92) Key activities 8

[3.](#_2250f4o) Incident Management 10

[3.1.](#_14ykbeg)  Incident Management 10

[3.2.](#_3oy7u29) Detection, Reporting and Monitoring 11

[Cyber Incident 11](#_243i4a2)

[Staffing Incident 12](#_j8sehv)

[3.3.](#_338fx5o) Incident Response 13

[3.4.](#_1idq7dh) Fire and Emergency Evacuation Plans 13

[3.5.](#_42ddq1a) Buffer Time and Standby Actions 13

[3.6.](#_2hio093) Site Closure 14

[3.7.](#_wnyagw) Incident Management Control Centre 14

[3.8.](#_3gnlt4p) Information Security Continuity within IT 14

[4.](#_1vsw3ci) Business Continuity: Invocation Procedures 16

[4.1.](#_4fsjm0b) Accessing information 16

[5.](#_2uxtw84) Communication 16

[5.1.](#_1a346fx) Internal Communications 17

[5.2.](#_3u2rp3q) External Communications 17

[5.3.](#_2981zbj) Communicating with Emergency Responders 17

[5.4.](#_odc9jc) Methods of Communication 18

[5.5.](#_38czs75) PR and Media Response 18

[6.](#_1nia2ey) Roles and Responsibilities 19

[6.1.](#_47hxl2r) Incident Management Team Actions - Summary 19

[6.2.](#_2mn7vak) Incident Management Team Actions - Detailed 20

[7.](#_11si5id) Resuming Activities 23

[7.1.](#_3ls5o66) Summary 23

[7.2.](#_20xfydz) People 23

[7.3.](#_4kx3h1s) Information and Data 24

[7.4.](#_302dr9l) Buildings, Work Environment and Associated Utilities 24

[7.5.](#_1f7o1he) Facilities, Equipment and Consumables 24

[7.6.](#_3z7bk57) Information Communications Technology 24

[7.7.](#_2eclud0) Transportation 25

[7.8.](#_thw4kt) Finance 25

[7.9.](#_3dhjn8m) Partners and Suppliers 25

[7.10.](#_1smtxgf) Return to normal 25

[8.](#_4cmhg48) Standing the Plan Down 26

[9.](#_2rrrqc1) Exercising, Maintenance and Review 26

[Appendix 1. Incident Management Team Members 27](#_16x20ju)

[Appendix 2. Salvage Team 30](#_3qwpj7n)

[Appendix 3. Salvage Team Recovery Request Form. 31](#_261ztfg)

[Appendix 4. Recovery Site Contacts 32](#_l7a3n9)

[Appendix 5. Succession Planning 32](#_356xmb2)

[Appendix 6. Telephone Cascade 32](#_1kc7wiv)

[Appendix 7. Meeting Agenda 33](#_44bvf6o)

[Appendix 8. Internal Contacts - Staff 33](#_2jh5peh)

[Appendix 9. External interested parties - defined 34](#_ymfzma)

[Appendix 10. Bank Account Details 34](#_3im3ia3)

[Appendix 11. Battlebox contents 34](#_1xrdshw)

[Appendix 12. Emergency Evacuation Plan 35](#_4hr1b5p)

[Appendix 13. Activity Log 35](#_2wwbldi)

[Appendix 14. Key Holder Rota 36](#_1c1lvlb)

[Appendix 15. Local, Regional and National Advisory Systems 36](#_3w19e94)

[Appendix 16. Insurance Company 36](#_2b6jogx)

[Appendix 17. IT Topography, Restore Details and Telephone Diversion Procedures 36](#_qbtyoq)

[Appendix 18. Holding Statement and Process of Release 36](#_3abhhcj)

[Appendix 19. Buffer Time Actions 39](#_1pgrrkc)

[Appendix 20. Pandemic Actions 40](#_49gfa85)

[Appendix 21. Impacts of not performing activity 43](#_39kk8xu)

[Appendix 22. Timeframe for Resumptions of Activities / Client SLA’s 44](#_2olpkfy)

[Appendix 23. Resource Requirements 46](#_13qzunr)

[Appendix 24. Decision to invoke 49](#_3nqndbk)

[Appendix 25. Assumptions 51](#_22vxnjd)

[Appendix 26. Communication Log 52](#_i17xr6)

[Appendix 27. Incident Reporting Sheet 53](#_320vgez)

[Version control 54](#_1h65qms)

# Purpose, Scope and Objectives

## Purpose

The purpose of this Business Continuity Plan (“BCP” or “Plan”) is to restore the operations and services provided by Yondr to their clients to an acceptable level in an acceptable timescale, when an event has made normal operations impossible.

The Plan is primarily designed for use by members of the Incident Management Team (“IMT”) but may be used in part by other members of Yondr as an information resource. The BCMS Policy and edited versions of this Plan may be shared with interested parties, where appropriate.

Within this Plan is the triggers for invocation, method of invocation, detailed responsibilities and timelines for recovery and a process for standing the Plan down.

The IMT (any member of the Executive Team / Managing Directors) have the responsibility for invoking the Plan. Once it is invoked, they have the responsibility for strategic and tactical decisions concerning recovery. They must also make the initial contact to the staff to inform them that the Plan has been invoked.

This document has been written to be a repository of information. It contains all the information required to restore operations in the event of acute disruption. It has also been designed to be a flexible recovery tool and can be used in part in the event of less serious incidents.

The Business Continuity Management System (“BCMS”) is driven by top management by means of allocation of resources, communicating the importance of Business Continuity, establishing roles and responsibilities and promoting continual improvement. This is further detailed in the BCMS Policy.

The Management System has been drafted by Biscon Planning and then agreed with management at Yondr. Biscon are a leading consultancy firm in Risk and Business Continuity.

## Maintenance

The responsibility for the maintenance of the localised BCPs and for the initial response lies with the appropriate Office Manager / Campus Lead. Responsibility for the maintenance of the Corporate BCP (this document) lies with the COO who will work with the relevant departments to maintain the Appendices.

Any unforeseen incidents or near misses ranking P0 or P1 will trigger a review of the System to ensure that any lessons learned will be fed back into the System.

Although there are no legal requirements for Yondr to have a Business Continuity Management System in place, it has done so as a matter of good practice, to mitigate or respond to incidents which affect the organisation and to protect the interests of internal and external stakeholders. If this changes, then the System will be reviewed against these requirements.

## Scope and Risks

This project covers Project management for design and development for scalable technology real estate. Research and development for implementation into scalable technology real estate. Asset management including operational and maintenance support to scalable technology real estate.

The possible risks for the Plan to react to are maintained in the Global Risk Register.

## Objectives

The main objectives of this Plan are:

* To ensure the safety of all staff is considered,
* To minimise the disruption to normal operations,
* To limit the extent of disruption and damage,
* To minimise the economic impact of the interruption,
* To establish alternative means of operation in advance,
* To ensure that critical activities can be recovered within the recovery time objectives and that return to normal operations happens as defined in the Business Impact Analysis (BIA),
* To ensure that a framework and structure exists for any predicted decision making, during times of disruption,
* Be compliant to ISO 22301 – the International Standard for Business Continuity.

## Triggers for Invocation

Incidents which may trigger invocation of the Business Continuity Plan are described in the Triage Plan and Appendix 24 of this Plan and may include (but are not limited to):

* Loss of access to a primary office (e.g. London) that is likely to last longer than one working day.
* Loss of ICT likely to last beyond 24 hours (or Cyber-attack).
* Incident which has an area wide impact on transportation affecting staff transport to their normal workplace, e.g. severe weather.
* External event likely to cause wide-scale disruption to Group critical activities, e.g. pandemic.
* Event occurs which has the potential to or is causing actual damage to the Group’s reputation.
* A significant Data Breach / Data Loss requiring notification to ICO and affected customers.
* An onsite incident where there is death or serious injury to a contractor or team member resulting in the possibility of the Group being held responsible e.g. H & S incident.
* Main supplier outage or loss.
* Significant pandemic incident (e.g. Covid 19) requiring specific response measures.
* Terrorist event affecting any of the primary Yondr locations.

This list is not exhaustive and any incident which could cause long-term or wide-scale disruption or damage to the Group a decision must be made whether (or not) to invoke the plan.

# Key activities

The overall business critical activity of Yondr is to datacentre design, construction and operations.

