PHYSICAL & ENVIRONMENTAL SECURITY POLICY

VARDHAMAN CAPITAL PVT LTD herewith referred as VCPL , is the SEBI registered Stock Broker & Depository Participant. The under-mentioned policy regarding Physical & Environmental security is created by the Compliance Officer and approved by the Board of Directors on 13/09/2022

The servers purchased, installed and maintained by the VARDHAMAN CAPITAL PVT LTD provides the platform for all its IT systems and services. The physical and logical security of VARDHAMAN CAPITAL PVT LTD is consequently a vital component in guaranteeing the confidentiality, integrity and availability of VARDHAMAN CAPITAL PVT LTD data.

SCOPE

This policy applies to all authorised servers hosted within the VARDHAMAN CAPITAL PVT LTD office. This policy also applies to storage area networks hosted within the site.

PHYSICAL SECURITY

- All servers will be hosted within dedicated server rooms.
- Server room will have secure perimeters.
- Server rooms will have access restricted by Access Control. Access will be limited to members of IT services engaged in server, network and telecommunication installation and maintenance work
- VARDHAMAN CAPITAL PVT LTD currently has 1 dedicated server room, situated at 25 Swallow lane Wardley house , 2nd floor Kolkata-700001
- All servers will be marked with an individual system tag and the server name.
- Proper documentation to be maintained for all entry into server room.

ENVIRONMENTAL CONTROLS

- All servers will be protected from surgers, spikes, sags or borwnouts in the electricity supply by the use of Uninterruptible Power Suppliers.
- Server room should always be kept cool with air conditioning units and checked regularly.
- All servers will be situated in racks, raising them above ground level and therefore reducing the liability of damage through flooding.
- All environmental controls equipment will be regularly maintained.
- Fire alarm systems to be installed, maintained regularly and checked under AMC.

LOGICAL SECURITY

- Remote access to server operating system shall only be granted by default to system administrators.

- Remote access may be granted to other authorised users on a case by case basis and where the request is appropriate and necessary.
- User access, where facilitated will be provided on a basis of least privilege, tight group policy implementation and limited access to programs.
- Use of utility programs is restricted to members of the systems support group.
- Desktop sessions on a server will be automatically locked after being inactive for 10 minutes.
- Server software and firmware will be patched in a timely manner

CONTROLS AGAINST MALICIOUS CODE

- Anti-virus software is installed on every server and kept up to date
- All employee desktops to be installed with anti-virus and is regularly updated automatically from the centralized server.
- All servers will sit behind firewalls.
- Internet explorer will only run in enhanced security configuration mode.

SOFTWARE

- All software on servers must be authorised and should have original licenses.
- Software on servers must only be installed by the IT department.
- All software installations, updates and removal will be subjects to the company's change management policy.
- Regular reviews of software and data content in servers classed as mission critical must be carried out.
- The responsibility to initiate reviews lies with the system owner.
- Unauthorized software or data will be removed.
- As per circulars, trading software to be upgraded with the latest versions and participate in mock trading.

MOINTORING

- Server status and operating system performance, including system resources usage and bandwidth usage, shall be monitored. Server hardware status shall be monitored. Audit logs shall record user activities, exceptions and information security events.
- Audit log information is only accessible by domain administrators.
- Keep track of all companies with proper documentation.

BACKUP

- All servers are backed up regularly and as per schedule.
- Backups are stored weekly on a continuous basis.
- Backups are to be considered a disaster recovery measures. They are not provided to restore users.

HARDWARE WARRANTIES AND REPLACEMENT

- All servers, firewall are provided with 1 to 3 years warranty.
- Warranties may be extended for further two years (up to a maximum of five years from point of purchase) as per the management decision and pricing.
- Hardware failures on in warranty services will be subject to immediate replacement.
- Replacement of servers and PC's should be done as per business requirement.

DISPOASL

- When server are removed from services their hard drives will be removed and degaussed before disposal.
- All hardware which has aged to be sold as scrap with permission from the management,
- Memory will also be removed from the chassis.

APPROVAL AUTHORITY AND REVIEW POLICY:

This policy is approved by the Board of VARDHAMAN CAPITAL PVT LTD ,

This policy may be reviewed as and when there are any changes introduced by any statutory authority or as and when it is found necessary to change the policy due to business needs.

POLICY COMMUNICATION

A copy of this policy shall be made available to all the relevant staff/persons such as: compliance officer / department in-charge /authorized persons.

Further, a copy of this policy has to be displayed on our website.