BUSINESS CONTINUITY POLICY

Policy Owner:	VP Global Security & Business Continuity
Approval authority:	ELT operations board
Version:	2.0
Approval date:	28-05-2025
Effective date:	28-05-2025

01. Purpose

This Business Continuity Policy aims to ensure that Yondr can respond to and recover from business-interrupting events, continue to meet stakeholder requirements with minimal disruption, and remain a profitable concern.

This Policy supports Yondr's Business Continuity and Information Security Management Systems, which highlights the systems and processes necessary to maintain and continually improve the Information Security and Business Continuity performance and efficiency within Yondr, and enables Yondr to set and achieve objectives and targets, to take actions as needed to improve its systems, and to demonstrate the conformity of its systems to the requirements of the ISO 22301 and 27001 standards.

Yondr's Business Continuity specifically aims to:

- **Minimise Disruption:** Ensure that there is no material impact on interested parties from disruption to Yondr's functions. Feedback is monitored to ensure that there is no or minimal disruption to services because of business continuity incidents.
- **Ensure compliance:** Meet any future regulatory and/or statutory requirements for business continuity.
- **Build confidence:** Create a level of reassurance with new and existing interested parties by demonstrating that the unexpected has been planned for.
- **Monitor risk:** Monitor and act on the level of risk from current threats and potential future threats or accept the level of risk within the risk appetite of the organisation. The risk

register is reviewed periodically and as part of the management review and maintenance procedures.

- **Raise awareness:** Ensure all are aware of the emergency response actions, this Business Continuity Policy and the Business Continuity Plan (refer to Appendix B). This is through training and participation in business continuity exercises.

02. Scope

02.1 Applicability

Yondr is ISO 22301:2019 (Business Continuity) accredited and specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented Business Continuity Management System (BCMS) to protect against, reduce the likelihood of occurrence, prepare for, respond to and recover from disruptive incidents. There is no statutory obligation to have a BCMS, but it is best practice and therefore sponsored by the Board. It is in place to safeguard the public, our people, the business and its customers and ensure that their interests are protected to the highest standard.

This Policy applies to all:

- full-time, fixed term, part-time, PEO, and temporary employees,
- officers and directors,
- interns and secondees, and
- agency workers, casual workers, volunteers, contractors, and consultants, as relevant to the nature of their engagement, and

  who provide work and/or are engaged to deliver goods and services on behalf of Yondr (referred to at times as “we,” “us,” “our,” and “ours,” and includes affiliates, subsidiaries, or entities in which Yondr holds a significant interest), regardless of where in the world they are situated.

This Policy should not be construed or implied to infringe on rights guaranteed by the laws of the local jurisdiction, thus, where this Policy conflicts with local rules, laws or regulations, the local framework shall prevail.

03. Policy requirements

03.1 Risk Identification and Management

Risks, including those that may be relevant to business continuity, are identified and managed in line with Yondr's Risk Management Policy (refer to Appendix B). The acceptable risk for Yondr is low i.e., risk averse as a rule. In the risk matrices, risks and impacts are scored pessimistically. Any material risks which could physically harm the organisation are considered with high importance. Each risk in the risk assessment is treated on its own merit.

03.2 Business Impact Analysis

Business Critical Activities are identified in the Business Impact Analysis (BIA) and their recovery objectives are set. None of the activities of Yondr are excluded from the scope, including any outsourced activities.

Yondr's Global Security Team facilitates a business impact analysis review at least twice each year. This exercise engages the relevant functions and managers from across Yondr to identify, assess and document the potential effects of various disruptions or disasters on their critical business functions and processes. It also considers any legal and regulatory requirements, as well as contractual requirements. This informs recovery efforts, prioritisation and continuity planning. The outcome of this exercise is documented in the Business Impact Analysis document. Relevant risks identified in this process are registered in line with Yondr's Risk Management Policy (refer to Appendix B).

03.3 Business Continuity Plan

The Business Impact Analysis informs the development of the Corporate Business Continuity Plan. This is refreshed at least twice each year and covers invocation criteria, strategies for maintaining or restoring essential operations, communication, resource responsibility and allocation, and recovery processes.

Specific Site Business Continuity Plans are developed and maintained for each office or data centre and stored on the Yondr Global Security SharePoint.

03.4 Communication

The Yondr BCP is published on Yondr's corporate intranet Yondrverse. Updates to the plan are communicated company-wide and to third party partners as relevant. Specific communication requirements during a business continuity incident are included in the Yondr BCP.

03.5 Drill Exercises

Scenario-based Business Continuity drill exercises are facilitated by the Global Security Team at least twice each year. These are conducted to ensure that relevant parties are well-rehearsed in response and recovery processes. The exercise is designed to test:

- The technical, administrative, procedure and other operational systems of the BCP.
- The business continuity management arrangements and infrastructure (including roles, responsibilities, and any incident management locations and resource requirements stipulated).
- The technology and telecommunications recovery, including the availability and relocation of staff.
- Recovery sites and critical vendors, where appropriate.

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).

The performance is reviewed after each drill and a post-exercise debrief report is produced which captures key actions and learning points. Relevant training or process and policy updates are implemented as required.

03.6 Continuous Improvement

Any unforeseen incidents or near misses with an incident severity ranking of P0 or P1 will trigger a review of the Yondr BCP to ensure that any lessons learned will be fed back into the Plan. Any significant changes within the organisation may also prompt a review of the Business Continuity Management System (BCMS).

03.7 Training

Everyone is trained on Business Continuity as part of the mandatory onboarding training curriculum. Third party facilities management service providers run their own drills based on the local BCP. General Contractors do not require training during the construction phase. Incident Management Team members are trained in the implementation and use of the BCP and this is refreshed during the drill exercises. Additional training sessions are arranged as required.