More specifically (in no particular order):-

1. Marketing – Marketing, Creative and Digital.
2. Operations - Develop, maintain and operate model for datacentres.
3. Commercial - Critical is procurement and ensuring that Finance can process new third parties.
4. Design & Construction - New build datacentres across the world largely using subcontractors.
5. Finance - Managing payroll, accounts payable, invoicing, treasury, procurement, tax accounting and accounts reporting.
6. People - Dealing with personnel issues including payroll, recruitment, L&D, and other staff benefits.
7. IT – Service delivery, network and application support, data and development and solutions delivery. Control outsourcing of support.
8. CEOs office – Y Suite support and leadership. Organisation wide and stakeholder communications.
9. Facility Management – Management of offices (contracts and services), employee housing, transportation requirements.

The above are supported by the management functions and other central services departments such as Office Management.

Other topics to consider in the restoration of ‘normal’ services include:

* Protection of staff, visitors and clients.
* The contact of suppliers, clients and stakeholders to reassure them that Yondr is still operational.
* Control of the flow of information about an incident.
* The communication to all staff of immediate contingency arrangements.
* Setting up temporary working accommodation if necessary.
* Recreating records and recovering or protecting files and documents.
* Securing original documents.
* Rebuilding servers and PCs, restoring data and making the systems available to in-house and remote users, in the stated timescale.
* Re-establishing the existing premises or creating new permanent premises.
* Collection and processing of inbound post.
* Formulation of an insurance claim with a loss adjuster.

The Plan is structured to deal with incidents that affect the following areas and resources, either singly or in combination:

* People
* Information and data
* Buildings, work environment and associated utilities
* Facilities, equipment and consumables
* IT systems
* Transportation
* Finance
* Partners and suppliers
* Brand and reputation

To ensure the maximum flexibility, it is not based around the response to specific scenarios but looks at the effects any incident might have. The impacts over time of not performing the activity and the timeframes for resumption are shown in Appendices 21 and 22.

# 

# Incident Management

## Incident Management

An incident may be any situation which might or could lead to a disruption, loss, emergency or crisis affecting the normal operations of Yondr.

Disruptive incidents occur on an almost daily basis. It is important to establish at what point a disruptive incident should be escalated to the IMT and when they should invoke the Business Continuity Plan. More guidance on incident classification and escalation can be found in the regional incident management quick reference guide.

In the event of an incident occurring, an Incident Report Log will be completed using the METHANE reporting sheet (Appendix 27). This document will be completed by the location / team receiving the initial call.

The IMT will assess the nature and extent of a disruptive incident and its potential impact on the operations and services of Yondr when taking into consideration the decision whether to invoke the Plan, use the ‘buffer time’ or deal with the incident as part of ‘business as usual’

IMT members should bear in mind that a minor emergency may have the potential to worsen and escalate.

The table in Appendix 24 may be used to assist in the decision whether to invoke, or not.

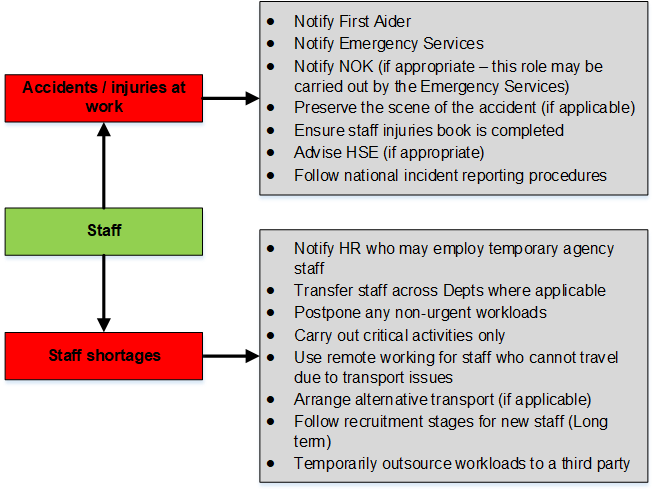
| **Reviewer** | **Status** | **Notes** |
| --- | --- | --- |
|  | Not started |  |
|  | In progress |  |
|  | Under review |  |
|  | Approved |  |

## Detection, Reporting and Monitoring

## Cyber Incident



## Staffing Incident

****

During working hours, most incidents will be resolved by the normal processes and procedures of the business, following normal reporting lines.

In case of a serious incident the following procedures must be followed:

Normal Working Hours

An incident internal or external to Yondr, which is outside the scope of normal business operations, should be immediately reported to the departmental manager or, in the manager’s absence, to that manager’s most senior report onsite. A decision will be taken as to whether the incident can be resolved or whether the information should be escalated. There should be no delay in this process.

If the incident affects a site, the emergency evacuation should be followed. The IMT will then assemble – regardless of the site affected – and assess the situation, taking advice from the emergency services if they have attended the site.

Cyber or power issues to a site will be dealt with staff in the relevant office seeking support from appropriate colleagues as needed.

**NB: Personal welfare is of paramount importance, and site evacuation (if required) and the instructions of the emergency services take priority over all other actions.**

During the night, at weekends or on public holidays

Outside working hours, the alarm monitoring company, onsite security or the landlord, or the emergency services will notify the local FPoC (first point of contact) (see Appendix 14). On arrival at the site (or earlier if the situation is clear) the key holder(s) will either resolve the situation, or escalate it to a member of the IMT, who will decide whether further information is required. They may then decide to notify other members of the IMT and discuss whether the Plan should be invoked.

In the event of an area wide issue (such as transport chaos) the IMT will meet via conference call to discuss the impact on Yondr. The same is true for other incidents such as a data breach.

Emergencies not notified to staff

If an incident affects a site outside normal working hours are not notified by the emergency services through the keyholder process, it will not become apparent until staff begin arriving for work. In this case, the first senior member of staff on site will be responsible for:

* contacting emergency services, if staff have not already done so, and
* informing the members of the IMT who will decide on the appropriate response

If the incident is a large public event and picked up by a member of staff, they should escalate to the Incident Management Team.

Monitoring Incidents

The IMT will monitor potential or actual incidents which arise, until the threat has diminished or the incident has been dealt with and the Plan has been stood down.

## Incident Response

Each incident will be unique in nature and consequently may involve a multi-agency response from emergency services, therefore the response from Yondr must be flexible to be able to adapt to these changing and demanding circumstances.

All staff involved in responding to the incident must keep a full record of any communications, actions or decisions (Appendix 13). These records may be used as part of the post incident debrief and will be kept for a period of no less than two years, should they be required for any further accountability / litigation / review purposes.

## Fire and Emergency Evacuation Plans

The company fire and emergency evacuation plans will be used and are not compromised or superseded by this document. A summary of the company document is in Appendix 12.

Fire Wardens will check their areas and report their status to the Emergency Services Liaison (Appendix 1). This information will then be passed to the attending emergency services. The emergency services Incident Commander should be identified.

In the event of a wide scale incident, information from the Local Government website should be referenced (Appendix 15) and where necessary, further advice sought.

If it is not safe to remain in the area of the incident, staff should make their way home, follow the advice to ‘go in, stay in, tune in’, and report their status to their line manager.

If an incident requires staff to remain on site, staff should move to the core of the building, closing windows and doors where it is safe to do so.

## Buffer Time and Standby Actions

‘Buffer Time’ is a concept to ensure that no time is lost in the response to an incident. If the impact of an incident is uncertain (e.g. a gas leak), a period of up to 24 hours (although it may be less at certain critical times) may be allowed to gather information and make a decision. During this time, actions that are time consuming may be started with the understanding that, if the situation is resolved, they may be stood down. These actions are detailed in Appendix 19.

At any time during buffer time, the Plan may be invoked or ‘back to business’ instructed. If the situation is not resolved after 24 hours, the Plan must be invoked by default, and no recovery time objectives should be passed.

## Site Closure

*Partial Closure*

In the event that only parts of the premises are affected by an emergency situation, it may be decided by the IMT to continue some presence at the affected premises. However, this will only be where:

* The emergency services recommend there is no further danger
* The Insurance Company agrees to this (where a claim will be made)
* Safe access / exit can be maintained or unassisted evacuation would be unsafe
* Date security is not at risk
* Heating, lighting, sanitation etc are available
* There is adequate containment (fire or security doors etc) from the damaged areas

*Full closure*

In severe incidents, the emergency services may require the closure of the premises. Where this decision is made during working hours, line managers will be informed to send staff home, or to another appropriate venue. Where closure is initiated out of hours, the IMT will organise notification of line managers about the situation via the telephone cascade and / or email / SMS. Dependent on the circumstances, line managers may be directed to:

* Stay at home pending further instructions
* Attend the premises, if closure is not the result of damage
* Attend the nominated recovery site
* Contact their staff according to the telephone cascade

*Security Arrangements*

Where it is not possible to secure the building by normal means (alarms and locks) owing to the nature of the damage, the Emergency Services Liaison will liaise with the emergency services and give consideration to:

* boarding up / sealing of potential points of entry (windows, doors etc)
* engagement of extra security staff to guard the premises

*Public access*

Regular visitors will be contacted by staff to notify them of any closure / restricted service and any alternative arrangements. Staff who have made appointments will contact their guests to either cancel or reschedule appointments, as necessary.

