Holborn Assets

DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN

HOLBORN

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 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
Ms. Jackie Evans
Mr. Robert Parker

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

Following the approval by the CEO or General Manager

The persons authorized to initiate an evacuation are:

Disaster Committee

Member Name
Mr. Robert Parker
Mr. Simon Parker

HOLBORN

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:

- .....

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. At least 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

Call IT personnel to report failure of individual office workstations or an emergency in an office area which jeopardizes 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 Director as his responsibility to contact the appropriate staff.

If the building is being evacuated, the following actions should be taken 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 on a daily basis. Back up shall include:

- Web Site (the site and the related Back Office system) is fully backed up in a top of the line hosting site. This site has its own sophisticated 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”
- Electronic files such as: Office documents (excel, word, PowerPoint, etc.), mail boxes, all home directories of all users are daily backed up by recording all the data on a backup tape for each calendar month.

The Disaster Committee and Building Owner record 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

PRIORITIES

- **All Files**
- **Server**
- **Backup Tapes / CD's etc.**

IT Security Policy

Scope

The scope of the IT security policy is to:

- Define terms that relate to the IT Security policy
- Communicate the objectives of IT security
- Specify the scope of IT resources to which the IT Security policy applies
- Indicate the responsibilities of the IT team for maintaining IT security and reporting security breaches

Approval of the IT Security policy is vested with the Directors of the Company.

Enforcement

Any breach of the restrictions contained in these policies may result in the invocation of the Company's Disciplinary Procedure, up to and including summary dismissal, and could give rise to criminal and/or civil liability.

User Privileges

This is an internal IT policy which defines and controls the access policy within the organisational network, specifically defining Privileged Access and Standard User privileges and control of sensitive or regulated data. Below are the main categories of users on the Company's domain network:

- **Standard User** – Applies to the majority of employees of the Company. This access allows users to connect to the internet, access network drives pertaining to their departments, access to a personal network drive on the network and connect to the Company's email platform.

- **Privileged User** – These users have access to the entire network, and are monitored through administrative login credentials. Employees with this level of access are generally part of the IT support team and require such access in order to support the entirety of the Company's domain network.

Internal Back-up Systems

The Backup policy is designed to protect data for a period of 5 years to comply with CySEC regulations and to ensure data can be recovered in the event of equipment failure, intentional destruction of data or disaster.

Definitions:

Backup – Critical data is backed up onto magnetic tape and stored off site on a weekly basis.

Archive – Monthly tapes are stored off site in a fire proof safe within a facility based in Cyprus.

Restore – Restoring data is tested on a monthly basis to ensure the data can be restored from tape and to check the integrity of the data once restored.

Backups are run each night starting at 10pm and run for a 4 weekly period until the month end backup tape in used. The data on the weekly tapes are then overwritten as the cycle starts again.

On the last day of each month a monthly backup is taken and this tape is then labelled and will not be overwritten. This tape is then stored offsite.

Validation of backed up data

Data from backup tapes will be restored monthly to ensure the backups are reliable.

This will involve a random sample of files to be restored from the tapes and opened to prove validity.

Client Document Archiving

All client verification documents are archived using an online scanning facility. Documents are emailed or faxed to the Customer Support team, who then scan the documents to the system. Hard copies are then destroyed. These files would include personal identification items, e.g., Bills, Passports, Driving Licenses, etc. Only customer support and compliance members of staff have access to this drive.

Email Archiving

Exchange email is archived ensuring that every Email sent and received through the Company's email platform is archived before any user intervention. This provides a searchable archive to the Company's compliance department and ensures all emails are kept regardless of deletion.

Support Access Permissions

The IT Team have full access to the entirety of the Company's network in order to be able to administer and manage the network and infrastructure.

- All changes impacting the system and/or users are performed under authorised change control.

Employee Network Access

New users will only be created upon confirmation of role and details in the HR system.

This will include access to:

- Email
- VPN access
- File Share Access

When an employee leaves the Company, HR will inform IT. The HR system and the AD system reconcile every 6 hours and email a report.

