12th May 2023

IT Security Plan

Introduction

This document covers the Red Mars Capital Ltd (hereinafter “the Company”) IT Security Plan (hereinafter “the Plan””) and focuses on determination of an appropriate level of security and arrangements of suitable security for departmental IT assets. The Company must take reasonable steps to ensure continuity and regularity in the performance of its regulated activities. In this respect it is understood that no department or PC is immune to compromise. Company’s information and network assets are of significant value and protecting them is our responsibility.

This policy is aimed at ensuring, in the case of an interruption to the Company’s systems and controls, that any losses are limited, the preservation of essential data and functions, and the maintenance of the Company’s regulated activities, or, where that is not possible, the timely recovery of such data and functions and the timely resumption of regulated activities.

Keeping the BCP Up-to-Date

As the Company’s Business Model becomes more established there may be a requirement to revisit the policies in this Plan in order to reflect the dynamics of the IT Security Plan at a given point in time.

The content of this Plan should be reviewed annually and at any time there is a material change in regulation, the Company’s business model or significant external changes within organisations where the Company has a dependency.

Circulation

Due to a high value of the security information contained, the present document is confidential. It is requested to keep it under the lock in case when it is not actually used. It is also not allowed to leave it lying around, photocopy it, send via e-mail or store on the server.

The following people are authorised to view this document:

- Mr. Petros Steriotis (CEO)
- Mr. Pavel Logunov (Managing Director_
- Fotios Dimitriou - IT Support Services

Asset Inventory

The following is an inventory of the physical and information assets of the Company.

Physical Assets

- Four laptops
- Twenty one monitors
- Server
- UPS
- MT5 backup server
- Firewall
- Switch
- Load balancer
- Two routers
- One access point
- One laser printer
- One TV
- Four IP phones
- Seven personal computers

Information Assets (Server Folders)

- Management
- Back Office
- Compliance
- Sales Department

Information Technology Security Safeguards

The major requirement of the present IT Security Plan that good management practices must be followed to implement information technology security based on the Red Mars Capital Ltd IT risk assessment.

The following is a list of requirements for all information systems maintained by the Company:

Physical Security

- All network servers shall be in a locked room and secured in a locked enclosure
- The office premises must have CO2 based fire extinguisher and fire blanket
- The network server room shall have a smoke detector installed in the room
- The network should be monitored for temperature and humidity
- All network servers shall be run on an uninterruptible power supply (UPS)
- An access list of personnel that are approved access to the server room or LAN/Phone closet shall be kept. A logging system shall be set up to document any visitors to the server room or LAN/Phone closet not on the approved access list. All visitors to the server room or LAN/Phone closet shall be escorted at all times
- No drinking is allowed around computer equipment
- Sensitive information shall not be stored on portable computers that are taken outside of secured areas
- Do not leave confidential information on desks after working hours or in rooms that are unattended
- When dealing with confidential information, ensure that no one is watching over your shoulders. This precaution shall also be taken when typing in passwords.

System Access Security

Authentication

The identity of each individual who accesses business information must be verified before given access to information. The identification process is normally performed using the user ID/password process.

- All users shall be forced to change their passwords every 90 days
- The Company's systems shall be set to lock out further logon attempts for at least 5 minutes after 5 failed attempts have occurred
- A notice of last logon time and date is recorded.

Password Policy

Passwords are generally obtained by 4 common methods. Therefore, the Company requires that all passwords have 4 characteristics that ensure they will not be found using one of the 4 common methods.

All password used by the Company must be:

- Long , i.e. minimum 6 characters to thwart brute force attacks
- Non-English, i.e., not in an English dictionary to thwart dictionary attacks, therefore the Company requires that all passwords have at least one non-alphabetic character in the password
- Un-guess-able, i.e. not obtainable from information known about the person. This characteristic keeps an attacker from guessing the password.
- Memorable, i.e. allow the user to remember the password without writing it down. This characteristics ensures an attacker will not find a written down password.

In addition to the 4 characteristics of individual passwords, to maintain good security individual passwords should not have any relationship to other passwords in use. That was if an attacker obtains one password, they will not be able to gain access to other passwords maintained by the same person. Passwords should not be accessible by anyone except by the owner of the password. Passwords should be changed regularly.

- Passwords should not be cyclical. When a password expires, do not name the new password as an identifiable iteration of the last password (i.e. pass1, pass2, pass3, etc.)
- Passwords used in the business should not be used on systems outside the business
- Do not share passwords with others
- Passwords must not be stored in readable form in batch files or other locations unless sufficient security precautions are taken to ensure the security of the password
- All vendor default passwords must be changed upon system installation
- If a suspected disclosure of passwords has occurred, all involved passwords shall be immediately changed
- Proof of identity is required to obtain a reset password
- All users will be forced to change their passwords at least every 90 days or their accounts will be automatically disabled
- New passwords will be issued in a state that requires immediately changing the first time the user logs on.

Data Classification

All sensitive information shall be labelled either (confidential) or (internal use only) in the document containing the sensitive information. At least once per quarter, the IT administrator will search the Company's network to ensure that confidential and internal use only documents are not accessible to the public.

- All personal data shall be treated as confidential information

- All storage medium shall be classified to highest level of information they may contain

- All storage medium must be destroyed or securely wiped before disposal.

Access Rights

Once a user is authenticated, they are only given access to information necessary to complete their job function. All data shall be controlled to limit access to individuals who need access to information.

- Inactive user IDs shall be removed every 12 months

- A list of access rights to network resources shall be generated and reviewed by management yearly.

Legal Safeguards

Licensing

- The Company must have documentation providing compliance with software license agreements. If an end user loads personal software on their PC, they must provide the Company's IT department with a copy of software license and proof of purchase or a statement saying that the users have in their possession a legal license for this software.

- The Company is committed to obey an intellectual property laws such as the copyright law as it relates to electronic information and copyrights

- The IT department will perform a periodic review of software licensing to ensure that the Company is in compliance with its software license agreements.

Privacy

- The Company shall attempt to ensure privacy of communications over its telephone and data networks

- All the Company's information systems, consisting of the equipment and information stored in the Company's information systems, are considered the Company's property, and as such may be accessed, moved, read etc. as needed to meet the Company's business requirements.

Network Usage Policy

- Any program adversely affecting the Company's information systems may be removed at the discretion of the Company's IT administrator. Programs may be considered to adversely affect the Company's information systems by consuming excessive processor time, disk space, processor memory or network bandwidth.

- Personal use of the Company's network must not interfere with normal business activities. It must not involve solicitations or be associated with any for-profit outside business activity.

Ensure System Integrity

Virus Protection

- It is the responsibility of each individual to scan their documents for viruses before sharing them with other people, both inside and outside of the Company

- A virus protection system shall be set up to automatically update all business virus scanners as new virus images released

- The virus protection system shall scan files immediately upon their saving on a server or workstation.

Redundancy and Backups

- All business data shall be stored in at least two separate locations

- Where possible, the Company's network shall be set up to limit the number of single points of the system's failure

- Monthly full backup set shall be stored for a minimum of six months.