PRIVILEGE IDENTITY MANAGEMENT POLICY

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

INTRODUCTION

Presently the individuals are not only using credentials of logins but also other type of network. The IT personnel who maintain servers, network components, and software use special passwords with elevated permissions needed to install new hardware and software, configure services, and service the IT infrastructure.

Called privileged identities, these logins allow unrestricted access to view data, alter configuration settings, and run programs. Typically associated with hardware and software assets (and not with any one user), privileged identities grant "super-user" access to virtually every resource on your network including:

- The operating systems that run all computer platforms,
- The directory services that control access to your network,
- Line-of-business applications, databases, and middleware,
- Network and security appliances,
- Backup and other service software and appliances,

PROCESS

Effective privileged identity management processes can improve staff efficiency and effectiveness by introducing the means to:

- Follow repeatable processes that reduce the time needed to maintain up-to-date lists of privileged accounts present on software and hardware resources;

- Reduce the time and uncertainty of changing privileged account passwords through use of up-to-date documentation of the accounts;

- Eliminate the time and uncertainty of obtaining approvals and retrieving passwords when needed to access systems for routine maintenance and emergency repairs.

- Automate the tasks to document the presence of privileged accounts and their access history, as required by regulatory standards;

- Support root-cause analysis to more quickly determine the reasons for undesired changes; giving staff the tools to know who requested privileged access to IT assets in question, when, and for what purpose;

- Eliminate staff time taken to re-mediate negative audit findings that would otherwise occur.

PROCEDURE

- Privileged identities allow unrestricted access to view and change data, alter configuration settings, and run programs.
- All Privileges are granted on users based on appropriate approval and as per user's roles and responsibility.
- Log reviews are conducted periodically.

CONCLUSION

As IT auditors become more aware of the threats posed by unmanaged privileged identities VARDHAMAN CAPITAL PVT LTD could face increasing pressures to bring these powerful logins under control. Hackers have also taken notice, increasing the frequency of attacks that exploit shared, elevated credentials to gain control of victim organizations' networks.

Fortunately, privileged identity management software can help you continuously secure privileged credentials throughout your network and provide an authoritative audit trail of their access. A successful implementation can also save IT staff time by providing login credentials instantly and on-demand, reducing the need for manual processes to discover, change, and document the accounts.

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.