Guest Access

Wifi

Any requirement for third party access to the internet is provided through Wifi Guest access.

Switches

All network switches are secured by strong usernames and passwords to secure against unauthorised changes. All default passwords are disabled during configuration.

Routers

The router settings are managed by the infrastructure team using a secure password to gain entry and make changes. The password is stored and is only accessible to the IT team. All default passwords are changed during install.

Firewalls

Rules set up on the firewall are in place to control inbound and outbound data transfer between the Company and any external sites or third parties. These rules are managed by the support team and are updated upon request of access to ensure no unauthorised access is allowed.

Should there be a requirement for a firewall change involving access for a third party, these rules will need to be authorised by the IT team.

Anti-Virus on Mail server and Desktop

The Company operates an anti-virus solution on its network, which is updated daily with latest definition files. The anti-virus suite is reviewed daily for any suspected virus alerts.

Emails are scanned for viruses as they arrive into the mail box and are also scanned when attachments are opened by a user on the desktop.

Internet / Website Security

Annual penetration / security testing is performed to ensure the Company's networks and websites are secure. Any recommendations are reviewed and appropriate action is taken.

Internet security is managed through a firewall allowing the incoming and outgoing of traffic into the Company's network.

There are a number of security checks performed on internet traffic in and out of the Company's network, covering:

- Domain Name System filtering – Open DNS offers the blocking of known phishing sites and prevents communications with known viruses;
- Intrusion Prevention – Identifies malicious activity, log information about said activity, attempt to block/stop activity, and report activity;
- Gateway Antivirus - Monitors download via web and FTP to prevent being exposed to malicious applications;
- Content Filtering – Allows the support team to filter up to 65 content filtering categories.
- Application Firewall - Places restriction on certain application and websites such as Social Networking Sites and Instant Messenger Programs.

Website Security (Client)

SSL (Secure Socket Layer) certificates are used to ensure data transactions between client web browsers and the Company's servers are secure.

All websites are managed with SSL certificates to ensure communication is encrypted. The SSL's are purchased yearly and managed through several providers.

A spreadsheet is kept up-to-date by the Support IT team detailing dates when the SSL was purchased and the expiry date. As a security measure, the third party will email the support team two weeks prior to the SSL expiration.

Guest Wireless

The following security measures are implemented on the Guest wireless network:

- Strong password encryption on the wireless network;
- Guest Wifi password is changed every six months and kept on KeePass.
- Wifi access is segregated from the Internal network and allows access to the internet only.

Monitoring / Auditing

All systems are monitored for both security and performance issues to both protect the organisation against loss of service and monitors servers for file space and performance or malicious use. The servers covered are the following:

- File servers
- Database servers
- Mail servers
- Application servers
- Domain controllers

- DNS servers

Further monitoring is carried out by the IT team on a daily, weekly, monthly and yearly basis.

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.

Appendix 3 – Marketing Policy

1. PURPOSE

The scope of this policy is to set out the procedures and guidelines established and implemented the Company regarding the information addressed to clients or potential clients, including marketing communication. This policy is designed to ensure that the marketing communication of the Company, is clear, fair and not misleading as required by the provisions of the Law 188(I)/2007 (hereafter the "AML Law") and the relevant directives and circulars issued by the Cyprus Securities and Exchange Commission ("CySEC" or "Commission") in regards to the information addressed to clients.

2. GENERAL REQUIREMENTS

In general, as per the legislative requirements, all information addressed by the Company to its clients or potential clients, including marketing communication, shall be *fair, clear and not misleading*. The aim of this policy is to ensure that all the persons employed by the Company as well as any service providers that are responsible for the preparation of marketing material and any service providers that communicate with clients and provides information on the investment and ancillary services as well as the financial instruments provided by the Company, are aware of their duties with respect to the following legislative requirements:

(a) Law 144(I)/2007, regarding the provision of investment services, the exercise of investment activities, the operation of regulated markets and other related matters.

(b) Directive DI144-2007-01, regarding authorization and operating conditions of Cypriot Investment Firms.

(c) Directive DI144-2007-02, regarding the professional competence of IFs and the natural persons employed.

