REGISTER OF AMENDMENTS

Amendment No.	Date of Amendment	Section Amended	Amendment Description
1	20/01/2023	Key Contact Personnel Alternate Physical Site Recovery Procedures for Computer Equipment Back Up IT priorities	Names and Mobile Numbers Location and transference of activity. Failure of individual office workstation and failure of a central system. What Back Up should include. Listing the IT priorities

Disaster Recovery and Business Continuity Plan

Overview

The primary objective of a Business Continuity Plan is to enable the Company to survive a disaster and to re-establish normal business operations. This document is a required reading for all staff.

The Company shall establish, implement and maintain an adequate business continuity policy aimed at ensuring, in the case of an interruption to its systems and procedures, the preservation of essential data and functions, and 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 its investment services and activities.

The business continuity policy shall be reviewed and approved by the Board. The policy shall be regularly reviewed and updated.

SUMMARY OF EMERGENCY PROCEDURES

MEDICAL EMERGENCY: Call 112/199. Describe the problem, give the exact location and your name.

FIRE: Call112/199/1460. If you have any doubts about your ability to extinguish the fire, secure and leave the area. Activate the nearest fire alarm. When a fire alarm is sounded, turn off all terminals. Save documents before turning off word processing terminals. DO NOT USE ELEVATORS.

FLOODING OR WATER DAMAGE: Call199. If it is safe to do so, move as many IT assets and files as possible out of the flooded area.

VANDALISM: Do not confront the vandal. Walk discreetly to the nearest phone and call 199. Arrange a meeting place so you can direct security personnel to the area affected.

POWER FAILURE: Turn off all terminals. Secure the area before leaving. Upon return wait for further instructions before turning terminals on again.

BOMB THREAT: Keep the caller on the telephone as long as possible and WRITE DOWN as much of the following as you can obtain: time set for the explosion, location of the bomb, and the type of bomb. Call112/199 to report the bomb threat immediately.

FIRE SAFETY TIPS:

- **ALWAYS REPORT A FIRE BEFORE ATTEMPTING TO EXTINGUISH IT**
- **ALWAYS KEEP YOUR BACK TO YOUR ESCAPE ROUTE**
- **NEVER ATTEMPT TO EXTINGUISH A LARGE FIRE**

PERSONS TO SUMMON WHEN A DISASTER OCCURS

All communication internally and externally, in case of disaster shall be alternate to the regular channels i.e.: Alternate site communication lines, Mobile phones, Home land lines as may be relevant and web based solutions using mobile devices (such as Laptops) in alternate locations.

It is the responsibility of the first person observing the disaster to contact one of the Disaster Committee members. The Disaster Committee, each of whom will be responsible for alerting the staff in the areas they represent, using telephone numbers listed below.

The following numbers will be available for contact in case of Emergency where the "Disaster recovery plan" is carried out:

KEY CONTACT PERSONNEL
Mrs. Soteroula Demetriou - Mobile number: + 357 99 528911
Mrs. Flora Parker – Mobile number: +357 96 717541

RECOVERY SCENARIOS

This section describes the   various recovery scenarios that   can be implemented, depending on the nature of the disaster and the extent of the damage. The Disaster Committee decides which recovery scenario to implement when it activates the Disaster Recovery Plan.

It is likely that the majority of 'disasters' that will impact the company will be relatively minor emergencies that can be resolved quickly and effectively with minimal impact upon the business.

There is however always the possibility that the company will be faced with dealing with a catastrophic event resulting in a major disaster, and it is important to plan for such an event even though it is likely to be rare.

Minor Emergencies

In these scenarios, the Disaster Committee is dealing with non-catastrophic events that are limited to reasonably short timeframes. The goal of the recovery process in these cases is to limit the impact of the emergency and to move the applications from the systems which are unavailable to the Standby Facility.

In these scenarios the building is still available, and the users can use normal office space to await the resumption of normal activities.

Major Disasters

In these scenarios, the Disaster Committee is dealing with catastrophic events whose impact will involve reasonably long timeframes. The goal of the recovery process in these scenarios is to move all affected Head office functions to the Standby Facility as little adverse impact to external and customers as possible.

These scenarios require a full recovery procedure, as documented in the Disaster Recovery Plan.

EMERGENCY EVACUATION PROCEDURES

<u>Following the approval by the CEO or General Manager</u>

The persons authorized to initiate an evacuation are:

Disaster Committee

Member Name
Mr. Robert Parker

Mr. Simon Parker

SUMMARY OF EVACUATION PROCEDURES

1. The fire alarm system or a verbal alarm stated by one or all of the above persons will alert occupants that an evacuation has been called.

