ACCESS POLICY

VARDHAMAN CAPITAL PVT LTD, herewith referred as VCPL, is the SEBI registered Stock Broker & Depository Participant. The under-mentioned access policy is created by the Compliance Officer and approved by the Board of Directors on 04/05/2022

POLICY STATEMENT

VARDHAMAN CAPITAL PVT LTD will establish specific requirements for protecting information and information systems against unauthorized access. VARDHAMAN CAPITAL PVT LTD Ltd will effectively communicate the need for information and information system access control.

PURPOSE

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of VARDHAMAN CAPITAL PVT LTD which must be managed with care. All information has a value to the company. However, not all of this information has an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorized use.

Formal procedures must control how access to information is granted and how such access is changed.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

SCOPE

This policy applies to all VARDHAMAN CAPITAL PVT LTD Employees and support staff with access to privileged administrative passwords), contractual third parties and agents of the company with any form of access to VARDHAMAN CAPITAL PVT LTD information and information systems.

RISKS

On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorization and clearance may intentionally or accidentally gain unauthorized access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

Non-compliance with this policy could have a significant effect on the efficient operation of the Company and may result in financial loss and an inability to provide necessary services to our customers**.**

Applying the Policy – Passwords (Also can verify our Password Policy for more details)

CHOOSING PASSWORDS

Passwords are the first line of defense for our ICT systems and together with the user ID help to establish that people are who they claim to be.

A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems. There are different type of password such as weak and strong passwords. Changing passwords are also recommended for better work and more details are given in our password policy. The password administration process of VARDHAMAN CAPITAL PVT LTD is well-documented and available to designated individuals.

Applying the Policy – Employee Access

USER ACCESS MANAGEMENT

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorized user access and to prevent unauthorized access. They must cover all stages of the life cycle of user access, from the initial registration of new users to the final DE-registration of users who no longer require access. Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. Review of user creation, deletion and marking of responsibility should be done periodically to prevent unauthorized access. It should be ensure that PC left unattended is locked or logged out.

NETWORK ACCESS CONTROL

The use of modems/Wi-Fi/Internet on non-VARDHAMAN CAPITAL PVT LTD owned PC's connected to the company's network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Approval must be obtained from IT Department before connecting any equipment to the Company's network.

USER AUTHENTICATION FOR EXTERNAL CONNECTIONS

Where trading trough the VARDHAMAN CAPITAL PVT LTD network is required, access to the network must be secured by two factor authentication wherever necessary. SSL certificate to be installed on the critical server

SUPPLIER'S REMOTE ACCESS TO THE COUNCIL NETWORK

Partner agencies or 3rd party suppliers must not be given details of how to access the company network without permission from IT Department. All permissions and access methods must be controlled by IT Department.

Partners or 3rd party suppliers must contact the IT Department before connecting to the VARDHAMAN CAPITAL PVT LTD network. Remote access software must be disabled when not in use.

OPERATING SYSTEM ACCESS CONTROL

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section and the Password section above must be applied. The login procedure must also be protected by:

- Not displaying any previous login information e.g. username.
- Limiting the number of unsuccessful attempts and locking the account if exceeded.
- The password characters being hidden by symbols.

All access to operating systems is via a unique login id that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g. administration rights).

APPLICATION AND INFORMATION ACCESS

Access within software applications must be restricted using the security features built into the individual product. The IT department / RMS department / Director of the software application is responsible for granting access to the information within the system. The access must be as per below list –

- Be compliant with the User Access Management section and the Password section above.
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorized higher levels of access.
- Be logged and auditable.

POLICY COMPLIANCE

If any user is found to have breached this policy, they may be subject to disciplinary procedure. If a criminal offense is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from IT Department.

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.