(d) Circular CI144-2012-16, regarding information addressed to clients with marketing communication included.

(e) Circular CI144-2012-10, regarding information addressed to clients with marketing communication included.

(f) Circular CI144-2013-07, regarding Marketing Communication.

(g) Circular C065, in relation to the granting of trading benefits to clients.

(h) Circular C053, regarding the use of market data reported by a trading venue.

(i) Circular C168, regarding the Updated version of ESMA's Q&A document relating to the provision of CFDs and other speculative products to retail investors under MiFID

(j) Circular C181, regarding the obligations of IFs when providing information to clients on the services and instruments offered.

(k) Any other directives or circulars issued by CySEC in regards to the respective subject matter.

The main focus of this policy is to ensure that marketing initiatives are aimed at the right audience and are conceived in such a manner as to be clear and easily understood by the average member of the group to whom it is directed. In addition, this policy aims to ensure the correct formulation of marketing communications and drastically reduce the possibility of the latter being misinterpreted or misleading, as per the relevant legislative requirements.

3. MARKETING COMMUNICATION

3.1 Definition of marketing communication

Any form of information to clients is considered as marketing communication, depending on whether it includes an invitation or incentive for clients and/or potential clients to engage in any investment and/or ancillary services offered by the Company.

3.2 Marketing Channels

The Company has an integrated marketing strategy to promote the Company's brand through the following marketing channels, which relate to both potential and existing clients:

Search Strategy:

(a) Pay-per-Click ("PPC") – Search

(b) PPC – Display

(c) Remarketing

(d) Search Engine Optimization ("SEO")

Marketing Channels:

(a) Online Media Buys

(b) Directory Listings

(c) Social Media Campaigns

(d) Videos

(e) Content Marketing

(f) Public Relations

(g) Offline Events (expos/events)

(h) Print Advertisements

(i) Sponsorship

(j) Affiliate Marketing

The marketing materials are sent to the above channels and vendors by the Company's marketing team.

3.3 Principles to be followed for marketing material and information addressed to clients

This section of the policy analyzes the general principles to be followed by the Company and the employees responsible for the preparation of any marketing material addressed to clients, so as to ensure compliance with the relevant legislative requirements. The below principles are applicable to both the Company and its affiliates. General examples of adequate and insufficient practices as regards to marketing communication addressed to clients are available at **Appendix 1**.

Furthermore, advertising material shall not in any manner promote sexually explicit materials, violence, discrimination based on race, sex, religion, nationality, disability, sexual orientation or age and/or any illegal activities or violate any intellectual property or other proprietary rights of any third party. Promotional Marketing material shall be limited to services/products for which a license has been obtained by the Company from CySEC.

3.4 Fair, Clear and not Misleading

As regards to information addressed to clients and/or potential clients, it is the Company's obligation that all information is fair, clear and not misleading. In particular, the Company shall ensure that all information addressed to, or disseminated in such a way that it is likely to be received by clients, classified as "Retail", or potential "Retail" clients, including marketing communications, satisfy the conditions laid down in paragraphs 6(2) -6 (8) of the Directive DI144-2007-02.

The Company is not allowed to make false, misleading statements such as:

- promised returns / guarantee profits;
- statements that mislead clients to consider that trading in Forex / CFDs carries little or no risk;
- references that do not reflect the real opinion of clients;
- advertising the provision of investment services that the Company has not been granted with an authorization from CySEC.

Promotions that fail to be fair, clear and not misleading can pose a risk as they could lead clients who are classified as "Retail", to trade with a financial instrument that is not appropriate for the client. The "fair, clear and not misleading" principle implies the balance in how financial instruments and/or services are promoted, so that for clients and/or potential clients to have an appreciation not only on the potential benefits but also of any relevant risks associated with trading.

