Risk 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 Risk Management Policy is to ensure that Veranda Learning is managing risk to the best of our ability to enable the successful achievement of the Veranda Learning's objectives. This policy outlines the risk assessment process in place at Veranda Learning and how and how often threats are identified, and appropriate risks identified along with security controls.

Scope

The Risk Management Policy applies to the following:

Personnel

- All Employees of Veranda Learning
- All Contractors of Veranda Learning
- All vendors / third-party/visitors who temporarily access Veranda Learning's equipment

Equipment

- All computers/laptops provided by Veranda Learning
- All mobile devices
- Internet and Intranet usage
- Software procured

Background

Risk assessment is a key component of the Information Security program at Veranda Learning. The primary objective of risk assessment is to identify vulnerabilities, assess the impact of that vulnerability being exploited, determine how likely is it for a threat to exploit the vulnerability, and define the consequence of that vulnerability being exploited. All these factors contribute to identifying risks at Veranda Learning. The risk assessment process also identifies security controls that effectively mitigate the identified risks. Senior management at Veranda Learning is actively involved in the risk assessment process and in reviewing and approving the controls to mitigate risks.

Policy

Veranda Learning maintains an information security risk management program to evaluate threats and vulnerabilities in order to assure the creation of appropriate remediation plans.

Risk Assessment

- A risk assessment is performed and/or updated every quarter.
- A representative from the information security team, a member from the senior management team, a member from the operations management team and the compliance team take part in the risk assessment process.
- Veranda Learning uses an asset-based risk assessment approach where each asset owner is asked to list down the vulnerabilities and threats their system face.
- A qualitative (1-5) assessment of the likelihood of that threat and the impact of exploitation is documented
    - Likelihood
        - Rare (1)
        - Unlikely (2)
          Possible (3)

        - Likely (4)
        - Certain (5)
    - Impact
        - Negligible (1)
        - Marginal (2)
        - Significant (3)
        - Critical (4)
        - Catastrophic (5)
- A risk score is calculated by multiplying Likelihood * Impact. The higher the score, the higher the risk for the organization.

Mitigating risks

- At the end of each assessment, risks are accepted or remediated. Security controls are created to mitigate unacceptable risks.
- One of the following risk treatments is applied
    - Avoid
    - Reduce
    - Transfer
    - Share
    - Accept
- Mapping of security controls to risks is maintained
- Action items are created to mitigate each risk
- A treatment plan for each risk is also documented.

Reporting Risks

- A report of risk assessment is generated post-assessment and sent to all senior management for review and approval.
- The report contains the following
    - Asset
    - Identified Vulnerability
    - Threat associated
    - Likelihood and Impact Score
    - Consequences
    - Risk level
    - Attached Controls
    - Residual Risk
    - Risk Owner

Mapping With Industry Standards

This policy addresses the following risks related to risk management and Information Security standards, frameworks:

Risk	Mapping to ISO 27001:2022
Failure to identify security risks	5.7 Threat intelligence 5.9 Inventory of information and other associated assets

	C 6.1 Actions to address risks and opportunities
Non- adherence to laws and regulations	5.31 Legal, statutory, regulatory and contractual requirements
Lack of systematic approach to risk management	5.1 Policies for information security 5.6 Contact with special interest groups C 8.2 Information security risk assessment C 8.3 Information security risk treatment
Absence of independent review of risk management practices	5.35 Independent review of information security

Enforcement

Risk management policy is the responsibility of the information security team, compliance team, and all asset owners. Compliance team is responsible for leading and coordinating risk assessment exercise.

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