*Assessment of Duration of Closure*

The IMT will determine the period of closure of the affected location. The closure status will be reviewed on a frequent basis.

## Incident Management Control Centre

The location of the Incident Management Control Centre will be appointed depending on the location of an incident. Details of proposed Control Centres are included in the local Business Continuity Plan (BCP).

Where appropriate, contact may also be made via conference call Google chat, WhatsApp or telephone call.

## Information Security Continuity within IT

* When Yondr invoke the BCP, information security should not be compromised, there are several technical controls we have put in place.
* All our corporate applications are SaaS based and utilize TLS 1.2 or higher to encrypt communications. The rarely used remote access to the Data Center is only via VPN, utilizing IPsec.
* Remote users protected via the latest AV Definition updates as this is cloud hosted.
* Yondr has security logging of endpoints to the cloud. There is nothing on-prem.
* When Yondr fail IT Systems over, the data is a direct replica of the systems in production. Therefore, there is no reconfiguration needed

# Business Continuity: Invocation Procedures

Once a situation has been evaluated, as per the table in Appendix 24. a decision must be taken whether to invoke the Business Continuity Plan.

During working hours, any incident that could affect the operations of Yondr should be brought to the attention of the Office Manager / Campus Lead or another member of the IMT. They must then assess the incident – if necessary, on an on-going basis and with other specialists – and keep the other members of the IMT informed so that they may decide as to whether they should invoke the Plan. It is possible that an incident may be of such magnitude that it is obvious the Plan should be invoked.

The members of the IMT are listed in Appendix 1, and their responsibilities are laid out in Section 6.

Once the decision has been taken to invoke the plan, the staff at the affected site and other locations must be informed. Appoint a Plan Reader to follow the incident with reference to the actions specifically in Section 6.2.

## Accessing information

It is the responsibility of the IMT to make decisions. Other staff should not make decisions arbitrarily, unless this authority has been specifically delegated to them by the IMT. In the immediate aftermath of an event the flow of information may be chaotic and a system is required to prioritise this information and assess its reliability.

**Priority**

Level One - information that has a direct and immediate impact on the staff or operations of Yondr.

Level Two - information that may indirectly impact on the operations of Yondr.

Level Three - information that will have no impact on the operations of Yondr.

**Reliability**

High - same information from two or more direct sources.

Medium - information from one direct source, internet, television or radio.

Low - information from an indirect or uncorroborated source.

|  | **Level 1** | **Level 2** | **Level 3** |
| --- | --- | --- | --- |
| **High** | **Critical** | **Important** | *Noted* |
| **Medium** | **Important** | **Relevant** | *Noted* |
| **Low** | **Relevant** | **Relevant** | *Noted* |

All decisions, reasoning behind them and available information that the decision was based on should be recorded in the activity log for the post event review (an example of an activity log will be found in Appendix 13).

# Communication

Effective communication is essential to an effective response. The incident should be evaluated and the impact on a variety of communications streams e.g. email, mobile voice networks and social media anticipated. All streams should be constantly assessed, with alternatives understood.

An incident can be passively monitored through television news streams and social media postings. Staff should direct any information that they have about the incident to the Incident Management Team, and this should be evaluated as per Section 4.1.

Members of the IMT will discuss and agree on the key messages to be distributed to staff, freelancers, temps, intermediaries, clients and the public generally. All incoming / outgoing communications should be recorded in the Communications Log (Appendix 26).

## Internal Communications

The IMT will be responsible for internal communications to all staff.

Normal working hours: It will be relatively easy to inform and update staff at the evacuation assembly point if the incident is onsite. However, the longer the initial communication from the incident is left, the more chance of staff drifting off, or making unauthorised communication.

Out of hours / offsite incident (e.g. IT outage): If a site is partly or wholly inaccessible, affected staff will be advised using WhatsApp, Google Chat or the telephone cascade.

Arrival at site: If staff arrive at the site and cannot gain access, they should advise Security or Reception on site that they have arrived and of the action they are going to take (return home, attend another site) leaving a contact telephone number.

If normal network or voice communication cannot be made, then staff will be advised verbally by their manager if possible.

The NOC, HoFM and COM will all communicate via radios, mobile phones and Google Chat if necessary.

## External Communications

The IMT will be responsible for contacting all key groups and interested parties (see Appendix 9).

Information received from national, regional of local advisory systems will be documented within the Communications Log (Appendix 26). Communications will be responded to or actioned where necessary by the IMT.

## Communicating with Emergency Responders

The IMT should appoint an Emergency Services Liaison (see Appendix 1) to deal with emergency services responding at the affected site. The Emergency Services Liaison should:

* Be senior enough to make a decision on the spot,
* Have knowledge of the site,
* Be available and not required elsewhere,
* Be available for communication – one channel in, one channel out,
* Be able to take concise, legible notes,
* Keep the IMT informed,
* Be replaced after an amount of time, if fatigued
* Provide the emergency services with contact details so that they can be easily reached.

It may be necessary on rare occasions for a member of the organisation to attend multi-agency meetings. In these circumstances, the person attending should be of senior status and be in full knowledge of the incident and the organisations response. One of the multi-agency organisations (usually the Police) will contact the organisation inviting them to the meeting.

## Methods of Communication

In the event of an incident that has caused a significant impact to the operations of Yondr or may be perceived as having done so (e.g. an incident in the local area), the following methods of communication should be utilised.

**Website -** the front page should be amended to one that details the nature of the incident, its impact on the operations of Yondr and the response that is underway. The message is to be reviewed by the IMT prior to publicising.

**Telephone -** all Yondr staff use mobile telephones (there are no landline requirements). Any specific telephone requirements will be included within localised versions of the BCP.

**Email -** if the email system is still functioning, an auto response should be put on all email accounts acknowledging that there has been an incident, directing people to the website for up-to-date information.

**Google Chat / WhatsApp –** groups / rooms can be set up as and when needed as well.

## PR and Media Response

Appendix 18 contains Holding Statements that may be released in the immediate aftermath of an incident. Press releases will be composed by the IMT with assistance as required from a PR agency.

The nominated spokespeople for the company are the C Suite Directors. No other member of staff is authorised to speak on behalf of Yondr. All inbound requests for information or comment should be forwarded to the IMT.

Additional advice for dealing with the media is in Appendix 18.

The preferred method for communicating with the media is face to face interviews. Passive statements will also be issued and TV interviews avoided where possible.

# Roles and Responsibilities

## Incident Management Team Actions - Summary

The following flowchart and timelines detail the actions from incident to plan stand down for the IMT. This plan has been designed as a flexible recovery tool, and these actions should form a guideline rather than a prescriptive framework. When informing IMT, always start with the most senior role.









































## Incident Management Team Actions - Detailed

BCP is invoked:

|  | **Description** | **Time (from incident)** | **Comment** | **Sign Off** |
| --- | --- | --- | --- | --- |
|  | Safety of staff and guests is paramount. Ensure that Incident Management Actions have been successful.  Appoint a Plan Reader to follow all the below actions for completeness. | Immediate |  |  |
|  | Staff cascade begins via the emergency telephone cascade / or Google Chat  Open Google Chat for each Team meeting needed and direct members to the relevant ones by recording on Chat therefore leaving an audit trail of which Chat to join.  Agree the time zone to be used. In the first instance this should default to GMT, but for a regional incident only affecting one time zone this can be adjusted. | Immediate |  |  |
|  | Prepare to switch between Azure nodes if necessary.  Email available immediately over the internet. | Immediate |  |  |
|  | Notify customers of any major incidents.  (Other timescales as per the EOP’s at the NOC) | Within 5 minutes |  |  |
|  | Ensure that all Teams record decisions and actions in Activity Logs (see Appendix 13).  Ensure that one PA has been appointed to monitor and update all Chats with the latest decisions which will also act as an Activity Log. | Ongoing |  |  |
|  | Gather information and use information sources. See Appendix 15. | Ongoing |  |  |
|  | Distribute laptops / remote access to staff needing access. Priority goes to staff working on urgent issues. | 0-4 hours |  |  |
|  | External contractors required, e.g. glaziers and security, to attend site identified and contacted.  Special attention is needed on the security of electronic and paper data. This assessment must extend to staff now working from home or remotely. |  |  |  |
|  | IMT rally at most suitable location and / or via conference call. There is a suggested agenda for this meeting in Appendix 7. | 0-4 hours |  |  |
|  | Battle Boxes are retrieved to aid recovery. Appendix 11. Note they will be virtual Battle Boxes on G Suite. | 0-4 hours |  |  |
|  | IMT coordinate information regarding any missing or injured personnel and disseminate this to the emergency services. | 0-4 hours |  |  |
|  | Messages for the media, staff, clients, suppliers and other stakeholders are formulated and cascaded.  Client contact is via the local Client Manager or the members of the C-Suite. | 2-4 hours |  |  |
|  | Send staff home to work in addition to any other essential staff with access if the network is up. | 4 hours + |  |  |
|  | If partial failover has been possible (or necessary), the critical services will be available. | 2-4 hours |  |  |
|  | Investigate secondary premises through an office broker or. Contact details in Appendix 4. | 4-24 hours |  |  |
|  | Urgent electronic payments managed from home or at the bank branch. | 4-24 hours |  |  |
|  | Affected site informs the Yondr legal department (see Appendix 16).  Need to liaise with the property owners. | 4-24 hours |  |  |
|  | Take an inventory of kit and supplies. | 4-24 hours |  |  |
|  | Hardware obtained and rebuild of servers and PCs starts if existing kit not available. | 4-24 hours |  |  |
|  | Couriers and post are diverted to recovery sites. | 4-24 hours |  |  |
|  | Website updated with message for clients | 4-24 hours |  |  |
|  | If less than three days until payroll is run, ensure that they can manage payment. | 24 hours |  |  |
|  | Start to retrospectively produce necessary paperwork. | From 24 hours |  |  |
|  | Review urgent work and prioritise recovery with the three Hub Leaders.  Start assessment of any lost data | From 24 hours |  |  |
|  | Assess impact on quotes / tenders and Development. | 24 - 48 hours |  |  |
|  | Consider impact on marketing campaigns especially any forthcoming events. | 24-48 hours |  |  |
|  | Temporary staff sourced where possible. | 24-48 hours |  |  |
|  | IMT decide whether to prioritise personal or business items if salvage is feasible. | 24-48 hours |  |  |
|  | Consider impact on billing and whether an estimated bill is required and a payment on account needed to third parties. | 24-48 hours |  |  |
|  | Serviced accommodation / other office space available.  Start to investigate property to be cleared to ISO 27001 standards (i.e. secure for data protection) through a risk assessment. | Ongoing |  |  |
|  | Regular updates provided to staff, the media and other interested parties | Ongoing |  |  |
|  | Ensure that any client complaints (if any) are being managed. | Ongoing |  |  |
|  | Finance calculate financial implications of disruption and consider cashflow and financing implications. | 7 days - ongoing |  |  |
|  | IMT review delivery to clients, liaise with Directors and stakeholders. | 7 days - ongoing |  |  |
|  | Ensure that staff are empowered to spend cash on any emergency equipment needed (if reasonable). | Duration of invocation |  |  |
|  | IMT maintain strategic overview of response and possible return to normal working. | Duration of vocation |  |  |
|  | Suppliers contacted to instruct new invoice address, and to establish any outstanding invoices. Key suppliers are listed in Appendix 9. | Month 1 |  |  |
|  | Affected site advises site recovery or reconstruction options to IMT. | Month 1 |  |  |
|  | IMT decides on move to a new site / return to original site. | Month 1-2 |  |  |
|  | Migrate operations from temporary premises back to the restored primary business location. | At the earliest opportunity |  |  |
|  | Normalise operations at the restored facilities. | At the earliest opportunity |  |  |
|  | Advise all interested parties that a return to normal working has been achieved. | Once ALL activities are resumed. |  |  |
|  | Incident debrief held with lessons learnt followed up and the Plan updated where necessary. | Within 1 month of plan stood down. |  |  |

# Resuming Activities

## Summary

For a period, calls and emails can be fielded from home if a location is affected until a new site with the correct communications is in place. Staff will be able to use the laptops which are offsite or home PCs if the network is up.

Continuity options detailed under each heading below are taken from ISO 22313 which together ensure that critical activities can be resumed in the times identified in Appendix 22.

Details of the minimum resources required to maintain the key activities are listed in Appendix 23.

## People

A major incident may lead to immediate casualties – including fatalities - amongst Yondr staff and subsequent loss of staff with long term injuries or medical conditions. The emergency services are responsible for next of kin contact.

In no circumstances should Yondr staff make this first contact unless explicitly directed to by the emergency services.

Many staff are located within the Amsterdam and London offices. As such, a serious event during the day could lead to a loss of large numbers of staff which may be irrecoverable. Such an event is unlikely.

There is coverage for most skills within and between departments, although there are some key client relationships. Contractors and external agencies can cover many of the roles and they would be sourced from agencies. Agency staff could also cover roles within Finance, HR, Facilities, and IT to a degree.

There is a succession plan for the IMT members to ensure the decision-making authority for the Business Continuity Plan is uninterrupted. Details are in Appendix 5.

There are procedures in place for delegating authority to approve payment of invoices if the primary authoriser is unavailable, especially when dealing with significant sums.

Communication with staff is key following an incident and contact details are available 24x7 outside of the network.

The immediate issue to address will be the safety and well-being of all staff, to ensure that they have the ability to get home and to get into their homes. Longer term, HR will be responsible for the pastoral care (including arrangements for working away from home), liaising with injured staff and their families, and the arrangement of grief and trauma counselling.

New staff will be recruited externally as per the normal recruitment process.

**Actions in the event of a Pandemic are held in Appendix 20**

## Information and Data

Critical applications are mostly hosted in Azure and G-Suite. Other SaaS applications are also used.

The Azure nodes used are EU West and North Europe. The primary EU West node has data backed up every hour in three locations within that data centre and overnight to the EU North location. There is storage for life.

Meraki hosts all switches for all locations.

PCs and Macs are standard issue and do not store any data

Paper data access has been highlighted for Finance but there are soft copy backups.

## Buildings, Work Environment and Associated Utilities

For the scope of this project – i.e. the office locations, the 2020 pandemic has proven that home working, whilst not ideal, works for all locations.

The complete recovery solution will make use of the existing buildings, home working and in the medium term, serviced accommodation / new rental property.

## Facilities, Equipment and Consumables

There is little exposure to consumables that cannot be readily replaced. Office supplies such as stationery, printers and office furniture can be replaced with minimal impact.

## Information Communications Technology

1. Telephony

Telephones can be diverted to a spare analogue line on-site or to mobiles if the switch is still up. If the switch is down, the comms would be available from Google Chat.

1. Data Communications

Currently there are two lines to all sites, and the Regus office in Amsterdam is under investigation with failover for fibre, switch and firewall failure.

1. PCs and Office Hardware

Most Macs, laptops and desktops are standard issue and could be replaced from the high street and built by IT – machines are encrypted.

1. Software

Off the shelf software can be mostly downloaded when needed.

1. Remote Access

There is access for all staff as remote users at present.

1. Documentation

There are IT staff who can manage the failover. However, this should be documented so that a trained, trusted third party could also manage the process.

## Transportation

Staff attending meetings offsite could be disrupted, but it is likely that the other attendees will be affected by the same incident. Foreign travel could be disrupted, but there is little mitigation possible for a long haul trip.

If there is an incident at the office locations and public transport is affected, then taxis may be used to take staff home. The IMT will deal with this as well as financing the journey and ensuring that staff can get into their homes. If staff are expected to be working from another site, then the IMT may decide to provide a coach service – it will be assessed on a case by case basis depending on numbers, duration and location of the secondary site.

## Finance

The IMT has experience of dealing with disruptive events. In the event that emergency purchases were required, it is likely that these would be funded by the Directors and reclaimed from the company or on company credit cards. Any significant outlay e.g. for replacement IT kit, would be of such a timescale that normal procurement procedures could be put in place and the insurance company involved.

Payroll is a key process for staff, with payroll run every month across the organisation. Payment is made by BACS. As a worst case scenario, the BACS file from the previous month would be re-run adjusting for known joiners and leavers.

## Partners and Suppliers

Consultants / Freelancers are critical to the process with their consultancy skills.

Multiple suppliers are encouraged to sign up on the Yondr website to be added to the suppliers / contractors list and as a result they complete a pre-qualification questionnaire (PQQ). This list of alternative suppliers covers the various backup supplier arrangements which Yondr may require and can quickly be set up to take over as / when necessary if a primary supplier / contractor is unable to deliver. Details are maintained in the Yondr Connect platform.

Several suppliers are audited annually to support continuity in the supply chain and ensure alternative suppliers and contractors are available. The supplier's audit are agreed annually between Yondr Head of Procurement & Risk and Biscon (who carry out the audit).