3.5 Risk Warnings

In accordance with the legal framework the Company should place a risk warning appropriate to the products it provides within the borders of each banners/ picture or sign/ invitation to open an account. Specifically, all banners included in the website for advertising purposes, as well as invitations to open an account shall bear a risk warning which must be contained within its own distinct border so as to draw the reader's attention. In particular, the Company must ensure compliance with the following requirements in respect of the risk warnings:

- Risk warnings are clearly stated within the main body of the marketing communication and ahead of a small print (i.e. legal text or contract information);
- Risk information appears on the website home page of the Company that clients and/or potential clients first arrive at, when following a promotional link.
- Risk warnings are properly included in all of the information addressed to clients, including electronic emails, affiliates landing pages etc.

3.6 General conditions for information addressed to clients

The Company must ensure that all information it addresses to, or disseminates in such a way that it is likely to be received by, retail Clients or potential retail clients, including marketing communication, satisfies the conditions laid down as follows:

(i) The information should:

(a) include the name of the Company and that it is supervised by CySEC;

(b) include the number and the content of the Company's authorization;

(c) be accurate and in particular shall not emphasize any potential benefits of an investment service or financial instrument without also giving a fair and prominent indication of any relevant risks;

(d) be sufficient for, and presented in a way that is likely to be understood by, the average member of the group to whom it is directed, or by whom it is likely to be received;

(e) not disguise, diminish or obscure important items, statements or warnings.

(ii) The information shall not use the name of any competent authority in such a way that would indicate or suggest endorsement or approval by that authority of the products or services of the Company.

Practical Guidelines – Emphasize potential benefits/Misleading Information
▪ The Marketing Officer shall be accurate and in particular shall not emphasize any potential benefits of an investment service or financial instrument without also giving a fair and prominent indication of any relevant risks. ▪ It is required to explain the impact of any leveraged products by using wording such as *'loses may be more than the invested capital'*. ▪ When talking about possible returns, possible losses should also be mentioned; use wording such as '*the investment value can both increase and decrease and the investors may loss all their invested capital*'. ▪ Don't include only the benefits of a financial instrument; drawbacks should be also mentioned.

In addition to the above the following conditions shall need to be satisfied:

A. Comparison:

Where the information compares investment or ancillary services, financial instruments, or persons providing investment or ancillary services, the following conditions shall need to be satisfied:

(i) the comparison must be meaningful and presented in a fair and balanced way;

(ii) the sources of the information used for the comparison must be specified;

(iii) the key facts and assumptions used to make the comparison must be included.

B. Past Performance:

Where the information contains an indication of past performance of a financial instrument, a financial index or an investment service, the following conditions shall be satisfied:

(i) that indication must not be the most prominent feature of the communication;

(ii) the information must include appropriate performance information which covers the immediately preceding 5 years, or the whole period for which the financial instrument has been offered, the financial index has been established, or the investment service has been provided if less than five years, or such longer period as the firm may decide, and in every case that performance information must be based on complete 12-month periods;

(iii) the reference period and the source of information must be clearly stated;

(iv) the information must contain a prominent warning that the figures refer to the past and that past performance is not a reliable indicator of future results;

(v) where the indication relies on figures denominated in a currency other than that of the Member State in which the retail Client or potential retail Client is resident, the currency must be clearly stated, together with a warning that the return may increase or decrease as a result of currency fluctuations;

(vi) Where the indication is based on gross performance, the effect of commissions, fees or other charges must be disclosed.

C. Simulated Past Performance:

Where the information includes or refers to simulated past performance, it must relate to a financial instrument or a financial index, and the following conditions shall be satisfied:

(i) the simulated past performance must be based on the actual past performance of one or more financial instruments or financial indices which are the same as, or underlie, the financial instrument concerned;

(ii) in respect of the actual past performance referred to in point (a) above, the conditions set out in sub-points (a) to (c), (e) and (f) of point (iii) above must be complied with;

(iii) the information must contain a prominent warning that the figures refer to simulated past performance and that past performance is not a reliable indicator of future performance.

D. Future Performance:

Where the information contains information on future performance, the following conditions shall be satisfied:

(i) the information must not be based on or refer to simulated past performance;

(ii) the information must be based on reasonable assumptions supported by objective data;

(iii) where the information is based on gross performance, the effect of commissions, fees or other;

(iv) charges must be disclosed;

(v) the information must contain a prominent warning that such forecasts are not a reliable indicator of future performance.

