DOS & DDOS ATTACK POLICY

VARDHAMAN CAPITAL PVT LTD herewith referred as VCPL, is the SEBI registered Stock Broker & Depository Participant. The under-mentioned policy regarding DOS & DDOS is created by the Compliance Officer and approved by the Board of Directors on 01/07/2022

Denial-of-service (DoS) or **distributed denial-of-service (DDoS) attack** is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. As clarification, DDoS (Distributed Denial of Service) attacks are sent by two or more persons.

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include

- attempts to "flood" a network, thereby preventing legitimate network traffic
- attempts to disrupt connections between two machines, thereby preventing access to a service
- attempts to prevent a particular individual from accessing a service
- attempts to disrupt service to a specific system or person

IMPACT

Denial-of-service attacks can essentially disable your computer or your network. Depending on the nature of your enterprise, this can effectively disable your organization.

POLICY

The scope of the policy is for all employees, clients and sub brokers who will be accessing VARDHAMAN CAPITAL PVT LTD website, computers and other peripherals.

- To avoid DOS & DDOS attack, Firewalls can be set up to have simple rules such to allow or deny protocols, ports or IP addresses. In the case of a simple attack coming from a small number of unusual IP addresses for instance, rules to implement to drop all incoming traffic from those attackers.
- Firewalls to be updated regularly with the Database servers to get updated with the latest firmware and Databases.
- Licenses to be renewed on regular basis.
- Logs to be checked on regular basis and all logs to be mailed regularly to the admin mail ID and checked regularly.
- Implement router filters as this will lessen exposure to certain denial-of-service attacks. Additionally, it will aid in preventing users on network from effectively launching certain denial-of-service attacks.

- Disable any unused or unneeded network services. This can limit the ability of an intruder to take advantage of those services to execute a denial-of-service attack.
- Enable quota systems on your operating system if they are available. For example, if your operating system supports disk quotas, enable them for all accounts, especially accounts that operate network services. In addition, if your operating system
- Supports partitions or volumes (i.e., separately mounted file systems with independent attributes) consider partitioning your file system so as to separate critical functions from other activity.
- Observe our system performance and establish baselines for ordinary activity. Use the baseline to gauge unusual levels of disk activity, CPU usage, or network traffic.
- Routinely examine our physical security with respect to our current needs. Consider servers, routers, unattended terminals, network access points, wiring closets, environmental systems such as air and power, and other components of your system.
- Use Tripwire or a similar tool to detect changes in configuration information or other files.
- Establish and maintain regular backup schedules and policies, particularly for important configuration information.
- Establish and maintain appropriate password policies, especially access to highly privileged accounts such as UNIX root or Microsoft Windows NT Administrator.
- Keep in regular touch with Tata Communications to check for any untoward surge in Internet Bandwith static wise and keep the router on monitoring mode.

PROCEDURE

- Immediately check for the source of the DOS attack, the machine and the switch.
- Have to shut down the computer immediately.
- Also get in touch with the ISP to know whether they have any details which static IP has been targeted, check their router for details.
- If possible , check for the logs on the firewall , take a case with Fortigate support team , send them the full tech files for investigation and take their support

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.