SECURE REMOTE ACCESS CONTROL 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

Policy Statement

The organization has adopted this Remote Access Control Policy in order to recognize the requirement to comply with the NIST 800-53. The access control and account management policy provides the understanding of gaining access to Platform services for internal and external users. The organization manages all access through the account management process. The Organization is responsible for managing privileged and non-privileged internal user access

Purpose

The Organization has chosen to adopt the Access Control (AC) family of security controls established in NIST SP 800-53, Revision 4 as the official policy for this domain. The purpose of this Remote access control Policy and Procedures (AC-1) document is to protect the integrity of the Platform by establishing access controls. All policies and procedures herein reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

Scope

The scope of this policy is applicable to all Platform resources owned or operated by the Organization and its affiliates. All Platform users, including the general public, Organization employees, contractors, vendors, or others, are responsible for adhering to this policy.

Roles and Responsibilities

Role	Responsibility
Management	• Reviews security plan to determine if plan is completely consistent and satisfies the stated security requirements for the information system • Approves the selected set of security controls, including all tailoring and supplementation decisions, any use restrictions and minimum assurance requirements.
Information owner	• Determines the suitability of common NIST security controls for use in information system • Determines assurance measures that meet NIST 800-53 minimum assurance requirements selected for the system • Defines a continuous monitoring strategy for the information system

Security officer	• Ensures the Information Security policy is submitted to the Information Owner • Supports the information system owner in selecting security controls for the information system • Supports documentation and dissemination of information system policies and procedures.

Mapping with Industry Standards

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

Risk	Mapping to ISO 27002:2022
Loss of CIA (Confidentiality, Integrity and Availability)	5.15 Access Control 6.7 Remote Working 8.1 User end point devices 8.24 Use of cryptography
Unauthorized access	5.15 Access Control 6.7 Remote working 8.1 User end point devices 8.22 Segregation of networks
Information Leakage	5.15 Access Control 6.7 Remote working 8.1 User end point devices

Compliance

The security controls defined in this remote access control policy and procedures document to comply with all applicable laws, directives, policies, regulations, standards, and guidance. The ISSO enforces compliance with audit and accountability controls described herein and disseminates reference materials to appropriate members within the organization. The content of remote access control policy and procedures is reviewed and updated at least annually by the Security officer

Procedures

Remote Access for Platform Workforce Members

1. Remote access is granted to all employees at Veranda Learning Technologies, working on supporting and managing the platform
2. Unique usernames and passwords are provided directly to the user
3. All employees must use Auth0 authentication to log into the Platform
4. All employees accessing any company systems must have MFA enabled to ensure secure access.

5. All employees who access Veranda Learning infrastructure (AWS)need to use bastion host
6. We use TeamViewer remote access and control software for supporting internal and external users when needed
7. We use VPNs externally to connect to some customers and these VPNs are managed predominantly by our vendor.

Remote User Responsibility

1. It is the responsibility of all Veranda Learning employees with privileges to ensure that unauthorized users are not allowed access to the internal organization's cloud and associated content.

2. All individuals and machines, while using remote access to log in to the cloud including Veranda Learning-owned equipment, are a de facto extension of the organization's network, and as such are subject to the code of conduct policy.

3. Veranda Learning does not have an internal network. All of our systems are cloud-based solutions hosted by AWS or a vendor partner.

4. All network activity during remote access is subject to platform policies.

5. Google authentication is enabled to connect between vendor platforms

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.