E. Tax treatment:

Where the information refers to a particular tax treatment, it shall prominently state that the tax treatment depends on the individual circumstances of each Client and may be subject to change in the future.

1. INFORMATION ADDRESSED TO CLIENTS

The Company is required to provide clients with specified legal information. A retail client or potential retail client must receive the following documents:

1. The Terms and Conditions which includes the following information:
    a. Means of communication.
    b. Company name and address.
    c. The languages in which the client may communicate with the Company and receive documents and other information.
    d. Company's contact details.
    e. Communication method for receiving orders.
    f. Statement that the Company is authorized and the name and contact address of CySEC.
    g. Summary description of the steps taken to ensure protection of funds the Company holds on behalf of its clients, including details about the Investor Compensation Funds.
    h. Information on costs and associated charges.
    i. A general description of the nature and risks of financial instruments taking into consideration the client's categorization either as retail of professional client. That description must explain the nature of the specific type of instrument concerned, as well as the risks particular to that specific type of instrument in sufficient detail to enable the client to take investment decisions on an informed basis.
2. Conflicts of Interest Policy.
3. Risk Disclosure Statement.
4. Privacy Policy.
5. Trading Conditions, available instruments, expiry dates, information of spreads and rollovers, as well as expiry rates as applicable for each product offered by the Company.
6. Details of the complaints handling process.
7. Order Execution Policy.
8. Client Classification Policy.
9. Dormant Accounts Policy, if applicable.
10. Investors Compensation Fund Policy.

The Marketing Officer shall ensure that at least on annual basis the following sections in the Company's website are reviewed and updated accordingly:

1. Link to the **Market Discipline and Pillar III Disclosures** is updated;
2. **List of payment service providers** is updated once a new collaboration is in place or when a termination has occurred.

The Company provides its clients with the prescribed information through the website which is accessible by all website users (clients or potential clients) at specified times. In addition, retail clients are notified on the exact information location through an email upon registration.

2. TRADING BENEFITS

The Company will not offer trading benefits such as Bonuses.

3. PLANNING, PREPARATION, REVIEW AND APPROVAL OF MARKETING CAMPAIGNS

The aim of the respective section of the policy is to provide a solid foundation and road map from planning to approval and the execution of marketing campaigns and marketing material while making sure all policies and procedures have been duly respected in the mentioned stages. The Marketing Officer of the Company would be responsible for the marketing of the Company's services to potential clients and therefore the planning and preparation of marketing campaigns.

The Marketing Function of the Company will be performed in-house by the Company's Marketing Officer and designated full-time employees.

First Step – Planning of Marketing Element and/or Campaign

The first step in the planning phase under which a request comes up to create a marketing element and/or campaign. The Company is required to clearly define the objective of the element and the audience / targeted clients to whom it is directed. Clearly defining the target audience is of prime importance as the marketing message and the delivery method (channel) will depend on this.

Second Step – Defining the Terms of Use

For all intended elements and campaigns, the marketing channel shall first be defined and applicable rules / policy of use / legal policies / terms of use of the channels must be studied and understood before actually planning the campaign for use on those channels.

Third Step – Prototyping information addressed to clients

One of the critical stages of the campaign planning process is to clearly define and prototype information that will be addressed to clients and potential clients. At this stage, the employees involved in the task shall take into consideration the objective of the campaign and accordingly define how the end message delivered to the client would look like and prototype this information. Prototypes will consist of the actual text. Messages, information, risk warnings and disclaimers to be used for the campaign.

Forth Step – Prototype Review by the Compliance Officer

Upon the completion of the prototyping stage by the Marketing Officer stage, the Marketing Officer is required to submit prototyped information to the Compliance Officer in order for the latter to review and approve its content. The prototype approval process is to evaluate the marketing materials and ensure that they abide by the internal marketing guidelines and the relevant legislative requirements. The Compliance Officer reviews the said material from compliance point of view and provides comments to the Marketing Officer until the prototype is finalized and approved.