## Return to normal

The organisation will restore and return business operations from the temporary measures adopted to support normal business requirements at the earliest opportunity following an incident. This may be achieved by:

* repairing the damage resulting from the incident:
* migrating operations form temporary premises back to the restored primary business location:
* moving to a new location:
* repair or replacement of essential equipment:
* recovery of information / data.

The decision on how best to ‘return to normal’ will need to be taken by the IMT and will be based on the severity of the damage caused by the incident and estimates of how long it might take to establish the necessary facilities.

Procedures for return to normal are included in the actions, section 6.2

A return to normal should include provision for the resumption of ALL activities and not just those identified as critical. “Normal” may indeed be different from how the organisation is currently – for instance, an office may not be reopened if it is damaged.

# Standing the Plan Down

The plan has an anticipated lifespan of up to three months. This is considered sufficient time for any damage to be identified and remedied, or for alternative accommodation to be sourced and equipped.

As such the plan is either stood down at three months or when:

* the affected site has been restored to full operational capacity or a new site has been sourced, equipped and is able to handle normal operations,
* data is secured and recovered,
* operations have been restored to pre-incident levels,
* staffing issues have been resolved and all departments have sufficient personnel to undertake their critical activities.

The decision to stand the plan down is taken by the IMT.

Once the plan is stood down, all the information used during the response to the incident should be collected and stored safely. A post incident review should occur to assess the success of the plan, using the information contained within the activity log. The lessons learned will be used to update the Business Continuity Plan.

# Exercising, Maintenance and Review

The responsibility for the maintenance of the BCP is covered in section 1.2

Exercising of the BCMS is undertaken on an annual basis (minimum) and the lessons learned fed back into the plan. Testing of arrangements at specific locations – e.g. testing the backup generators at a Data Center will be carried out in line with local maintenance and testing schedules / SOPs.

Testing of the SLA’s with the clients will be carried out as part of the main Corporate desktop exercise and crisis communications escalation procedures, at least annually. An example is the ability to escalate to a client if there has been an incident within five minutes. The exercising schedule is maintained on the Gantt chart maintained by Biscon.

Exercises will be attended by members of the IMTs and consideration will be given to including other staff as and where appropriate e.g. where an exercise may be more IT specific and require additional attendees.

## Appendix 1. Incident Management Team Members

The responsibility for the maintenance of the BCP is covered in section 1.2

Exercising is undertaken on an annual basis and the lessons learned fed back into the plan.

Exercises will be attended by members of the IMTs and consideration will be given to including other staff as and where appropriate e.g. where an exercise may be more IT specific and require additional attendees.

Diagram

Description automatically generated

| **EXECUTIVE LEADERSHIP TEAM** | | |
| --- | --- | --- |
| **Global or P0 Impact incidents only e.g. COVID** | | |
| **Strategic Governance as required, authorities for global actions. Sets long term strategy.** | | Chief Executive Officer |
| COO Operate the asset Managing Director EMEA |
| COO Build The Asset -Managing Director of Design & Construction AMER |
| APAC Senior Management |
| **Regional Head** | **Gold Response Leader** | ELT lead to oversee recovery. |

| **GOLD TEAM (STRATEGIC)** | |
| --- | --- |
| **COO Operate the Asset Managing Director EMEA** | **Supports/directs COM monitors impact on operational risk register for site** |
| **Group HSQE Director** | **Oversee the HS&E issues** |
| **Head of Legal EMEA** | **Functional Advice & Command Support** |
| **People Director** |
| **Group Commercial Director** |
| **Global Security Manager** |
| **Head of Facilities** |
| **Marketing Communications Director** |
| **Head of IT** |
| **COO Design & Construction or Deputy** | **Impact Planning, command support** |

| **SILVER TEAM (TACTICAL)** | |
| --- | --- |
| **Regional Operations Manager COM**  **(Silver Team Leader)** | **Authority to invoke BCP, LMT Team leader.** |
| **Customer Services / Client Liaison** | **Assist in customer communication and commercial decisions** |
| **Regional HSE Manager** | **Site lead for HSE** |

**Additional members may be added depending on the incident, function and region. From e.g. People, IT, Marketing**

| **BRONZE TEAM (OPERATIONAL)** | |
| --- | --- |
| **Site Lead** | **Person with responsibility for response at the location** |
| **Facilities Shift Manager(s)x5**  **(Trigger Role)** | **Incident management process, recover technical situation, contractor management** |
| **Facility Services / Contractors** | **Assist and support the facility manager / Act as Emergency Services Liaison** |
| **Team leader for FM Contractor** | **Relocating, security, cleaning and reception services** |
| **Team leader for Security Contractor** | **Assist and support the facility manager and recovery of the data centre** |

**Additional members may be added depending on the incident, function and region. From e.g. People, IT, Marketing.**

## Appendix 2. Salvage Team

Contact should be made with the insurance company before any salvage is undertaken as it is likely that they will be able to provide expertise and resources.

Depending on the nature and severity of a disaster at the affected site, emergency services may allow a company Salvage Team into the building to retrieve personal effects, equipment and files. Co-ordination should be made with the Incident Commander. A corporate decision will have to be made as to the priorities given to the Salvage Team, especially if the site is in a bad condition, access is for a limited time and further access is unlikely.

The IMT will need to co-ordinate any information gathering exercise for personal effects, with the type of item and description, location (and where any keys are, if the location is likely to be locked) and value (physical or emotional).

If information is to be retrieved, consideration should be given to the type of material, the nature of the incident and the effect this combination could have had. For example, if paper material is to be salvaged from a fire damaged site, there is the possible combination of the effects of fire, smoke, heat and water. Specialist data retrieval companies exist and may be procured by the insurers.

All departments will need to clearly define any documents and files required and their location. The following Appendix should be used.

## Appendix 3. Salvage Team Recovery Request Form.

The Salvage Team will be appointed post-event.

To be completed for salvage:

| **Department** | **Items Required** | **Location** | **Notes** | **Priority** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Appendix 4. Recovery Site Contacts

In the first instance, staff will work from home in addition to using spare office space (i.e. it may be that only a portion of the office is unavailable or the alternate office can be used).

If required, alternative locations can be arranged. Preferred suppliers (e.g. Regus) and contact details are documented in the local BCP. Facility Management may be contacted for assistance.

## Appendix 5. Succession Planning

**Gold, Silver and Bronze Team members and successors for each location will be appointed from existing resource at the time of incident and details recorded in regional BCPs’ logs.**

## Appendix 6. Telephone Cascade

The telephone structure for each location is detailed in the localised BCP.

The latest version of the Yondr organisational structure is held within the Yondr HR system – ‘HiBob’.

## Appendix 7. Meeting Agenda

1. Names of any Team members not successfully contacted -reasons
2. Details and latest report of incident as known – injuries to people, damage to premises, equipment etc.
3. Likely timing and contact for next report.
4. Initial extra management resource sent as back-up to the catastrophe location.
5. Extent of damage – habitable/part habitable/non-habitable.
6. Success in containing all staff based at damaged location.
7. Extend and types of media attention.
8. Spokesperson appointed confirmed / statement issued.
9. Which specific plans to be activated
10. Define immediate needs:

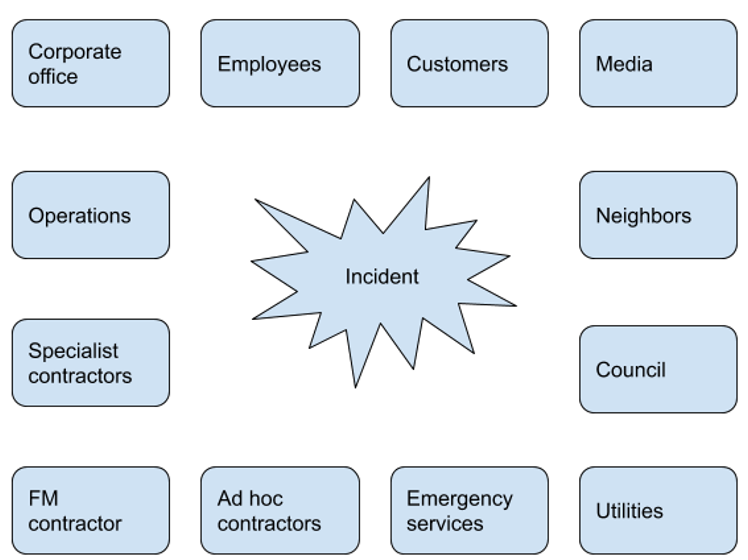
| Accommodation | Special Requirements | Telecom |
| --- | --- | --- |
| Furniture | People | Computer |
| Transport | Temporary Task Force |  |

1. Need for additional resource to provide immediate needs
2. Own insurance Advisor appointed.
3. Date and time of visit to site to verify facts and plan future action.
4. Location of meeting place close to damaged site.
5. Future action to be taken by each team member clearly understood.
6. Date, time and place of next meeting.

