# BUSINESS CONTINUITY AND DISASTER RECOVERY POLICY

**February 12, 2024**

## 1. Purpose and objectives

This document describes the business continuity and disaster recovery measures in place at the level of Power Gold ENP" UAB (the ”**Company**”).

The purpose of the Business Continuity and Disaster Recovery Policy (the “**Policy**”) is to outline the course of action for the continuation of critical business functions and the measures for recovery in the event of a disaster.

This Policy’s main and immediate goals are to:

(i) provide an orderly and efficient transition from normal to emergency conditions;

(ii) provide specific guidelines appropriate for complex and unpredictable occurrences;

(iii) assure consistency in action throughout all levels of the Company and prevent activity inconsistent with the philosophy and policies of the Company;

(iv) establish a management succession and allocate emergency powers and authorities;

(v) provide a standard for testing the implementation of the Policy;

(vi) safeguard the operation of the critical activities and return the same to the normal course of business;

(vii) provide rules on the implementation, functionality, and review of the Policy;

## 2. Applicability

This Policy encompasses a general framework applicable for all potential threats, crises, and emergencies, irrespective of their origin, severity and type, that may affect the Company’s essential operations and disrupt its activity for more than 48 hours. Response to temporary events or business interruptions of less than 48 hours duration is not within the scope of this Policy.

The situations that this Policy covers include, but are not limited to:

(i) the primary facility cannot be accessed due to a natural or man-made disaster (weather events, fire, flood, utilities outages, pandemic, civil unrest, etc.);

(ii) the primary and/or alternate data centre suffers a disruption due to natural or man-made disaster (physical breach, unauthorized access, fire, flood, malware, ransomware, cybersecurity incident, etc.);

(iii) utilities at the primary facility are not available (power, telecommunications);

(iv) access to vital records (servers or systems crash) is lost;

(v) the key personnel, partners or supplier are either affected or significantly impaired from performing their duties or conducting business as usual.

Based on the information available when the threat or disruptive event occurs, the Policy will be activated by the Emergency Lead, as defined at Section 4, in case of a business interruption lasting longer than 48 hours.

## 3. Assumptions

The Policy has been developed according to the best practices in continuity and disaster recovery planning and pursuant to performing a business impact analysis and a risk analysis. The assumptions below describe the state of the premises, data centres, and the organizational and technical measures in place at the Company level.

### 3.1. Premises

The Company's registered office is located at Architektų g. 56-, LT04111 Vilnius, Republic of Lithuania.

The Company's physical office is located at Jankiškiq g. 43A (unique No. 1098-8004-2017), LT-02300 Vilnius, Lithuania.

Both the registered office and the physical office have access to essential utilities for carrying out the activity in optimal conditions. Also, the security and protection of these offices is ensured with adequate security elements, while the physical office benefits from 24/24 surveillance and monitoring.

In the event that access to these premises is compromised for 48 hours or more, or if the utilities essential to the Company's operation are interrupted for more than 48 hours, the Company's activity will not be affected and will be able to continue as usual since:

- the Company has developed its own Aurora blockchain based on an Ethereum Layer-2 built on top of NEAR Protocol that is hosted in Aurora Cloud and not on prem – see more details at Section V.5., from withe paper at https://www.datocms-assets.com/105238/1701851525-whitepaper_release1_en_20231129.pdf;

- the KYC and KYB activities are supplied by Synaps - https://synaps.io/ - based on an individualized back-office online platform developed, operated and owned by the same through which the potential investors data may be collected and verified;

- the Company's business model and architecture allows it to function properly even remote and online as the Company's employees and management as well as interested collaborators and investors can interact and support the Company's business and operations in a normal way without being affected by possible crisis situations; the registered office and the physical office are more relevant only from an administrative and regulatory perspectives, with a low impact on the Company's operational activity.

The Company’s IT services are provided by a specialised external IT services provider, respectively Zenos (Orizont Business Intelligence Srl), www.zenos.ro (the “**IT Services Provider**”); the IT Services Provider assures technical assistance 24/7.

### 3.2. Data centre, access to data and back-up

The Company server is stored in a cloud-based solution, while the back-up is done via FTP on an external storage box in the datacentre. The server can be accessed from the laptop only through a password protected VPN connection. The contents of the server are backed up daily.