Fifth Step –Design and Development

Subsequently to the content approval by the Compliance Officer, the Marketing team creates mock-ups/samples and builds the respective mock-ups in the marketing element.

Sixth Step – Final Approval

Upon completing the design of the material, the designer shall send the material via email to Company's Compliance Function. If the Compliance Function is not satisfied that the material meets all of the conditions mentioned above, it shall revert to the h Marketing Officer via email stating the reasons why the material is not up to the appropriate standards requesting the appropriate changes.

In case where the Compliance Function is satisfied that the material meets all of the conditions it shall inform the Marketing Officer via email. In this respect, the Marketing Officer will proceed with registering the material into a spreadsheet (in this Section "the registry") that will include the following information:

- The name and a description of the material and the promotion for which the material was created for (EMAIL/BANNER/VIDEO/LANDING PAGE)
- The name of the person who provided the initial approval of the material;
- Date of initial approval by the Marketing Officer;
- The name of the Compliance Officer who approved the material;

- Date of approval by the Compliance Officer;

Upon registering the material to the registry, the designers shall upload the material into a folder in web server. This web server shall be restricted from view and editing to all persons in the Company and to any affiliates/outsourced parties to the Company with exception of the Company's Compliance Function.

The Marketing Officer shall complete the Promotion Form, found at Appendix 2 and send it to Compliance Officer for final approval.

The marketing material is stored in the server of the Company.

The Company shall make available the folder in the server, the marketing material as well as any emails of the persons described above to its Internal Auditor and CySEC upon request.

Seventh Step – Approved / Rejected Marketing Material

Once a marketing element has undergone the final compliance approval process and it has been verified and approved that the marketing element is compliant with regards to existing legislative requirements, the Marketing Officer shall proceed with the launch of the campaign.

Duties of the Head of the Department

The Head of the Marketing Officer will have the following duties and responsibilities:

- *Responsible for the overall activities of the Marketing Officer*
- *Manage the marketing and creative team to ensure all activities are align with the Company's goals and objectives through online and offline channels*
- *Manage all external marketing agencies including Strategy, Design, Marketing and Technology.*
- *Preparation, planning and control of global marketing strategy and budgets*
- *Managing marketing plans both at global and country-specific level*
- *Develop and supervise the management of the Public Relations strategy and plan for all target markets and regions*
- *Responsible for all website changes and redesign of the client's portal*
- *Manage all social media activities and content marketing activities*

- *Manage and set up all companies' events and exhibitions globally*
- *Manage and oversee the activities of the creative team members to ensure that all content and collateral are on brand*
- *Provide strategy direction for all marketing activities for the creation of integrated marketing communication plan across all channels*
- *Monthly reporting*
- *Perform effective time schedules for the efficient operation of officers within the department*
- *Advise the Company's management for measures to increase the quality and speed of service*
- *Monitor and communicate competitive activity*
- *Work with sales and operation to identify customer needs*
- *Work together with other departments by integrating the sales force, customer service, service management and marketing research areas within the Company*

Marketing Officer Responsibilities

The overall responsibilities of the Marketing Officer are the following:

- *Ensuring smooth and efficient operation of the Marketing Officer*
- *Advertisement services by creating all necessary elements and content, i.e. banners, flyers, expo booths, videos etc.*
- *Develop promotional plan for key countries*
- *Website maintenance within the CySEC guidelines*
- *Inform Compliance Officer and get any approval for the financial promotions*
- *Preparing regional marketing budgets*
- *Preparing regional and global integrated campaigns – PPC, media buys, content marketing, T.V., social media etc.*

Specific roles of persons in the Marketing Officer

(a) Chief Marketing Officer

Please refer to point 7.1. of this policy in relation to the Duties of the Chief Marketing Officer

