GRAVITY | PRIVATE WEALTH

Business Continuity Policy

File Information

Responsible Unit	Date of issue	Publication No
Regulatory Compliance & AML	01/08/2024	v.1

Archive History

Publication No	Date	Description of Modifications
v.1	01/11/2024	Original Edition

Board of Directors Approval

Board of Directors	Meeting Date

Table of Contents

1. Introduction 4
2. Scope 4
3. Significant Business Distruptions (“SBDs”) 5
4. Business Continuity Principles 6
5. Organisational structure, Roles and Responsibilities 7
6. Recovery Methods 11
7. Awareness and Training 16
8. Implementation and Review 17
Annex A: Notification priority list 18
Annex B: Damage assessment report template 19
Annex C: Third party contact list 20
Annex D: Systems 20
Annex E: Critical functions 21

1. Introduction

Gravity Private Wealth Ltd (hereinafter the "Company") is an Investment Firm incorporated and registered under the laws of the Republic of Cyprus, with registration number HE 442079. The Company is authorized and regulated by the Cyprus Securities and Exchange Commission (“CySEC”) under license number 447/24.

The Company acknowledges the need to to mitigate the risks associated with business failures which would be caused by an event causing a failure to deliver financial services as a result of a significant business disruption.

In this context, the Company establishes the Business Continuity Policy (hereinafter the "Policy” or the "BCP”) in order to reduce the risk of business failures resulting from business disruptions and safeguard its ability to produce a minimum acceptable level of outputs and services in the event of failures of internal or external mission-critical information systems and services.

2. Scope

The Policy aims at ensuring, in the case of an interruption to the Company’s systems and procedures, the preservation of essential data and functions, and the maintenance of investment services and activities, or, where that is not possible, the timely recovery of such data and functions and the timely resumption of the Company’s investment services and activities.

The Policy sets out the framework in which the Company shall respond to a Significant Business Disruption (“SBD”) event by safeguarding its employees and property, by means of making a financial and operational assessment, quickly recovering and resuming operations, protecting all of the Company’s books and records, and to the extent practicable, allowing its clients to transact business as soon as possible following an SBD. This Policy is assessing the appropriate level of security needed taking into account the risks that are presented by processing, from accidental or unlawful destruction, alteration, unauthorized disclosure of, or access to data transmitted, stored or otherwise processed.

In the event that the Company determines that it is unable to continue its business, the Company will take steps to provide clients with prompt access to investments and the underlying issuers of those investments.

The objectives of this Policy, within others, are to:

- Provide a business continuity planning framework that will ensue adoptability during the time of a major incident or a disaster;
- Minimize the impact than an incident will have on the critical functions, systems and data of the Company;
- Allow for the efficient resumption of business functions, systems and data in the event of a major incident;
- Provide guidelines to all the staff of the Company on the procedures and actions that must be followed in planning for and during the time of a disruption in achieving the recovery of operations;
- Minimize the reputational impact on the Company's image as perceived by clients and the Regulator;
- Eliminate regulatory and financial impact on the Company and financial impact on clients from the occurrence of such events.

3. Significant Business Distruptions ("SBDs")

The Policy anticipates two types of SBDs, internal and external. Internal SBDs affect only the ability of the Company to communicate and do business, such as a fire in its premises. External SBDs prevent the operation of the market, including terrorist attacks, pandemics, city floods, or wide-scale regional disruptions. The response of the Company to an external SBD relies more heavily on other organizations and systems.

Potential impact of an SBD

- Trading and market making: Delays in executing trades, difficulty in managing risk, and reduced liquidity.
- Asset management: Difficulty in managing investment portfolios, reduced access to research, and reduced ability to provide financial advice.
- Payment processing: Delays in processing transactions, difficulties in reconciling accounts, and reduced cash flow.
- Risk management: Difficulty in identifying and assessing risks, reduced ability to implement risk controls, and reduced compliance with regulations.
- Compliance: Reduced compliance with financial regulations, difficulty in managing regulatory relationships, and increased legal issues.
- Customer service: Reduced responsiveness to customer inquiries, difficulties in processing orders, and increased customer complaints.

- Information technology: System outages, difficulty in restoring data, and reduced cybersecurity.