2. The Emergency Evacuation Director, will control the evacuation.

3. Departmental Managers are responsible for clearing each floor of all occupants and directing them to exit safely using the stairways.

4. No one is allowed back in the building unless directed by the Emergency Evacuation Director.

Alternate Physical Site.

In case the Limassol site is not functional for any reason, the senior manager in charge may announce a temporary cessation of the location and transference of activity to one of the following locations:

- **Holborn Group entity Paphos**

Communication between existing personnel will be conducted via email, cell phone, land phone and courier services for urgent matters. All personnel have Internet connections at home which can allow temporary operation from these locations as staff all have Laptops and can work in a mobile environment via VPN secure networks.

STAFF MOBILIZATION- Phase 1

A major disaster in the offices would necessitate the evacuation of all personnel. In such a situation, actual recovery procedures to salvage the collections would have to wait until the building was officially declared safe to enter.

In the case that the disaster does not necessitate the immediate evacuation of personnel, all employees will have to follow the following steps before evacuating the building, if safe to do so:

- Save documents before turning off terminals
- Tidy your desks and put away all hardcopies
- Put aside any items that may be in the way
- You may take valuables with you that are easy to carry
- Walk (not run) to the exit
- DO NOT USE THE ELEVATOR
- Use the stairs and be very cautious of other people on the stairway

DAMAGE ASSESSMENT- Phase 2

Meeting location for reports and first phase planning:

The meeting point of all staff following evacuation will be outside the Building

Police and Fire Department officials will gather for a status report on the situation that should cover the extent of the damage and when the building can be entered for recovery purposes. The Disaster Committee will devise site visit procedures according to the extent of the damage and accessibility of the building.

Basic site visit procedures:

The Disaster Committee and Building Owner enter building to assess damage when entry to the building has been approved by fire officials. High priority areas will be assessed first, followed by other affected areas

IT systems

The IT Department shall establish procedures to ensure that in situations of an interruption to the Company's systems (trading, telephones, etc.) and procedures, the following are met:

i. Preservation of essential data and functions.

ii. The maintenance of providing its investment services and activities.

iii. The timely recovery of such data and functions and the timely resumption of its investment services and activities.

The Company shall identify specific systems which shall be considered as core systems required to ensure business continuity. These systems shall ensure:

a. The continued and uninterrupted access to the internet.

b. The continued and uninterrupted operation of the trading platform.

RECOVERY PROCEDURES FOR COMPUTER EQUIPMENT

Contact IT personnel to report the failure of individual office workstations or an ongoing emergency in an office area which could jeopardize computer equipment.

In the event of a central system failure or any emergency (electrical, plumbing, etc) which could cause the failure of a central system, contact the IT Director as it is their responsibility to contact the appropriate staff.

If the building is being evacuated, the following actions should be taken but only if safe to do so:

PROCEDURES:

1. "Save" work being done on systems and close files.

2. Turn off workstation and peripherals.

IN CASE OF A DISASTER THAT DESTROYS OR SEVERELY CRIPPLES THE COMPUTING RESOURCES

The disaster recovery plan has the following primary objectives:

1. Present an orderly course of action for restoring critical computing capability to the Company within a few hours of initiation of the plan.
2. Set criteria for making the decision to recover at a cold site or repair the affected site.
3. Describe an organizational structure for carrying out the plan.
4. Provide information concerning personnel that will be required to carry out the plan and the computing expertise required.
5. Identify the equipment, floor plan, procedures, and other items necessary for the recovery.

Back up

A full back-up of all information is to be recorded daily. Back up shall include:

- Web Site is fully backed every night up on its hosting site. This hosting site has its own backup systems.
- Sensitive original paper documents such as substantial contracts and an updated version of this Manual etc. shall be stored in a “fire proof safe”
- Mailboxes, SharePoint and OneDrive are backed up constantly throughout the day

The Disaster Committee and Building Owner will record the extent of damage in indicating the following:

- Type of damage (water, fire)
- Extent of damage
- Condition of surrounding area

RECOVERY PREPARATION- Phase 3

Second meeting of Disaster Committee:

After Phase 2 damage assessment, the Disaster Committee will return to the designated Control Center, or the home of one of the committee members and begin to plan a salvage operation for damaged materials. Based on information recorded during the site visit of affected areas, the committee will:

- Establish priorities.
- Develop and assign teams for affected areas, using the names and telephone numbers recorded above as well as the volunteer names and telephone numbers.
- Assemble supplies
- Develop a schedule for implementation.
- Define reporting mechanism and communication lines, including an established chain of command for recovery operations. This should include a method to deal with unforeseen modifications that need to be made during the recovery operation.
- Update the backup site of the situation and schedule the transfer of responsibility back to the Limassol site.