## Appendix 8. Internal Contacts - Staff

A full list of staff and other internal contact details is held in the Yondr HR system – ‘HiBob’.

## Appendix 9. External interested parties - defined



## Appendix 10. Bank Account Details

Lloyds - Kingston Branch

## Appendix 11. Battlebox contents

Battleboxes are located on G Suite.

Documents and data:-

Business Continuity Plan

Staff contact details

Client contact details

Key supplier contacts

Fixed Asset Register

Bank account details

Company headed paper and stationery.

Electronic copy of office floor plans

IT Documentation esp. Network diagram and IT DR procedures

## Appendix 12. Emergency Evacuation Plan

In the event of an evacuation alarm being sounded, follow the instructions contained in your office Emergency Evacuation Plan, and assemble at the primary meeting point. Due to the nature of some threats, your primary meeting point may be within an emergency services exclusion zone. If this is the case, you should assemble at your secondary meeting point.

If you receive instructions from the emergency services, these override the company plans. Some incidents will occur where it is safer to remain in the core of the building. In this case, follow the instructions to assemble at your invacuation point or safe internal area.

For detailed information regarding the location of primary and secondary meeting points, refer to the ~~Yondr~~ Emergency Evacuation Plan for your location.

## Appendix 13. Activity Log

The activity log should be used to record actions, information and communications during incidents. It should contain details from the time of Plan invocation through to being stood down. The log should be submitted to the IMT and retained for the post incident review:

| **Action Taken** | **Authorised by** | **Date & Time** | **Any other Comment** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Appendix 14. Key Holder Rota

Keyholders:

| **Location** | **First Point of Contact** | **Out of hours contact details** | **Second Point of Contact** | **Out of hours contact details** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Details will be included in localised BCPs

## Appendix 15. Local, Regional and National Advisory Systems

Local and regional advisory systems will be utilised where appropriate to provide regional specific information e.g.

World Health Organisation

<http://www.who.int/csr/don/en/index.html>

Weather Warnings

<http://www.metoffice.gov.uk/public/weather/forecast>

*Further details regarding local / national advisories will be included in the localised version of the BCPs*

## Appendix 16. Insurance Company

The Legal Department will manage communication with the insurers. Where appropriate, Office Managers / Campus Leads should forward information to the Legal Department.

## Appendix 17. IT Topography, Restore Details and Telephone Diversion Procedures

**Refer to the IT Disaster Recovery Plan held by IT.**

**Website amendments** are carried out by members of the Marketing team.

**Telephone Diversion Procedure** if required, management of the transfer of telephone lines will be detailed within the localised versions of the BCP.

## Appendix 18. Holding Statement and Process of Release

The following can be adapted for immediate response to an incident. All such communications wherever possible should be referred to the IMT for approval prior to release to the press / media.

Today at (insert time and explanation of what has occurred).

*[If relevant, thank the emergency services for their response.]*

*[If staff are missing / injured then do not give details (“I don’t wish to speculate at this time” can be used to rebuff questions) and confirm that the emergency services are leading the operation with your full cooperation.]*

We have invoked our business continuity plan, and our operations are being restored from our recovery site. Clients should not notice any variation in service quality. We are in contact with the (families, clients, stakeholders, suppliers, etc depending on the nature of the incident).

The company has a helpline number which is XXXX. At this time, clients are requested to call only if they have an urgent enquiry. We will be issuing regular updates through [website / media / local radio]

The following adds more detail to the process of dealing with the media.

**Process of release**

The most difficult aspect of PR to handle is bad news. But there are ways of handling it to ensure damage limitation, or even to turn bad news to your advantage.

The media can become your best friend post-incident. Journalists are not all out to trick you and make it up as they go along. If you follow a few basic public relations rules, a crisis could become the basis of positive publicity.

Below are few guidelines as to how to cope:

1. Don’t say no comment
   * it looks as if you have something to hide
   * if a journalist can’t get the right info from the top, they will seek it (and get the wrong info) from the bottom.
2. Forget trying to keep bad news quiet
   * news travels fast and bad news travels fastest, particularly if you have lots of staff
   * Plan A might be to keep a lid on it, but Plan B must be how to deal with it if word gets out
3. Preparing a written press statement: what to say
   * issue a press release. Get professional help to write it if need be.
   * stick to the facts – honesty is the best policy
   * keep it simple: who, what, where, why, when and how
   * don’t think one sentence will do the trick. A little info is as bad as saying nothing. If journalists cannot get more info from the top, they’ll start digging at the bottom – that’s their job
   * don’t try burying the bad news in the last paragraph
   * don’t be afraid to say sorry. A little concern goes a long way in print
   * when things go wrong and you’re in the damage limitation zone
   * add quotes (short, meaningful and jargon-free). This is what matters most. It’s what your staff and clients will see. The quotes shouldn’t be changed by a good journalist. But if they are woolly, long and riddled with jargon they won’t be used. Worse, your words will be paraphrased
   * ·write what the public will believe
   * add Editor’s notes, history, basic info at the bottom of the press release
   * add spokesperson’s contact details
   * send it to the right department, usually the Newsdesk
   * send a copy to your own staff
   * upload it on to your own website
   * be prepared for a call from a journalist who will want more information and possibly a picture
4. Talking to journalists
   * ·If you have to talk to a journalist in person start by getting a note of their name, phone number and email address
   * listen to the info they’ve already got
   * challenge misconceptions, false assumptions
   * establish what they intend to say, when the story’s going in, and where
   * consider whether to respond now, or later, by phone or written statement. On radio, either live or pre-recorded
   * use simple statements (jargon won’t be quoted)
   * speak slowly and steadily, appearing confident and in control
   * limit response to 2/3 points you think most important
   * don’t fill silences with waffle, especially on radio
   * be positive, especially on radio
   * don’t be flippant
   * don’t be hostile or defensive
5. When the story published is ‘all wrong’
   * there are two sides to every story. And yours won’t be the only one published
   * your press release won’t be used as you sent it
   * use the Letters page to correct false assumptions
   * don’t be rude, be realistic

## Appendix 19. Buffer Time Actions

| **Action** | **Completed** |
| --- | --- |
| Assemble (physically or virtually) the IMT |  |
| Advise departmental managers that the BCP might be implemented |  |
| If the event is wider than Yondr (for instance an exclusion zone / transport chaos) monitor information sources |  |
| If IT is down or there is a data breach, do not delay and inform the IMT immediately |  |
| Establish lines of contact with the emergency services |  |
| If the incident has caused casualties implement HR policies for retrieving next of kin information: make this available to and maintain ongoing liaison with the emergency services and hospitals |  |
| If there is structural damage to the building advise repair contractors of the scale and earliest access to site |  |
| If there is damage to services advise the service suppliers of the scale and earliest access to site |  |
| Prepare external press releases |  |
| Contact office brokers or serviced accommodation suppliers and establish sites available, timescale to occupy and payment terms |  |
| Prepare the voice supplier for transfer of lines. Clarify the numbers to be moved and the numbers they are to be moved to |  |
| Advise staff that they may need to relocate to the recovery site |  |
| Inform PR resource |  |
| Test access to details for stakeholders and other information stored offsite for immediate access in time of emergency, to be used until systems are restored |  |
| If staff cannot work at the site, either because the site is inaccessible or services are unavailable, implement the staff cascade |  |
| If the building is inaccessible ensure that it is secure |  |
| Inform the insurers that there is potentially a claim, arrange for a loss adjuster visit |  |
| Inform the bank that Yondr might need emergency cash funds and emergency banking arrangements |  |
| Review point at which clients should be informed that there is a difficulty |  |

## 

## Appendix 20. Pandemic Actions

**Background**

These notes refer to situations where large numbers of staff are absent from the office at the same time due to a Virus, either through their own indisposition or the indisposition of a dependent or dependents. The absences may be repetitive due to external influences (e.g. school closure) or because the individual has been infected and then subsequently absent on further occasions because their dependents are infected.

**Scope**

A virus can affect people of any age group.

**Procedures**

The World Health Organisation (WHO) has a scale which it increases if the disease is becoming more threatening to humankind or the seriousness of the outbreak is escalating. Information is available at [www.who.int](http://www.who.int/).

Key advice will be based on the concept of ‘social distancing’. As the virus is thought to be transmitted in saliva, particles shouldn’t be able to travel great distances. As well as direct contact, it is possible to transmit via a third party, e.g. door handles.

The government has imposed restrictions on the assembly of large groups, e.g. sports crowds and public transport with schools closing. International travel is also restricted or completely barred.