4. Business Continuity Principles

Policy Principles

- A process and a number of provisions is aimed to be developed and maintained for Business Continuity throughout the Company for incidents concerning internal failure of systems and infrastructure, fire, power failure and burglary.
- BCP copies are stored in a remote location at a sufficient distance to avoid any damage from a disaster at the main site. The BCP Coordinator ("BCPC") and Crisis Management Team Members ("CMTM") should ensure that the copies of the BCP are up-to-date and safe.
- All efforts are made in order to apply similar provisions on the alternative location(s), as in the Company's main office.
- The BCP is tested and updated regularly to ensure that it is up to date and effective.
- The BCP considers the following:
    - Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations and to bring business processes back into operation.
    - Resumption activities, which describe the actions to be taken to return to normal operations.
    - The responsibilities of the individuals involved.

Assumptions and Presequisites

- The disaster may occur at the worst possible time. A disaster is any unplanned and unforeseen event outside the ordinary course of business that makes the Company or any significant part thereof inoperable for a period of time.
- Sufficient Management and Staff, who are familiar and trained in the procedures and tasks comprising this Policy, will be available subsequent to the interrupting event to implement response, resumption and recovery. Some of the staff may be unavailable for work following an emergency incident.
- Function's recover priority is set for all critical operations, based on:
    - the maximum time of unavailability and the relative importance of each function to: financial, regulatory, customer and reputational impact. Some other factors such as the specific time of execution of the function and dependency on outside providers.

- the financial, regulatory, customer and reputational impact factors over time.

- Operational flows are established for critical operations and the related contact persons (including external parties) and related systems (including outsourced systems) are identified.
- In circumstances, involving a localized event (i.e. limited to the Company), equipment vendors and local utility companies should normally be able to install replacement computers and communications hardware in one calendar day.
- In the event of a regional emergency, such as an earthquake, the time required to acquire the necessary computer equipment and dial telephone service could be as long as 1-3 days. All business documentation and files that are necessary for resumption and recovery purposes are backed up and stored.
- All computer files required to implement resumption of the current operating environment, and/or that support time-sensitive business operations should be backed up daily on magnetic tapes. The backup tapes are to be stored in a secured fireproof place. In addition, once a year a full back up should be done on a magnetic tape, and the tape should be kept in a safe deposit box.
- In the event of a major incident, such as pandemic or similar event which "work from home" mode can be activated, the Company can provide within reasonable time equipment and remote access for all employees to all their functions including telephone.

5. Organisational structure, Roles and Responsibilities

This section of the BCP defines the Company's Business Continuity organizational structure, the members of the BCP team and their roles and responsibilities.

Business Continuity Policy Coordinator ("BCPC")

The role of the BCPC which is undertaken by the General Manager is to take ownership of the BCP and the coordination of the overall activities. BCPC works closely with Crisis Management Team and manages the overall recovery activities. This includes but is not limited to the below:

- Assessing the incident that has led to the disaster/discontinuity and declare an emergency.
- Working closely with the team members to determine recovery activities and provide information regarding progress and recovery status.
- Working closely with the team to manage the overall recovery activities in an efficient and effective manner.
- Reviewing the BCP for accuracy and completeness at least annually or whether significant changes occur.

- Coordinating the re-location to an alternative location(s) if required.
- Depending on the type of incident, the BCPC will also be responsible for coordinating salvaging activities for equipment and important confidential documents.
- Notifying the disaster or disruption situation to all department heads and third parties.

Crisis Management Team ("CMT")

CMT works closely with BCPC and is responsible for managing and controlling the plan execution phases, which include initial response, problems assessment and escalation, plan implementation logistics and recovery and resumption. More specifically, the team is responsible for:

- Evaluating options based on the damage assessment of the disaster site, and the decision as to whether or not to activate the Business Continuity Policy and associated activities on an alternative location(s).
- Notifying the disaster situation to all relevant parties by initiating the BCP activities addressing notification to heads of functions and third parties (Annex A).
- Providing on-going support, management, and co-ordination of the overall recovery effort in co-operation and based on continuous communication with the BCPC.

