ACCESS 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 Access Management Policy is to define the level of access each user has to company-owned or managed information systems and the data in Veranda Learning's systems. This policy document describes the general access rules for all company-owned or company-managed information systems.

Scope

The Access Management Policy applies to the following.

- All Employees of Veranda Learning
- All Contractors of Veranda Learning
- All vendors / third-party/visitors who temporarily access Company's equipment
- All information systems of the Veranda Learning
- All data repositories of the Veranda Learning

Background

The Access Management Policy defines the rules put in place to help prevent unauthorized, illegal, or malicious access to information systems and resources owned by Veranda Learning. This policy also defines the rules for how access is requested, granted, and revoked to the information systems for an employee or third-party contractor. This policy also defines the rules in place for an individual to request elevated/privileged access to systems and resources for temporary use. This policy also defines at a high level the type of accounts used however the actual implementation of these accounts is delegated to the individual systems themselves. The policy also outlines strong authentication mechanisms such as passwords and multifactor authentication, but those are discussed in detail in the Password Policy document.

Policy

The Company shall implement the principle of "least privilege" and "role-based access control" within logical access control mechanisms so that only authorized users can access company systems and data.

Types of account

All information systems must have one or more of these account types.

- Administrator accounts (with Superuser access)
- User accounts based on role in the information system
- System accounts
- Privileged accounts

General User access management

- All employees, contractors, and third-party users are assigned a unique identifier.
- All information systems of the Company must require at least a User Id and a password to log in and gain access to the system.
- Each information system must enforce the password and login restrictions based on the password policy.
- Each information system should define, document, and implement its unique access management covering all aspects of the user lifecycle from onboarding to offboarding.

- Each information system must follow a minimum privilege policy, ensuring that the access rights to the users are minimum and required to perform the tasks expected of the users.

New user onboarding

- All new employees of the Company must onboard using an onboarding checklist or an onboarding process.
- Employees or users must request access to department-level information systems to the appropriate department manager, who must approve access to department-level information systems.
- Special privilege requests must be submitted based on the new employee's ROLE to the appropriate information system owners.
- Elevated access must have at least two levels of approval and must be strictly reviewed and only provided if users' day-to-day tasks require it.

User offboarding

- The responsible party must revoke terminated employee's access by the end of the day of the employee's last working day in the Company.
- The responsible party could be the terminated employee's direct manager, Company's HR department, or the IT department. The responsible party must ensure the review and revocation of access of the terminated employee.
- System owners must access review orphan accounts or access terminated employees.

Elevated access management

- Elevated access must be formally requested from the IT team or from the information system owners whose access is required.
- Elevated access must be time-bound and have a date and time at which the access will expire and be revoked.
- Elevated access can also be granted for an incident, and it is the responsibility of the owner to revoke that access.
- Elevated access should follow the principle of minimum privilege.
- Elevated access must be reviewed at least every six months to ensure that the users with elevated access are still in the roles requiring elevated permissions.

Access management for third parties/contractors

- All-access requests for contractors and partners should follow the same process as mentioned in the sections above.
- Access for third-party workers, contractors, and partners must be enabled for the approved period during which their partnership agreement or contract is valid.
- Remote access to third-party contractors must be provided only after a formal request.

Password and other authentication mechanisms

- All information systems must enforce a login with password requirements as defined in the password policy document.
- Information systems with highly classified data should enforce multi-factor authentication (MFA) as defined in the password policy document.

Audit and Log

- All user access to information systems must be logged.
- At the minimum, logs must contain the unique Id that can be linked backed to a system user.

- All logs must be stored for at least 60 days.
- All logs must automatically alert for malicious access attempts or be reviewed manually every 30 days

Mapping with Industry Standards

This policy addresses the following risks related to Access control and Information Security standards, frameworks:

Risk	Mapping to ISO 27001:2022
Loss of CIA (confidentiality, Integrity and Availability)	5.15 Access Control 5.16 Identity Management 5.18 Access Rights 6.7 Remote working 8.2 Privileged Access Rights 8.3 Information Access Restrictions 8.4 Access to source code
Unauthorized access	5.15 Access Control 5.16 Identity Management 5.17 Authentication Information 5.18 Access Rights 5.33 Protection of records 6.7 Remote working 8.2 Privileged Access Rights 8.3 Information Access Restrictions C 10.1 Continual improvement
Information Leakage	8.3 Information Access Restrictions 8.5 Secure Authentication 5.17 Authentication Information

Enforcement

The Access Management Policy is enforced by all system administrators and department heads to all company administered information systems and any exceptions must be reviewed and approved by the information security team. All and any breaches of this policy will be subject to the company Code of Conduct and Sanctions Policy.

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.