**What can you do?**

It is worth considering at the outset that it will be very difficult to avoid exposure to a virus.

Generally, in terms of social distancing, think about where and when you have large assemblage of people, and how you can avoid this. Examples on first knowledge of the virus include:

* Working hours. Many people generally enter and exit the building together when they all have the same working hours. Consider staggering the working hours of each floor or department, so that there are fewer people entering or exiting at any one time.
* Quarantine floors. Whilst face to face contact is useful to many business processes, is it essential? By isolating each floor from any other you may help to limit the spread of the virus.
* Lunch arrangements / Coffee bar arrangements. Consider staggering lunch hours to limit the number of people together at any one time. There are likely to be additional Health and Safety measures imposed.
* Video/voice conferencing. Can traditional face to face meetings be conducted by video/voice conference?
* Meetings. Eliminate meetings wherever possible. If face to face meetings are unavoidable consider the use of face masks (ensure there are adequate disposal facilities for used masks)

Specific early actions defined by Business Asset (before any stay at home or school closures by the government)

* People
  + Urge caution and best to report symptoms asap
  + Reintroduce handwash gels etc
  + Think about agency staff / freelancers who may be outside of the scope of your comms and policies
  + Think about parents and also staff looking after elderly – can they be allowed to work from home for a period?
  + Test any staff cascade now to make sure that it is being received by everyone
  + Appoint a lead for monitoring human resource levels and cascading / escalating relevant information
* Self-isolating
  + Will people be allowed to self-isolate with no symptoms showing either themselves or from colleagues?
  + Think about increased cleaning for e.g. the lifts, canteen, meeting rooms etc
  + Close public access to offices / reception areas but point people in the direction of alternative means of communication with the organisation
  + Consider security of the building if closed for prolonged periods
  + Does home working comply with Health and Safety policies, especially over a prolonged period?
* IT / Data
  + Home working – are staff taking laptops home as a company policy?
  + Remote access. Do you know for certain that if all staff were home working that there is enough bandwidth for concurrent use?
  + Do staff have access to the relevant files / folders if homeworking?
  + Is the data secure if staff are using their own computers? Can sensitive data and conversations be overheard by people outside your company?
* Transport
  + Technically networks could be closed, but it is probably more relevant that the fear factor of public transport may come into play – answer – remote working.
  + Do you need a policy on business travel? There is little you can do about personal travel.
* Suppliers / freelancers
  + Can you check the policies of suppliers who are visiting the site?
  + Can your suppliers still maintain a supply of critical terms?

Also consider enhanced cleaning schedules. This need not be through external cleaners, but through education of your workforce. Alcohol wipes and hand wash provide an effective deterrent to the virus, and staff should be educated in their use. If you are likely to use these, it is worth remembering that as soon as it is mentioned in the press, stocks will run low nationwide.

You should also record all procedures that you put in place, and how staff are informed. Whilst one would hope it is unlikely that you would be challenged after the event, it will be helpful if you can show that you have discharged your duty of care to all staff.

You will also need to appoint someone to monitor the situation and give early warnings where staff levels are falling dangerously low in any area of the operation. This should not only cover absences but also monitor the progress of recovery (when are people likely to return to work, if they or their dependents are hospitalised, deaths of employees and / or dependents and appropriate support and counselling). Forecasting should be considered and transfers from less critical to more critical posts planned, for identified capable individuals.

**Other Points to Consider**

* You should have an idea of how many of your staff would be required to care for children who could not attend school, or where other childcare arrangements ceased to function.
* Consideration needs to be given to not just staff with children of school age. Any staff with dependents of any sort will have to be given sufficient flexibility to care for their dependents and reduce the likelihood of spread of pandemic to a minimum. There is also the issue of whether or not staff will be able to work if they are supervising children.
* Home working. Whilst your IT infrastructure may support home working, do staff have the necessary equipment or space to work from home? How will this be impacted if schools are closed?
* Impact on infrastructure. With many industries predicting absence rates of 50% or higher, you need to be aware of the ‘bigger picture’. It is impossible to predict, but consider issues such as withdrawal of public transport, ongoing planned or spontaneous loss of utilities, perceived shortage of staple foodstuffs (lack of products in shops is more likely to be an effect of transport problems and panic buying).
* Perhaps most importantly, whether people will want the services we are supplying. There is no point being up and running if you have low demand from clients in a similar situation and in turn their clients. In any event it is important to involve your staff in this exercise – as well as demonstrating to them that you are planning for them; they are one of your greatest resources!

Specific later actions defined by Business Asset (after stay at home, lockdown and school closures announced by government)

* People
  + Will remote workers be allowed time off for childcare?
  + Do you need to double up now on staff resourcing critical activities due to childcare?
  + Are you in a business where you need to increase staffing, for example home deliveries?
  + What training or procedure documentation can be provided to enable a multi-tasking workforce?
* Premises
  + If you are in a multi-tenanted building, have any other tenants had a case/outbreak?
  + Think about what security arrangements are in place for a two to three month closure.
* Equipment and supplies
  + Office / IT equipment such as desks, chairs, computers, monitors, printers etc.
* IT/ Data
  + Agile working – do you have sufficient licence / secure access to the network for critical staff, including those who have career responsibilities. Do they have the appropriate equipment (e.g. laptops, phones, payment card readers) and access to Wi-Fi?
  + Can you use landlines, Skype, Google Chat or WhatsApp as alternative forms of communication if staff are home working?
* Transport
  + Consider your reliance on Logistics requirements, particularly fuel. It is difficult to estimate but you need to be thinking about specific scenarios, for example if the Oil Refineries close down due to staff shortage.
* Suppliers / contractors / freelancers
  + Seek alternative suppliers / contractors required for maintaining critical functions now
  + Are you able to maintain supply if your business is in retail?
* Finance
  + Do you have clients that are at risk of going under? What is your situation with creditors? What is your insurance cover?
  + Will you need additional liquidity from a bank?
  + Issue further credit-cards where needed to enable crucial spend to be immediate
  + Is there an impact on investments / pension funds from the stock market and interest rate falls?

## Appendix 21. Impacts of not performing activity

The following table identifies the impact over time of not performing each business critical activity.

| **Activity** | **< 24 hours** | **24 – 48 hours** | **48hrs – 1 wk** | **> 1 week** | **> 1 month** | **> 3 months** |
| --- | --- | --- | --- | --- | --- | --- |
| Marketing |  |  |  |  |  |  |
| Operations |  |  |  |  |  |  |
| Commercial |  |  |  |  |  |  |
| Design and Construction |  |  |  |  |  |  |
| Finance |  |  |  |  |  |  |
| People[[1]](#footnote-0) |  |  |  |  |  |  |
| IT |  |  |  |  |  |  |
| CEOs [[2]](#footnote-1)office |  |  |  |  |  |  |

|  | No significant operational impact |
| --- | --- |
|  | Moderate operational impact |
|  | Significant operational impact |

[1] Soft skills support from HR needed in a crisis

[2] Communications needed immediately.

## Appendix 22. Timeframe for Resumptions of Activities / Client SLA’s

The following terms and definitions are taken from ISO 22301, the international standard for Societal security - Business continuity management systems

| **Activity** | **Minimum Business Continuity Objective [[3]](#footnote-2)** | **Recovery Time Objective [[4]](#footnote-3)** | **Target time for Return to Normal Operations [[5]](#footnote-4)** |
| --- | --- | --- | --- |
| Marketing | Ensure Crisis Comms are happening. | Immediate communication. One week for rest of work. | One month |
| Operations | Response to outages needed within minutes. | One hour. | One month |
| Commercial | Ensure processing happens in Yondr Connect. | 48 hours | One month |
| Design and Construction | Ensure that contractors are onsite and working. | 24 hours | Two weeks |
| Finance | Provide cash for immediate response to a crisis.  Pay contractors.  Invoice if possible as payments are not in advance.  BACS payroll as a minimum and pay pensioners. | 72 hours (apart from Payroll – one day).  A recovery point objective of 24 hours is acceptable for electronic data. | One month. |
| People | BACS payroll as a minimum.  To provide any counselling and support to staff. | One week (apart from Payroll – one to two days).  A recovery point objective of 24 hours is acceptable for electronic data.  Immediate support for staff from HR resource. | One month. |
| IT | Provide remote working if possible and communicate with staff in issues and likely restoration times. | One day for IT. | One month |
| CEOs office | Internal and external communications and leadership | 1 hour | One week |

**Customer SLA’s**

Contact Buckingham within **5 minutes** of a major outage

Redbrick?

