Asset Management Policy

CHANGE HISTORY

Date	Version	Created by	Approved By	Description of change
08/10/2024	1.0	Bharath S	Ashwin Khosla	Basic document outline and submitted for review

Purpose

The purpose of the Asset Management Policy is to outline the guidelines and practices that govern decisions on asset management at **Veranda Learning** and also to ensure that assets and data in those assets are properly classified (based on their business value). This policy's measures are implemented to protect **Veranda Learning** data from unauthorized disclosure, regardless of if it is being shared, transmitted, or stored. The policy describes how to identify and draw up an inventory of assets in the Company.

Scope

The Asset Management policy applies to the following assets & equipment

- All assets such as servers and network
- All corporate assets issued and used by the Company's employees
- All assets, computers, and devices issued to vendors/ third-party/visitors
- All software and other information systems such as file drives etc
- Any other tangible and intangible information asset

Background

Asset management is the process of receiving, tagging, documenting, and eventually disposing of equipment. It is critically important to maintain up-to-date inventory and asset controls to ensure computer equipment locations and dispositions are well known. Lost or stolen equipment often contains sensitive data. Proper asset management procedures and protocols provide documentation that aids in recovery, replacement, and insurance activities.

Policy

Asset types

The Company must maintain an inventory of its information systems which include

- **Tangible Information Assets:** A tangible information asset has a finite monetary value and usually a physical form. (e.g., laptops, server)
- **Intangible Information Assets:** Intangible assets include non-physical assets that usually have a theoretical value. (e.g., trademarks, patents)
- **Physical IT assets:** Switches, routers, Wi-Fi access points, VoIP telephony devices, personnel identification, authentication/access control devices (card-access systems, etc.), and other security devices (CCTV, etc.)
- **IT Hardware:** Computing and storage devices e.g., desktops, workstations, laptops, tablets, servers, communications devices (network nodes), printers/copiers/FAX machines and multifunction devices, and other IoT devices.
- **IT Service Assets:** User authentication services and user administration processes, firewalls, proxy servers, network services, wireless services, anti-spam/virus/spyware, intrusion detection/prevention, teleworking, security, FTP, email/IM, Web services, software maintenance, and support contracts.

Asset inventory

Each asset should, at the minimum, have the following information in the asset inventory.

- Identifier
- Name

- Serial Number
- Owner
- Location information
- Stores PII information or not
- Asset classification
- Value
- Purchase and other procurement information

Wherever available following information must be also tracked

- Date of purchase,
- Make and Model
- OS type and version
- Serial Number
- Asset Category
- Department
- Risk Level

Asset inventory must be up to date, current, and reflect the Company's latest assets.

Ownership and assignment

Ownership must be assigned to each asset in the asset inventory.

Asset owners must ensure that assets are appropriately classified and protected, and access requirements are periodically reviewed.

The asset owner must determine the asset's value or criticality using assets impact confidentiality, integrity, and availability.

Acceptable use

The Acceptable Use Policy governs the acceptable use of each asset. In general, the policy requires that under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing company-owned assets. The use of all assets must be strictly for the Company's business purposes.

Asset disposal

- Employees, Contractors should return organization assets upon termination of their employment, contract, or agreement.
- Assets containing confidential information should be disposed of securely. (e.g., by incineration or shredding, or erasure of data for use by another application within the organization)
- Assets should be properly recycled before reassignment.

Enforcement

Asset Management policy is enforced by the Information security team. All exceptions to the policy should be brought to the attention of the information security team along with the executive management of the company. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Mapping with Industry Standards

This policy addresses the following risks related to Asset Management and Information Security standards, frameworks:

Risk	Mapping to ISO 27001 2022
Unauthorized access	5.9 Inventory of Information and Other Associated Assets 5.10 Acceptable Use of Information and Other Associated Assets 5.11 Return of Assets 5.12 Classification of Information 5.13 Labelling of Information C 7.1 Resources
Information Leakage	7.9 Security of Assets Off-premises 7.10 Storage Media
Theft	5.9 Inventory of Information and Other Associated Assets 5.10 Acceptable Use of Information and Other Associated Assets 5.11 Return of Assets
Physical Loss or damage	5.10 Acceptable Use of Information and Other Associated Assets 5.11 Return of Assets

Non- Compliance

Violations of the policy may subject employees to disciplinary action, including removal of privilege to the systems, up to and including termination of employment. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

- Disciplinary action according to applicable Veranda learning policies.
- Termination of employment.
- Legal action according to applicable laws and contractual agreements.

Validity and Document Management

The owner of this document is the management, who must check and, if necessary, update the document at least once every 12 months.