ASSET MANAGEMENT POLICY

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

INTRODUCTION

VARDHAMAN CAPITAL PVT LTDrecognizes the importance of ensuring its assets are identified, recorded and protected. The company ensure that all assets which it manages and owns are accounted for, maintained and controlled through the implementation of best practice, recording mechanisms, processes and procedures.

PURPOSE

The purpose of this policy is to ensure that all Company's assets are identified recorded and to establish professional good practice in the maintenance, protection and classification of all VARDHAMAN CAPITAL PVT LTDassets.

The Company's categorizes assets as:

- Information and Information Systems:
    - Hardcopy documents
    - Data files
    - Databases
    - User guides
    - Training material
    - Policies, Procedures
    - Financial Data
    - Business Continuity plans
- Software:
    - Applications
    - System software
    - Development software
    - Utilities software
- Physical:
    - Computer equipment
    - Communications equipment
    - Media – storage and recording
    - Property and accommodation
- Services:
    - Utilities (power. lighting, environmental controls)
    - communication
- Personnel:
    - Knowledge
    - Skills
    - Experience

SCOPE

This scope of this policy extends to all Company's departments, employees, elected members, contractors, vendors and partner agencies who utilize or who are responsible for the development, management and maintenance of all Company's ICT assets. The Company's must take the following steps to ensure all assets are appropriately identified, recorded and maintained.

INFORMATION AND INFORMATION SYSTEMS

Data and information held and maintained by the Companies can either be in hard copy form stored in physical locations, filing systems, office locations or stored electronically using software and electronic backup systems.

Types of Information and Information Systems assets:

- Databases – Access to these must be given to authorized employees only and logs should be maintained to record all access to and changes made to any data held within any database system
- Data files – log maintenance system should be developed whenever logically possible.
- Hard copy documents – All hard copy documents containing sensitive and personal identifiable data must be accessed, processed, maintained and securely stored.
- Training material – All relevant training material(s) must be stored and made readily accessible to all relevant employees. Duplication or physical reproduction of training manuals must be kept to a minimum and avoided wherever possible
- Policies, Procedures – All Company's Policies and Procedures should be made available and disseminated via official mail – All original copies of Policies and Procedures documents whether electronic or hard copy must be safely stored, regularly reviewed and a version history control record must be maintained for each document to ensure they are up to date
- Business Continuity plans – All Business Continuity plans must be regularly reviewed, disseminated to appropriate employees and stored safely for easy retrieval as and when necessary
- Financial Data – Data and Information relating to company financial data must be restricted to authorized employees only. Recording mechanisms must be in place for logging access, changes and use of financial data and information

SOFTWARE

Computer and IT systems software is widely used across the Company's and is vital to the day to day running of the Company's and in providing essential services to the public

The use of software has continued to change the way the Company's works. Substantial investment has been made in Software along with accompanying ongoing costs and expenditure such as annual software/systems support, licensing and staff training.

- Applications – *Software used by the Company must be appropriately sourced and must be evaluated for business need, suitability, efficiency, ease of use, cost effectiveness and integration into existing company systems. Appropriate numbers of software licenses must be purchased to cover volume of use and to satisfy legal requirements. Software media must be stored (physically and electronically) in a secure, centralized location. Access to Software media by employees must be controlled and limited to authorized employees only. All installations with the original software's to be done by the IT department only. All applications licenses to be

reviewed, renewed and updated for next renewal or updating.

☐ System software – Server/system software such as Operating Systems, must be evaluated for business need, suitability, efficiency, cost effectiveness and integration into existing company systems. Operating System installation media must be stored in a secure area along with installation codes. Access to Server/system software media by employees must be controlled and limited to authorized employees only. Backups of complete Server/systems installations must be routinely carried out for disaster recovery purposes. Installation, configuration and maintenance of Server/system software must only be undertaken by employees who are trained and qualified to do so. Wherever required Licenses to be renewed and updated regularly.

☐ Development software – software for the support of existing systems and for the development of in-house solutions must follow the same processes for procurement and use as for the Applications and Server/systems software. Development software should only be used by employees who are trained or who are undergoing training to use the Development software.

PHYSICAL

VARDHAMAN CAPITAL PVT LTDmost visible assets are those which are physically located throughout the company such as computers, printers and phones etc. Offices and buildings must also be considered as company's assets – providing location for the housing and installation of the company's Data and Communications Network infrastructure and physically stored documents and information.

☐ Computer equipment – A large number of computing devices - which includes PDAs, laptops, monitors etc., are in use across the company. Computers are one of the costliest single items of equipment and must be subject to controls from procurement to disposal. The company must be able to track all activity and use relating to all company computing devices using various means Each computer must have the tag number and major up gradation whenever required.

☐ Communications equipment – Mobile phones, office IP phones are widely used communications devices in use across the Company. Other network and communications devices identified as assets include routers, switches, video conferencing equipment etc. Along with computing equipment, these devices must be allocated an asset tag number.

☐ Media storage and recording – Media such as CD/DVDs, Magnetic tape, and flash/portable hard disks are valuable assets because they are used to save and retrieve Company information and data. The portable nature of this type of media requires responsible use and adherence to all Company policies, procedures and processes which are in place for the protection of information and data. Appropriate labelling and recording mechanisms should be in place to ensure the safety and integrity of media - enabling tracking of essential media such as for data backups e.g. media required to carry out data/file restores must be signed in and out from a secure location.

SERVICES

- Communications – It is vital for the company to maintain its ability to communicate in many different forms. E-mail/sms is also a vital means of communication and as such, requires a robust, reliable infrastructure to enable the company to communicate effectively and reliably, both internally and externally
- Utilities (power. lighting, environmental controls) – These services are assets as they provide fundamental requirements for the Company's to function appropriately, safely and effectively. It is essential that property maintenance and inspections are routinely carried out and that employees are proactive in reporting faults, whenever noted.

PERSONNEL

VARDHAMAN CAPITAL PVT LTDcannot function without its workforce – it is its largest asset. The provision of good public services requires all employees to have the necessary skills, knowledge and ability to work within many different areas and departments across the company. The number of unique functions and specialisms across the company requires a varied knowledge and skills base which must be supported by robust recruitment processes, appropriate training provision and good management of employee skill identification, work placement and allocation. When an employee leaves the company, and other assets to be taken back from him and checked.

ACCEPTABLE USE OF ASSETS

All Company's departments, employees, elected members, contractors, vendors and partner agencies must observe and abide by all Acceptable Use policies and procedures pertaining to all Company's owned ICT assets

BREACHES OF POLICY

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to company's assets, or an event which is in breach of the company's security procedures and policies. This obligation also extends to any external organization contracted to support or access the Company's Assets.

The Company's will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

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.