The CMT comprises by the following members:

Contact Person	Position	Department	Email	Phone Number
Charalampos Giampanas	General Manager	Senior Management	harris@gravitypw.com	+447800561687
Andrea Savvidou	AML and Compliance Officer	Regulatory Compliance & AML	andrea@gravitypw.com	+35799013093
Benjamin Albert	Chief Technical Officer	IT (outsourced)	benjamin@adwconnect.com	+442080891111

Other Key Individuals and Third Parties

Below is a list of other key individuals and third parties who can assist in the operational recovery of the office in case of a disruption.

Contact Person	Description of Services	Email	Phone Number
Ermina Topintzi	Chief Operating Officer	ermina@gravitypw.com	+306932554690

Police / Fire Service / Ambulance			199 / 112

Damage Assessment

For Damage Assessment, the BCP teams' main purpose is to assess the extent of any damage, salvage undamaged resources and begin the process of recovering the Company's resources. The team is mobilized after the occurrence of a disruption and is responsible for assessing the extent of the damage at the site of the disaster, making an initial estimation of the time to recover lost resources. This information is utilized as input to the team that will perform the evaluation of the situation as detailed above. In undertaking some of these actions, it may be necessary to use specialist contractors, for example, a security firm, building surveyor, architect or a specialised building and equipment salvage Company.

The damage assessment performed by the team describes the damage arising from the incident and provides sufficient detail to make a decision on the next course of action. Details of damage are recorded along with time, and date within the Damage Assessment Report (Annex B) that provides a description of the extent and type of the damage observed. The team also helps determine requirements for building access. During the initial assessment, it considers the following, at a minimum:

- Assesses extent of damage to building, facilities, and assets.
- Assesses areas viable for occupancy.
- Locates a suitable meeting location (Assembly Point).
- Prepares an initial Damage Assessment Report, providing details of the impact and risks arising as a result of the incident.
- Estimates the time delay before full / partial service can be restored at the affected site.

Logistics and transportation

The BCP team with the help of the assisting member is responsible for ensuring expedient and timely acquisition of resources and equipment needed for recovery. It is also responsible for mobilizing people, resources and supplies to the alternative recovery site(s) or any other site decided for the execution of employee's functions. The responsibilities of the team are the following:

- Transportation of people, equipment and documents situated in the site(s) of the disaster, to the recovery site or any other site designated during Damage assessment phase.
- Contacting all vendors whose services and/or supplies are needed at the recovery site (Annex C).
- Ensuring that there are adequate office supplies, food and water at the recovery site.

- Travel arrangements and hotel reservations, if necessary.
- Physical recovery site preparation.

Following relocation at the recovery site, the team is responsible for arranging transportation for people, equipment and documentation between the recovery site, main site and any other designated site.

Information Technology

The success of the BCP depends heavily on the successful recovery of key business functions and supporting information systems. Information Technology (IT) services are of supreme importance for the Company and as a result the BCP strategy is supported by a set of IT Disaster Recovery Procedures to assure these services can be re-established quickly and adequately in the event of a disaster. The IT Disaster Recovery approach is described below and is structured to include the necessary technical steps and relevant IT operations that must be executed in the event of an incident at the Primary site.

The technical steps are specific to each information system and are executed based on the recovery priority defined for business processes and information systems. A list of key software systems, platforms and important external access portals utilized are included in Annex D.

With respect to information technology, the CMT team is responsible for the following:

- Ensuring that the standby equipment meets the recovery schedules.
- Installing the computer hardware and setting up the Operating system.
- Obtaining all appropriate historical / current data from the vault location and restoring an up-to-date application system environment.
- Providing the appropriate management and staffing of the standby computer processing center, data control, helpdesk and media control / tape library in order to meet the defined level of user requirements.
- Supporting operable versions of all critical functions (Annex E) needed to satisfy the minimum operating requirements.
- Performing backup activities at the recovery location(s).
- Providing on-going technical support at the recovery location(s).
- Working to restore local and wide area data communications services to meet the minimum processing requirements.
- Providing sufficient personnel to support operations at the standby facility.
- Re-establishing the Help-Desk, and Media control/tape library functions at the recovery location.
- Managing the standby facilities to meet users' requirements.
- Arranging for acquisition and availability of necessary computer supplies.

- Ensuring that all documentation for standards, operations, vital records maintenance, application programs, etc. are stored in a secure fire-proof place.