03.8 Incident Management

Incidents occur on an almost daily basis and are governed by the Incident Management Policy (refer to Appendix B).

Incidents may be disruptive and require the invocation of the BCP. During working hours, any incident that could affect Yondr's operations or business continuity must be raised to the relevant Office Manager, Campus Lead or 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 BCP. Out of working hours, each site will follow their respective site BCPs for escalating to the appropriate stakeholders.

Once the BCP is invoked, Business Continuity Policy rules apply and supersede the Incident Management Policy (refer to Appendix B).

03.9 Tools and Recording

Yondr has implemented a specialist tool to record, track and manage any business continuity incidents.

03.10 Building Resilience

To reduce the likelihood or impact of disrupting incidents, Yondr:

/ Maintains a risk register.

/ Considers potential new risks via horizon scanning.

/ Maintains Incident and Business Continuity Plans.

/ Runs exercise drills.

/ Supplies remote working IT equipment.

/ Splits activities across sites.

/ Maintains backup infrastructure.

/ Maintains IT/telephony resilience.

/ Maintains staff succession plans.

/ Identifies back-up suppliers.

/ Trains staff to support other roles.

/ Trains the IMT in crisis communications.

03.11 Non-Compliance

Failure to comply with this Policy and Associated documentation may lead to disciplinary and/or legal action.

04. Roles and responsibilities

The Board has overall responsibility for Business Continuity. In addition to roles and responsibilities noted in Section 3, the following also apply:

04.1 All covered by this Policy

/ Conducting their activities in accordance with this Policy and reporting any security related concerns or incidents.

/ Promptly disclosing any potential policy breaches they become aware of.

/ Communicating Yondr's policies to third parties where required.

/ Reporting incidents and potential risks in a timely manner.

/ Following the instructions of the IMT.

04.2 Line Managers

/ Ensure team members understand this Policy and abide by it.

/ Provide guidance as necessary.

/ Consult with those who request such under this Policy.

/ Ensure staff report incidents and potential risks in a timely manner.

/ Responsible for the continuity of their team's activities and their safety, security and welfare.

/ Participate in annual drill exercises.

/ Confirm the safety of their staff in the event of an incident and manage the resumption of their activities with support from the IMT.

/ Support the identification of lessons learned.

04.3 People Team

/ Provide guidance as necessary.

/ Consult with those who request such under this Policy.

04.4 Workplace Director / Campus Operations Managers

/ Maintenance of the Site Business Continuity Plans.

/ Initial response to incidents and escalation to the IMT.

04.5 VP Global Security & Business Continuity

/ Maintenance of the Corporate Business Continuity Plan.

4.6 Incident Management Team

/ Decide whether to invoke the Business Continuity Plan.

/ Response for strategic and tactical recovery decisions.

/ Initial communications to relevant parties regarding the invocation of the Plan.

Appendix A: Key terms

Business Continuity
Yondr's ability to maintain or recover essential functions and services during and after an incident.

Business Continuity Management System (BCMS)
The overarching process encompassing the development, implementation, and maintenance of a Business Continuity Plan to ensure Yondr's ability to continue critical operations during an incident.

Business Continuity Plan (BCP)
A comprehensive and documented strategy that outlines how Yondr will continue its essential functions and operations during and after an incident.

Business Critical Activities
Those business functions, resources and infrastructure that may, if disrupted, have a material impact on the ability of the organisation to operate effectively, deliver its products and services, and meet the requirements of its customers.

Business Impact Analysis (BIA)
A systematic process used by Yondr to assess and document the potential effects of various incidents on their critical business functions and processes, helping prioritise recovery efforts and continuity planning.

Incident
A specific event that is currently occurring and has a negative impact on business operations and objectives. It requires immediate attention and action.

Incident Management
The formal process to resolve an incident and prevent its reoccurrence.

Incident Management Teams (IMT)
Teams that manage and co-ordinate Yondr's reaction to large or small-scale incidents aiming to minimise downtime and restore vital functions. They assess situations, make critical decisions, and deploy resources to swiftly implement recovery strategies. Yondr has established three levels of Incident Management Teams:

- **Gold or Strategic Team** responsible for strategic decision making and consisting largely of members of the Executive Leadership Team.
- **Silver or Tactical Team** responsible for overseeing incidents and consisting of the relevant Heads of Department.
- **Bronze Teams** responsible for the Operational response.

Issue

A risk that has materialised and is currently impacting Yondr and/or its ability to achieve its objectives. It is normally ongoing in nature and requires attention and action in the short term.

Risk
An uncertain event or consequence that could negatively impact Yondr and/or its ability to achieve its objectives, but it has not yet materialised.

Risk Management
Activity focused on anticipating risks and putting in place action to reduce uncertainty and impact to a tolerable level.

Site BCP - Corporate Offices
The Workplace Team are responsible for keeping BCPs up to date. These plans detail the required steps to prepare for, respond to, recover and restore the critical functions in the building in the event of an incident.

Site BCP - Data Centres
Each Campus Operations Manager is responsible for their respective data centre Yondr BCP (Emergency Response Plan), with input from the relevant functions. These Plans detail the required steps to prepare for, respond to, recover and restore the critical functions in the building in the event of an incident. CBRE also produce their own BCPs for each data centre.

Yondr BCP
The Global Security Team are responsible for the Yondr Business Continuity Policy and BCP. The purpose of the Yondr BCP is to restore operations and services to an acceptable level within an acceptable time when an event has made normal operations impossible. It is designed primarily for the Global Incident Response Team but may be used by others as an information resource.

Appendix B: Associated documentation

Document name
/ Business Continuity and Information Security Management Systems
/ Risk Management Policy
/ Incident Management Policy
/ Business Continuity Plan
/ Global Security SharePoint