The Company has a strict procedure of saving the documents on the server immediately after receiving the same from our customers, suppliers, collaborators, employees, etc. The staff is trained and follows the procedure of saving the documents in the dedicated folders for each client, customers, suppliers, collaborators, employees, etc. and no documents will be saved elsewhere.

Each collaborator and/or employee has access at an on-premises device and/or a laptop. For the purpose of communicating between us, with our clients, with our vendors or any third parties we use Microsoft Outlook and we have a business subscription to Microsoft Office 365.

### 3.3. IT architecture behind the Company's business model

Data collected for KYC and KYB purposes is stored in a secured personal back-office space provided by Synaps, into which access is provided by way of 6-digits code authentication process.

Furthermore, the Company‘s business model is based on Aurora environment which is Ethereum Layer-2 built on top of NEAR Protocol. Aurora is fully interoperable with Ethereum and all existing Ethereum tools being able to work out of the box.

NEAR Protocol is a blockchain-based, ultra-scalable, developer-friendly platform for decentralized applications. NEAR’s platform provides decentralized storage and compute that is secure enough to manage high value assets or identity information.

Validators are responsible for creating new blocks and verifying the transactions contained within them. They do this by running a node that maintains a copy of the blockchain and participating in consensus rounds to determine the next block in the chain.

With Aurora Silo customers can implement multiple-levels of access control, perfect for KYC/AML-restricted "permissioned" environments, members-only access to games, or any context requiring the management of network access and activity — and without closing the door to interoperability and cross-network composability with public protocols like Ethereum, Aurora or NEAR.

## 4. Emergency Team and communication

### 4.1. Emergency Team

The Emergency Team is responsible for centralized crisis management and for ensuring a smooth transition from normal to emergency conditions and consists of:

(i) the Emergency Lead;

(ii) the Co-Founding Shareholders of the Company;

(iii) the representative of IT Services Provider.

The Emergency Team can and will take any other appropriate measures to safeguard the interests of the Company and to protect the security, health and safety of its staff.

The contact details of the Emergency Team members are listed in the table below.

| Role | Name | E-mail / mobile |
|---|---|---|
| Emergency Lead (Co-Founding Shareholder) | Florin Danilov | florin.danilov@powergold.tech<br>(00 40) 752 161 977 |
| Co-Founding Shareholders | Laurențiu Udrescu | laurentiu.udrescu@powergold.tech<br>(00 40) 0722 942 815 |
| | Gelu Maravela | gelu.maravela@powergold.tech<br>(00 40) 723500005 |
| Representative of IT Services Provider | Horia Șerban | horia.serban@zenos.ro<br>(00 40) 744 620 013 |

The Emergency Lead will regularly check and update, if necessary, the contacts list and the contact information.

### 4.2. Communication guidelines

To ensuring a transparent communication and decide the next steps to be taken, the Emergency Lead will follow the below steps:

(i) immediately contact the other members of the Emergency Team via phone;

(ii) if the Emergency Team's members cannot be reached by phone, immediately send text message and e-mail, requesting confirmation of receipt; alternatively, Slack, Telegram or WhatsApp will be used too;

(iii) immediately contact the relevant client, customers, suppliers, collaborators, employees via phone and, in case no answer is received, immediately send text message and e-mail, requesting confirmation of receipt.

The Emergency Team has the responsibility to notify:

(i) the staff about the activation of the Policy and indicate the immediate actions to be taken by the same (stand-by, telework, wait for further instructions);

(ii) client, customers, suppliers, collaborators, etc., for whom the Company must meet deadlines and whose projects are directly and significantly affected by the disruption.

### 4.3. Emergency contacts

In case of occurrence of a disaster to the premises of the Company, the emergency contact is the Emergency Lead followed by the Emergency Team if the former is not available.

In case of a disaster to the data centre, the emergency contact is the representative of the IT Services Provider or the Emergency Lead should the former is not available.