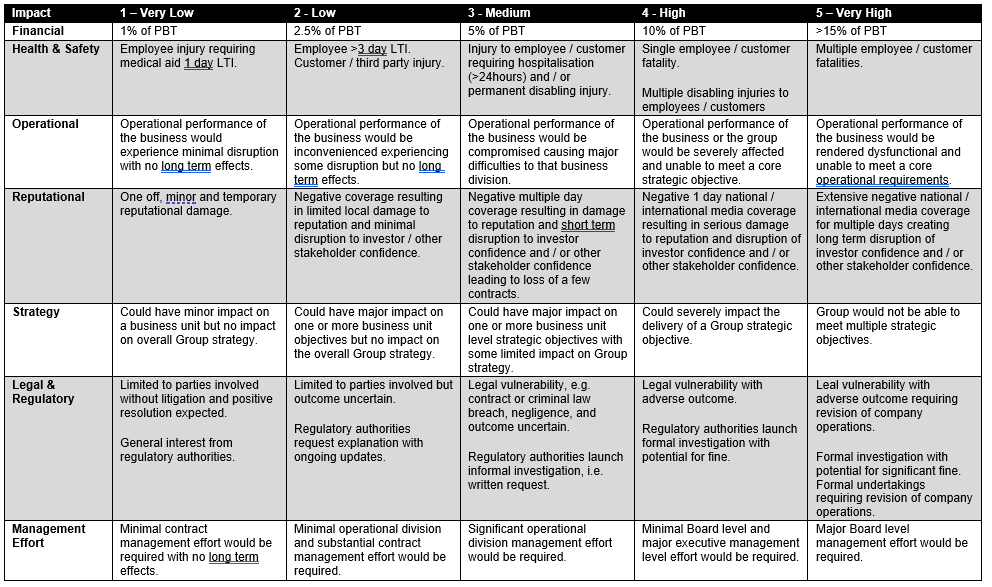
**Data Centre Requirements**

* Maintain temperature: between:18 and 32 degrees
* Humidity: 8 and 80%
* Power outage: Less than or equal to 30 seconds (99.99885%) - non CCNR/SSNR area

## Appendix 23. Resource Requirements

| **Activity** | **People** | **Information and data** | **Buildings, work environment and utilities** | **Facilities, equipment and consumables** | **Technology** | **Transport** | **Finance** | **Partners and suppliers** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Marketing | Six internal staff. Also external design team and copywriter. | Network data. | Can work remotely. | Material for events. | G Suite, Adobe, IFS, phones.  Text Magic.  Website.  LinkedIn. | n/a | n/a | Translators, Copywriters, Designers. Printers.  Mystique, Adobe. |
| Operations | 17 Ops staff. CBRE facilities staff. | All network data. | DC and remote working.  Power and generators. | Kitted out DC with all facilities and security systems. | BMS, Power Management Systems, G Suite, Maximo, Fire and Security systems. | Access to DC for goods in and out. | n/a | Engie, subcontractors (there are successors). |
| Commercial | Two staff | Network data and Yondr Connect. | Could work from home. | Office kit. | G-Suite, OCG platform. | n/a | n/a | OCG |
| Design and Construction | Up to staff and 3,000 contractors | Network and Cloud | Office space but can work from home.  Onsite – all Utilities, powerplants, security, networking, PPE etc | All contractors kit needed and machinery. | Telephones, network data and G-Suite, MS Office, email, internet, Primavera, Procore | Goods in to sites and waste removal.  Normal staff transport to the office and site meetings. | Staff could expense minor costs and claim back.  Contractors will finance materials needed | Jones Engineering, Blu-3, Ardmac, yondr tech, Logitech, Ask romein, H&MV (substations), ISG |
| Finance | 11 staff and HLB partner staff for AP.  ADP for payments to Netherlands staff.  Would also require authorised bank signatories. | Network and system data.  Paper invoices (which are later scanned). | Could work from home. | Could purchase IT equipment and stationery locally.  Banking cards and readers. | PCs, phones, printers, network data.  G Suite, IFS, Hibob, banking portals. | Normal staff transport to get to site. | Immediate payment could be made by company credit card. | HLB, ADP, Bank, BDO. |
| People | Two staff in Aldgate, three in Amsterdam.  L&D manager and talent acquisition in Amsterdam and one recruiter in Aldgate. | Network data, Celergo, Hibob.  HR paper files (mostly archived). | Could work from home. | Could purchase IT equipment and stationery locally. | G Suite, Celergo, Hibob, International SOS, Text Magic, PCs, phones, printer, network data. | Normal staff transport to get to site. | Immediate payment could be made by company credit card. Also, have credit accounts with the majority of suppliers. | Celergo (ADP), HiBob. ASR, Scottish Widows, De Goudse, leased car providers. |

## Appendix 24. Decision to invoke



## Appendix 25. Assumptions

The plan makes assumptions in the following areas:

**Geographical Assumptions** – that an incident that affects Yondr will not affect the recovery sites (i.e. other offices / homes) at the same time (with the possible exception of severe weather, catastrophic loss of IT systems and national pandemic lockdowns).

**Personnel Assumptions** – whilst the loss of some staff is covered by succession planning and external contractors, the plan assumes that the majority of staff will be available for the recovery process.

**IT Assumptions** – that the back-up process meets the defined needs of the business in terms of Recovery Point and Recovery Time Objectives. Where it does not, source documentation required for the recreation of electronic data is available. Any electronic data that is required for recovery is held on network drives, rather than on local drives which are not backed up.

**‘Overwhelming Events’** – however comprehensive the Business Continuity Plan is, an event may occur which exceeds Yondr’s ability to recover using the resources available to it. In this situation a decision will be made elsewhere as to the future of the business, which may or may not be restored. This decision is outside the scope of this BCP; however, the information contained may assist in the final outcome.

## Appendix 26. Communication Log

| **Date** | **Time** | **Type**  Tel, Email, Fax, other | **Originator** | **Priority**  Routine, Urgent, Immediate | **What is being reported?** | **Decision / Action taken** | **Follow Up**  Date/Time |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

## Appendix 27. Incident Reporting Sheet

**INCIDENT REPORT**

**DETAILS**

| **Date** |  | **Time notified** |  |
| --- | --- | --- | --- |

| **Incident Description** |  |
| --- | --- |

**CALLER**

| **Notified by (name)** |  |
| --- | --- |
| **Role / Title** |  |
| **Contact telephone number(s)** |  |
| **Email** |  |

**METHANE**

| **M** | **Major Incident declared?** |  |
| --- | --- | --- |
| **E** | **Exact Location** |  |
| **T** | **Type of incident** |  |
| **H** | **Hazards present or suspected** |  |
| **A** | **Access - routes that are safe to use** |  |
| **N** | **Number, type, severity of casualties** |  |
| **E** | **Emergency services present and those required** |  |

**ACTIONS**

| **Has the incident resulted in evacuation?** |  |
| --- | --- |
| **Have the appropriate Gold Team member(s) been notified of the incident?** |  |
| **What actions have been taken so far?** |  |

## Version control

| **Revision** | **Date** | **Review by** | **Notes** |
| --- | --- | --- | --- |
| 3 | April 2020 |  | ISO 22301 / COVID-19 |
| 4 | May 2020 |  | Updates from WW and IMT info updated |
| 5 | May 2020 |  | Details of other documents (pg. 2) added and IMT structure updated |
| 6 | June 2nd 2020 |  | Succession planning C-suite added |
| 8 | Feb 21 |  | Design and Construction added |
| 9 | Mar 21 |  | IMT structure updated |
| 10 | Mar 21 |  | IMT structure amended to be more generic |
| 11 | Apr 21 |  | Section 3.1 updated and App 27 added. |
| 12 | Jun 21 |  | Contents table added. Invocation details expanded. |
| 013 | 03 Aug 21 |  | Formatting changes (Footer / version control) |
| 014 | 17 Aug 21 |  | Section 3.8 added |
| 015 | 31 Aug 21 | July 2022 | Client SLA’s added to Section 6.2 and Appendix 22. Section 7.9 updated |
| 016 | 13/7/22  22/08/22 | Dec 22 | Removed Tech  Title changes to reflect new Org Chart |
| 017 | Feb 2023 | July 2023 | Several changes post re-org and review meetings |

1. Soft skills support from HR needed in a crisis [↑](#footnote-ref-0)
2. Communications needed immediately. [↑](#footnote-ref-1)
3. minimum level of services and / or products that is acceptable to the organisation to achieve its business objectives during disruption [↑](#footnote-ref-2)
4. period of time following an incident within which product or service must be resumed, or activity must be resumed [↑](#footnote-ref-3)
5. the length of time after which all elements of the service are once again being delivered [↑](#footnote-ref-4)