6. Recovery Methods

Clients' access to Funds and Securities

The Company does not maintain physical possession of clients' funds and securities. Both clients' funds and securities are maintained by qualified custodians. In the event of an internal or external SBD, if telephone service is available, the Company will continue to take client orders or instructions and, to the extent practicable, assist such clients in contacting custodians. In the event that clients are unable to access the Company, either at its primary phone number or the Company's emergency number, clients will be able to contact the custodian directly for instructions on how they may obtain prompt access to funds and securities, subject, however, to any limitations set forth previously by the custodian.

Data Back-Up and Recovery

The Company maintains its primary hard copy books and records at its premises in Cyprus; its electronic records are saved and backed up on Microsoft's servers as the Company uses cloud services for electronic storage.

We specifically note the following concerning how Microsoft keeps data safe:

- Data is always mirrored in at least two data centers that are located in the same region. This way Company's data is protected against natural disasters or other forms of a service-impacting outage.
- The data in OneDrive and SharePoint are retained with a two-stages recycle bin and can be restored by the Company within 93 days. Besides the recycle bin, different versions of a file can also be restored in SharePoint.
- Mailboxes are retained for 30 days by default and individual mailbox items can be restored within 14-days (by default).
- Microsoft also keeps a 14-day backup of the Company's Office 365 data and a backup is created every 12-hours. In case of a ransomware attack, for example, Microsoft Support can restore a backup of the data.

The General Manager is responsible for the maintenance of these books and records. The Company maintains the following document types and forms that are not maintained electronically: (i) certain documents that have been unable to be scanned due to age or quality of copy; (ii) certain documents from

former clients that were not previously scanned; (iii) certain financial records and corporate records of the Company that were not previously scanned.

In the event of an internal or external SBD that causes the loss of paper and/or electronic records, the Company will either physically recover the storage media or electronically recover data from Microsoft's back-up servers as per the process set out above.

Financial and Operational Assessments

In the event of a SBD, the Company will immediately identify what means will permit the Company to communicate with its clients, employees, critical business constituents, critical banks, critical counter-parties, and regulators. Although the effects of a SBD will determine the means of alternative communication, the communication options the Company will employ will generally include (a) e-mail; (b) telephone; (c) telephone voice mail; (d) cellular and mobile phone services; (e) service providers, including compliance consultants, attorneys and accountants; (f) messenger; and (g) mail service.

In the event of a SBD, the Company will determine if the business interruption causes the Company to interrupt its operations to the point that alternative measures cannot be implemented.

Mission Critical Systems

"Mission critical systems" are those systems that ensure prompt and accurate processing of securities transactions, including order taking, entry, execution, comparison, allocation, the maintenance of client accounts, access to client accounts, and the delivery of funds and securities.

The Company has a responsibility to reasonably ensure that mission critical systems are always available and functional, and inform relevant parties in case of interruptions that could prevent it from performing its basic functions. For mission critical systems that are provided by external vendors, a strict due diligence process is undertaken to ensure their reliability and operational resilience. Moreover, external vendors are assessed on a regular basis to re-underwrite their appropriateness.

Order Taking

Currently, the Company may communicate with clients and counterparties for order taking purposes, via telephone, live video conferencing, or electronic mail. During a SBD, either internal or external, the Company will continue to correspond in any of these methods that are reasonably available to it and reliable, and in addition, as communications permit, the Company will inform its clients when communications become reasonably available to inform them about available alternatives.

Clients

The Company currently communicates with its clients using the telephone, e-mail, live video conferencing, delivery services and in person visits at its offices or at the clients' premises. In the event of a SBD, the Company will assess which means of communication are still reasonably available to it, and use the means closest in speed and form, either written or verbal, to the means that have been used in the past to communicate with the other party.

Employees

The Company currently communicates with its employees using the telephone, fax, video conferencing, e-mail and in person. In the event of a SBD, the Company will assess which means of communication are still reasonably available, and use the means closest in speed and form, either written or oral, to the means that have been used in the past to communicate with the other party. The AML and Compliance Officer shall be responsible to contact and/or communicate the SBD to the employees by telephone, e-mail, messenger or in person.

