BUSINESS CONTINUITY POLICY

1. BUSINESS CONTINUITY POLICY

Overview

The primary objective of a Business Continuity Plan is to enable **A.N. All New Investments Limited** (hereafter "**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.

Continuity of 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.

The Company will adopt and implement detailed Business Continuity Policy.

2. Disaster and Recovery Plan Policy

Overview

This document sets out the Security policies for the IT systems of A.N. All New Investments Limited (hereafter "**The Company**").

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 organizational 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 most 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 authorized 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

Wi-Fi

Any requirement for third party access to the internet is provided through Wi-Fi Guest access.

Switches

All network switches are secured by strong usernames and passwords to secure against authorized 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 unauthorized access is allowed.

Should there be a requirement for a firewall change involving access for a third party, these rules will need to be authorized 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 several 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 Wi-Fi password is changed every six months and kept on KeePass.
- Wi-Fi 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 organization 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 server

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