(b) Digital Marketing Manager

- Responsible for managing and implementing successful paid search campaigns, demonstrating revenue goals, efficiency and volume
- Identifying and planning a keyword strategy for appropriate campaigns
- Tracking, reporting and analyzing PPC performance campaign data from paid search campaigns and strategies
- Optimizing copy and landing pages for search engines in collaboration with Web Development and Content Marketing to improve PPC performance
- Understanding creatives in PPC campaigns to improve advertisement performance and quality CTRs
- Ensuring evaluation and tracking is in place to monitor campaigns
- Identifying opportunities to generate leads and improve profitability of campaigns
- Responsible for bid management, keyword search and specific country targeting and other targeting criteria
- Optimizing campaigns with text for advertisements
- Developing and strengthening the Company's brand utilizing PPC techniques
- Supporting the digital Marketing Manager and preparing relevant reports
- Provide SEO analysis and recommendations in coordination with elements and the structure of our lead website, microsites and other web pages
- Perform keyword research to optimize existing content and uncover new opportunities
- Execute strategies for content development in coordination with SEO goals – general and keyword specific

- Monitor and administer search engine analytic programs and platforms
- Monitor and evaluate search results and search performance across the major search channels
- Help to create effective marketing content for use on website, microsites, and mobile platforms and for the support of social media programs
- Test and implement various search engine marketing techniques, web site layouts, content and paid search strategy for SEO/SEM optimization
- Regular communication with team and reporting to management on project development, timelines, potential areas of improvement and results

(c) Web Developer

- Maintenance, development and optimization of both new and existing projects
- Extensive PHP / server side programming
- Development of modular / reusable code with MVC frameworks
- Extensive JavaScript / client side programming including API integration
- Interpretation of design specifications / images to fully responsive pages
- Design and development of web sites
- Web-based applications and solutions as well as related software for both in-house and client use.
- Responsible for maintenance and support of such systems to ensure their smooth operation.

(d) Senior Analyst

- Write daily reports on macro / equity / technical analysis for website and distribution amongst journalists
- Author content marketing articles

- Week-ahead report
- Build relations with media contacts
- Webinars – from introductory to more advanced.
- Seminars –present once in UK, write any other training seminars necessary for presentation across the globe.
- Write trading videos script to add to library – Getting started / Technical Analysis / Fundamental Analysis
- Recorded TV market updates
- Live TV interviews
- Website review
- Assist on Spanish website
- Any other request that comes from the management e.g. analysis reports

(e) Media Production Manager

- In house videos for new product set-up and configuration
- Social Media Videos: Creative, buzz videos not related to product launch
- Establish video budget requirements
- Develop scripts, outlines or creative briefs
- Provide reporting on viewership
- Manage video placement on YouTube or company/brand web sites
- Media production and education

(f) Content, Media and Education Officer

- Write clear, original and persuasive copy that sparks interest and generates sales

- Determine what makes products appealing to consumers and convert that into engaging copy
- Develop unique new concepts and produce copy for effective advertising and email campaigns
- Work with the Marketing team to create and develop new content ideas
- Oversee all content campaigns from start to finish
- Work within tight deadlines
- A/B test and monitor advertising/email campaigns, making necessary changes to the content without being prompted to do so
- Research competitors and stay up-to-date of market trends
- Creates, implements and manages social media campaigns
- Skilled at using available social media tools to schedule and optimize reach

(g) Third Party Content Providers

- Trading central – daily technical analysis emails

4. CONTINUOUS MONITORING

The Chief Marketing Officer is assigned by the Company which is responsible for the establishment of the necessary procedures relevant to the continuous monitoring of any marketing information to be addressed to clients. The Chief Marketing Officer reviews on a daily basis any marketing information. A relevant work plan is maintained, for the Company's records.

In the event which the Chief Marketing Officer identifies any possible variations from the version which initially has been approved, it communicates it to the Company's Executive Director for further actions and relevant ticket is send to the Marketing Officer for the rectification of the deficiencies identified.

5. WEBSITES OPERATED BY THE COMPANY

5.1 Launch of a website

For the launching of a website, the Marketing Officer shall undergo a similar procedure, as per Section 6 of this policy. In particular, prior to launching a website the Marketing Officer must receive final written approval from the Digital Marketing Manager responsible for the preparation of marketing material and an Executive Director of the Company.