Regulatory Reporting

With respect to regulatory reporting, the Company shall file reports with the respective regulatory authorities, including CySEC, by means of using paper copies and delivery services, electronically using facsimile, e-mail, and through service providers who provide access through the same methods. In the event of a SBD, the Company will check with the competent regulatory authorities to determine which means of filing are still available to it, and use the means closest in speed and form (written or oral) to previous filing methods utilized by the Company. In the event that the Company cannot contact its regulators, it will continue to file required reports using the communication means available to it.

Back-up Facilities and Arrangements

The Company has taken a series of steps to ensure that adequate redundancy is in place to provide resilience during a SBD. The Company has focused on key technology infrastructure and strategic third-party vendors to support recovery of its core functions. Some of the methods it uses include:

- Phone redirection service: A service provided by the Company's telecommunications carrier that allows a predetermined group of incoming calls to the Company and toll-free numbers to be forwarded to an alternate location.
- Multiple data centers: The Company's strategic relationship with a reliable technology services company enables it to distribute critical applications across multiple data centers.
- Diverse network infrastructure: The Company has built resilience into its data communications network using redundant circuits to key sites supported by diverse carriers.

- Recovery work site location: A series of alternate worksites exist specifically to support the Company's employees in the event of a building evacuation or structural failure. These sites are tested regularly to support core business functions.
- All systems are protected by username and passwords where all users are required to change their passwords on a regular basis.

Epidemic/Pandemic Outbreak Event

In the event of an epidemic/ pandemic outbreak in Cyprus, CMT takes decisions regarding measures that should be taken to prevent the interruptions of the business:

- All employees could work from home at any possible moment not affecting the business normal operation and could report to the management via the internet or telephone or any other available method of communication;
- Enhance network capacity to support remote access if necessary. Ensure that necessary software and network infrastructure is available to support remote access;
- Check if the corporate systems can be managed remotely without the physical presence of IT employees;
- Set up sufficient IT support for remotely working employees;
- Prepare the need to close down office or business premises;
- Create alternative communication channels for the employees, clients and/or service providers and consider whether those options would be undisrauptive in the worst case scenario (e.g. if the office is shut down or employees with important functions are unable to work for a period of time).

In case of pandemic event like Covid-19, the Company is prepared to follow the below procedures:

- Evacuation and return from infected areas (office) and workplace hygiene and sanitizations;
- Travel restrictions and mobility guidelines. Request employees that have been abroad to work from home for the quarantine purpose;
- Make arrangements for work that cannot be done remotely;
- Provision of personal protective supplies at workplace;
- Regulate norms for workplace physical interaction, this include meetings, conferences, trainings and other public events;
- Define criteria for workplace rotation;
- Provision of official information and instructions to enhance employee awareness.

Share response plans and organizational actions with employees.

Hacker's and Cyber-Attack

The Company has taken a series of steps to ensure that it is protected and can avoid cyber-attack events, indicatively including:

- Installation of antivirus software;
- Use of firewalls and intrusion detection/prevention systems;
- Data encryption;
- Implementation of two-factor authentication and strong password policies;
- Security awareness programme for employees;
- Implementation of data governance policy;
- Implementation of BYOD policies;
- Regular data back-up;
- Restricted access to sensitive and personal data

Fire prevention

The Company has taken a series of steps to ensure that it is protected against fire, indicatively including:

- Arrangements in advance for all employees to be able to work remotely should the Company's office become temporarily unavailable;
- Installation of smoke detection sensors and sprinklers;
- Employee training on premises evacuation and incident reporting;
- Employee training on the use of fire extinguishers and the activation of building alarms;
- Insurance coverage

Burglary

The Company has taken a series of steps to ensure that it is protected against burglary, indicatively including:

- Installation of alarm systems and high quality locks;
- Implementation of access control systems and motion detectors;
- Restricted access to certain areas;
- Alert notifications in case of unusual activity;
- Insurance coverage

Recovery Locations

The Company represents that both itself and all relevant service providers (including any clearing firms as the case may be) back up client records and operate a back-up operating facility in a geographically

separate area, in any of the Company's regional establishments, with the capability to conduct the same volume of business as the primary sites.

The Company provides for flexible work from home arrangements, including implementation of hybrid work models, BYOD policies, use of automation and communication tools and remote access to system network and IT support.