The chair of the Disaster Committee will appoint an assistant to take minutes during all meetings, telephone for supplies and other necessities, organize deliveries of supplies, answer telephones, and assist in the management of the recovery process from the Control Center, as needed.

In the event of a major disaster, the Disaster Committee will direct a recovery operation using the procedures contained here. Minor emergencies and small scale disasters, should be reported to the director.

Alternate 3rd party solutions: essential 3rd party providers are fully backed up as follows:

- Telephones and Mobiles are backed up by Internet communication lines.
- Electric power is backed up by UPS devices to enable operation of all electric consuming appliances.
- Internet: fully backed up by holding two totally independent lines by two independent providers
- MT$ Software Servers are in office of Hong Kong Software Provider with Back Up Server in Data Centre and Cyprus (to be implemented)

- Liquidity Providers can be reached by Telephone and the Company will have more than 1

IT priorities are as follows:

- Access to users personal and shared mailboxes
- Access to company SharePoint files and folders
- Access to personal OneDrive files and folders
- Access to Dynamics365 (Advisor Connect provide by Morning Star)
- Activation and access physical and virtual servers and NAS storage
- Access to telephony system

Please refer to the IT Security Policy for further clarification of the various IT systems

BOMB THREATS

If a suspicious object or package is found, call 112/199 immediately.

If an evacuation is necessary, follow the emergency evacuation procedures above.

If a staff member receives a call reporting a bomb threat, he or she should remain calm and WRITE DOWN the answers to the following questions:

- When will the bomb explode?
- Where is the bomb?
- When was it planted?
- What does the bomb look like?
- What type of bomb is it?

The staff member receiving the threat should carefully WRITE DOWN the following information:

- The exact words of the caller.
- The quality of the caller's voice: does the caller sound young or old, male or female? Does the caller have an accent? Does the caller sound nervous, determined, etc?

While on the phone, the staff member should signal a nearby employee to call 112/199. It is his duty to notify all other appropriate individuals, including the Police and/or Fire Departments.

When the appropriate personnel are notified, they will make a decision to evacuate based on the following criteria :

- The accessibility of the area to intruders.
- The terminology used in the bomb threat.
- The time of day.
- Current events.
- The logistics of an evacuation.
- The means by which the threat was communicated: by mail, hand delivery or phone call.
- The advice of the Police or Fire Department.

VANDALISM

Vandalism includes but is not limited to the following: damaging or defacing the office building, furniture or equipment; damaging or defacing files, such as tearing out pages, tearing out sections of pages, stealing files, writing in files; and smoking in the office, including bathrooms.

To report cases of vandalism, contact 199.

EARTHQUAKE

Earthquakes are caused by a shifting of the earth's rock plates beneath its surface resulting in violent shaking and movement of the earth's upper surface. Severe earthquakes can destroy power and communication lines and disrupt gas, water and sewerage services. Significant damage to structures can occur including total collapse of buildings, bridges or other elevated structures. Earthquakes can also bring landslides, damage to dams, and aftershocks and resulting damage can hinder rescue efforts. In addition to being trapped in a collapsing building, of particular danger to human life is the possibility of falling glass or other objects.

When structural damage occurs, call the Police or Fire Departments if necessary. After inspection, they will determine when it is safe to enter the area. DO NOT ATIEMPT TO ENTER THE AREA UNTIL IT HAS BEEN INSPECTED.

STRUCTURAL COLLAPSE

Structural accidents, such as the collapse of a ceiling or a wall, can be the results of explosions, earthquake, flood or natural deterioration.

When structural damage occurs, call the Police or Fire Departments if necessary. After inspection, they will determine when it is safe to enter the area. DO NOT ATIEMPT TO ENTER THE AREA UNTIL IT HAS BEEN INSPECTED.

SUMMONING MEDICAL ASSISTANCE

The decision to notify or render medical services should be made only by authorized personnel.

If someone is injured or sick and in need of emergency help, call 199/112

Accessibility to the plan: Each employee shall have a copy of the plan and a full set of reserve copies shall be kept in the bank safe and distributed to the employees in a case of distress.

Review and update: This Plan shall be reviewed at the sooner of a change of the location of the company or annually. The annual review shall be done via a presentation of the "Disaster recovery plan” in a management meeting. Discussion addressing the suitability of the plan will take place and any required changes will be implemented. Minutes of such meeting will be taken and maintained in the firm's files for a period of five years. If the plan is revised, copies of the revised plan will be distributed to all employees.

Training: Each employee will be required to read, understand and acknowledge in writing having done so with regard to the Supplement to the Supervisory and Compliance Manual. In addition, an annual drill will be scheduled to check the plan. Such drill should be documented and results filed in a Compliance file/Binder.