### 4.4. Order of succession and delegation of authority

The order of succession list below provides the order and protocol of succession for the leadership of the Company.

| Order | Primary | Alternate |
|---|---|---|
| Emergency Lead | Florin Danilov | Laurențiu Udrescu<br>Gelu Maravela |
| Co-Founding Shareholders | Laurențiu Udrescu<br>Gelu Maravela | Florin Danilov |

In case of a disruptive event, the Co-Founding Shareholders and the Emergency Lead or specifically designated successor maintains authority to delegate authority with or without the need for succession. The Company's leadership will be responsible for such functions as business recovery management, staff notification, coordination and oversight for resumption of normal operations.

## 5. Essential functions of the Company

The Company essential functions have been determined based on the business impact analysis and are listed in the table below.

| No. | Essential function | Recovery time objective | Priority rating | Dependencies |
|---|---|---|---|---|
| 1. | Consultancy and assistance services | < 6 hours | Critical | • Electricity;<br>• Access to internet;<br>• Access to server;<br>• VPN;<br>• Postal services. |
| 2. | Representation of clients | < 6 hours | Critical | • Electricity;<br>• Access to internet;<br>• Access to server;<br>• VPN;<br>• Postal services. |
| 3. | Billing and payroll | < 24 hours | High | • Electricity;<br>• Access to internet;<br>• Access to server;<br>• VPN;<br>• Postal services;<br>• Finance Manager;<br>• Access to the billing platform. |

## 6. Vital records

Vital electronic records, files and databases are needed to perform essential business processes, conduct key business operations while the Policy is activated, and to reconstitute normal operations after the event. The Company has a "*no hard copies*" and "*no originals*" policy that is strictly observed by our staff. All our vital records are stored in electronic form on our online server.

All documents and information received from our clients and information related to the administrative and organisational aspects of the Company are saved on the server following dedicated rules.

Our e-mails and sharepoint documents are also uploaded automatically on our cloud solution (Microsoft Office365).

The staff has been instructed not to keep any official documents at the office premises.

## 7. Disaster recovery measures

Depending on the circumstances of the disaster that occurred and based on the information at hand when the Policy has been activated, the Emergency Team will take the following measures:

(i) if the office premises become unavailable, staff will be instructed via e-mail to telework until further information becomes available; confirmation of receipt of the e-mail will be requested;

(ii) return to work will be scheduled and organised in groups; the Emergency Team will develop a spreadsheet describing the schedule and the componence of each group; the spreadsheet will be available on the administrative dedicated folder on the server and sent via e-mail to the staff;

(iii) the Emergency Team will send updates at least each two hours or immediately after new information become available;

(iv) if the disaster renders the access to the server unavailable, the IT Services Provider will re-establish the connection to the server in up to 30 minutes;

(v) before returning to work on the office premises, the Emergency Lead installs, checks and brings all business functions to operational status.

## 8. Policy testing timetable

The Emergency Team members undertake to accomplish evaluations of the Policy recovery processes and procedures and will document the results of those evaluations.

Upon request, our clients can be provided with a copy of the latest records of our Policy and additional documents testing.

Testing, Training Exercise Program below, provides a timetable by which this Policy, and various elements of this Policy are tested and exercised.

| **Test, exercise or training** | **Timetable** | **Comments** | **Actual dates tested or exercised** | | | |
|---|---|---|---|---|---|---|
| Business Impact Analysis | Twice a year | | | | | |
| Business Continuity Policy | Twice a year | | | | | |
| Risk Analysis | Twice a year | | | | | |
| Update Emergency Contact List | Quarterly | | | | | |

| **Test, exercise or training** | **Timetable** | **Comments** | **Actual dates tested or exercised** | | | |
|---|---|---|---|---|---|---|
| Evacuation exercise | Quarterly | | | | | |

## 9. Policy implementation

The person responsible for the implementation, maintenance and review of this Policy is the Emergency Lead.

The Emergency Lead will review the Policy and the data associated with it (business impact analysis, risk assessment) at least once a year. Any changes of the content of this Policy or the data associated with it will be documented and attached to the Policy.

Each member of the Company's staff has been properly trained and informed about their role and responsibilities to assure the implementation of the Policy and the actions that are required on their behalf when the Policy is activated.

A copy of this Policy has been distributed to the staff at the beginning of the collaboration with the Company. A copy of this Policy is also available on the server in the dedicated folder, as well as on the Company's website.

The appropriate implementation of the Policy will be assessed at least twice a year according to the standard described at Section 8.