5.2 Website Monitoring

The Company operates a number of websites which may change from time to time. The Company needs to ensure that at all times, that the communication made to clients through its websites is clear, fair and not misleading. In this respect and at least on a semi-annual basis, the Company's Chief Marketing Officer reviews the Company's websites in order to ensure that the material displayed on the website is in accordance with the website approvals issued by the Company. The Company needs to perform at least two (2) reviews for each of the Company's websites during a calendar year and relevant records shall be kept as evidence.

6. TRAINING

The persons employed by the Marketing Officer of the Company shall have the necessary knowledge and experience to carry out the functions assigned to them and to ensure that all employees act with the highest integrity to complete the tasks assigned to them. In addition, the Executive Directors shall ensure that the Marketing Officer is aware of the relevant legislative requirements regarding marketing communication.

The timing and content of the Marketing training shall be determined within the Company's Annual Training Plan by taking into consideration the needs of the Company. The frequency of the training can vary depending on the amendments of legal and/or regulatory requirements, employees' inquiries as well as any other changes where this is deemed necessary. However, it is noted that the Marketing Officer shall attend at least once a year to relevant training sessions, presented either in-house or by external trainer. The Executive Directors shall also arrange meetings with the Marketing Officer on a regular basis, so as to assist her/him accordingly. On-going training may be provided as and when the

need occurs so as to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments.

7. RECORD KEEPING

The Company shall ensure the proper maintenance of records in regards to the preparation, review and approval of marketing material as well as in regards to the conducting of ongoing monitoring of marketing material. In particular, the Company shall ensure the record keeping of at least the following:

1. All marketing material prepared by the Marketing Officer as per the provisions of section 6 of this policy, as well as the correspondence in regards to the approval / rejection of marketing material.
2. Work plan in regards to the conducting of ongoing monitoring of marketing material.
3. Marketing Material Monitoring Registry, as per the provisions of section 8 of this policy.
4. Evidence in regards to the approval of websites operated by the Company, as per the provisions of section 9 of this policy, as well as evidence in regards to the conducting of at least two (2) reviews for each of the Company's websites during each calendar year.

The Company shall retain all marketing material in electronic form, subject to the requirement that the Company is, at any time, in a position to retrieve them without undue delay and present them to CySEC, if requested.

In addition, the Company shall keep adequate records of any other significant communications in regards to marketing material in an electronic form. The relevant records shall be kept for at least five (5) years, as of the date that the marketing material was disseminated to clients.

8. ACKNOWLEDGMENT

This policy is required to be acknowledged by all the Company's employees as part of the Company's Internal Operations Manual.

9. UPDATES

The Company shall ensure that this policy is kept up to date and in accordance with the relevant legislative requirements. The Executive Directors of the Company, with the collaboration of the

Marketing Officer, where applicable, have the responsibility to perform a periodical review of this policy, at least once a year. The Company has the right to amend the current Policy at its discretion and at any time it considers it suitable and appropriate.

APPENDICES

Appendix 1 – Examples of good and poor practice

EXAMPLES OF GOOD PRACTISE

The following are considered as examples of good practice; although the list is not exhaustive:

- Important information, statements or warnings are presented using clear and bold type styles.
- The size of important information such as risk warnings is proportionate, taking into consideration the content, size and orientation of the marketing material as a whole.
- Both the benefits and drawbacks of a financial instrument and/or service are balanced through equally prominent feature statements.
- Risk warnings are contained within their own distinct border, thus drawing the clients' and/or potential clients' attention to them.
- Risk warnings are clearly stated within the main body of the banner/picture and/or sign/invitation for account opening and ahead of a small print.
- Risk information appears on the website(s) landing page that the clients and/or potential client first arrive at when following a promotional link.

EXAMPLES OF POOR PRACTISE

- Risk warnings are diminished through the use of small fonts sizes and unclear type styles and due to their location being outside of the main advertisement border.
- Important information, statements are covered across colored or patterned backgrounds which diminishes their visual impact.

- Important information is hidden and is only accessed through significant scrolling down and/or multiple page links.
- References which refer to indicative information and/or to fictitious and/or non-existing persons.
- Use of CySEC's and/or other regulators logos and trademarks.

HOLBORN