The Company confirms that both itself and all relevant service providers (including any clearing firms as the case may be) test their back-up arrangements at least twice a year. Recovery-time objectives provide concrete goals to plan for and test against. They are not, however, hard and fast deadlines that must be met in every emergency situation, and various external factors surrounding a disruption, such as time of day, scope of disruption, and status of critical infrastructure – particularly telecommunications – can affect actual recovery times.

7. Awareness and Training

Awareness of the need for and the process of maintaining a viable business continuity capability and of the respective role and responsibilities for each staff member are essential. This awareness is achieved through formal education and training sessions that are conducted on a periodic basis. This provides a way of ensuring that personnel who is responsible for maintaining and executing the tasks possess the necessary awareness and understanding of the Business Continuity Plan and processes.

The objectives of the training are to:

- Train the key employees and Senior Management who are required to help maintain the plan in a constant state of readiness.
- Train the key employees and Senior Management who are required to execute various plan segments in the event of an extended disaster situation.
- Heighten planning awareness for those employees not directly involved in maintaining and/or executing the plan.

The BCPC aims to schedule seminars addressing BCP, on an annual basis or when a significant change occurs, and inform all new employees of their role and responsibilities. These seminars may include overviews of the:

- Business continuity strategy
- Business continuity priorities and timeframes

- Business continuity organization and responsibilities
- Key BCP tasks and activities
- Plan administration, maintenance, and testing

8. Implementation and Review

The Company has the right to amend the current Policy at its discretion and at any time it considers suitable and appropriate. Where any amendments take place, the updated version of the present Policy shall be approved by the Company's Board of Directord, shall be published to the Company's website and shall be distributed to the Company's employees who shall acknowledge that they have read and understood the updates.

Annex A: Notification priority list

NOTIFICATION PRIORITY LIST						
Contact Priority Level	**Contact Person**	**Position**	**Department**	**Email**	**Phone number**	**To be contacted by**
1	Charalampos Giampanas	General Manager	Senior Management	harris@gravitypw.com	+447800561687	PwC, any other means or employee
2	Ermina Topintzi	Chief Operating Officer	Operations	ermina@gravitypw.com	+306932554690	General Manager
3	Andrea Savvidou	AML and Compliance Officer	Regulatory Compliance & AML	andrea@gravitypw.com	+35799013093	General Manager
4	Benjamin Albert	Chief Technical Officer	IT (outsourced)	benjamin@adwconnect.com	+442080891111	General Manager

Annex B: Damage assessment report template

DAMAGE ASSESMENT REPORT TEMPLATE	
Date/Time	
Location	
Departments affected	
Name of BCP Team Member	
Description of the incident	
Listing of identified damages	
Listing of inaccesible areas (if applicable)	
Listing of information systems affected (if applicable)	
Listing of human resource losses or injuries	
Listing of external entities affected (with regards to the Company's liabilities)	
Overall assessment of the situtation	

Annex C: Third party contact list

THIRD PARTY CONTACT LIST					
Company	System/ Matter	Department	Contact Person	Email	Phone number
ADW Connect https://adwconnect.com/	IT and Cloud Services	IT	Benjamin Albert	benjamin@adwconnect.com	Dir: +44 208 089 1111
Police/ Fire Service / Ambulance					199 / 112

Annex D: Systems

Priority Number	System/Platform/Online Access
1	Addepar (Reporting/Portfolio Management Platform)
2	Microsoft 365 (Communication, collaboration, online storage tools)
3	Cisco Webex Telephony (Recorded telephony)
4	Bloomberg terminal (Market data provider)

Annex E: Critical functions

CRITICAL FUNCTIONS/TASKS					
Order of resumption	Function/Task name	Department Owner	Importance	IT system (if any)	Recovery Time Objective (hours/days)
1	Communications (internal – external)	COO	High	Microsoft 365, Cisco, Bloomberg	2 hours
2	Investment advice, Order transmission, Portfolio management	Investment Strategy	High	Addepar, Microsoft 365, Cisco, Bloomberg	2 hours
3	Client data storage	COO	High	Microsoft 365	4 hours
4	Finance – Accounting	COO	Medium	Microsoft 365	2 days
5	Human Resources	COO	Medium	Microsoft 365	5 days