INFORMATION SECURITY 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
This information security policy defines principles, objectives, and basic rules for information security management in Veranda Learning.

Scope
Information security policy applies to all personnel, third-party vendors, suppliers, assets, facilities, physical locations and information systems.

Background
Information security at Veranda Learning is built on the 3 essential tenets of information security

- Integrity
- Confidentiality
- Availability

This policy outlines how the Information security program in Veranda Learning is built on these above principles by effective use of

- Senior management resources
- Written policies and procedures
- Quarterly risk assessments
- Employee security awareness training
- Incident management
- Business continuity and disaster recovery

This policy also defines management roles and responsibilities for the organization's Information Security Management System (ISMS). Finally, this policy references all security controls implemented within the organization.

Policy

Information Security Program

Veranda Learning has implemented a comprehensive information security program that will secure all information assets commensurate with each asset's value as established by risk assessment and mitigation measures.

The information security program is updated and re-approved by Veranda Learning's Infosec team

- Annually
- When there is a material change in the organization
- Material changes to infrastructure
- New security incidents/threats
- Updated risk assessments.

Management Responsibility

Information security is a management responsibility, and decision-making for information security is not delegated. While specialists and advisors play an important role in helping to make sure that controls are designed properly, functioning properly, and adhered to consistently, it is the manager in charge of the business area involved who is primarily responsible for information security.

Primary Departments Working On Information Security - Guidance, direction, and authority for information security activities are centralized for all Veranda Learning organizational units in the Information Security Program and summarized in this document. Veranda Learning management is responsible for establishing and maintaining organization-wide information security policies, standards, guidelines, and procedures.

Compliance checking to ensure that organizational units are operating in a manner consistent with these requirements is the responsibility of department managers. Investigations of system intrusions and other information security incidents are the responsibility of the IT/Security and Product teams. Disciplinary matters resulting from violations of information security requirements are handled by local managers working in conjunction with the HR department.

Although all security policies and procedures play a critical part in Veranda Learning's information security, below are essential areas on which the overall Information Security Policy is built.

Access Control

Veranda Learning implements 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.

- Each information system enforces the password and login restrictions based on the password policy.
- Each information system also defines, documents, and implements its unique access management covering all aspects of the user lifecycle from onboarding to offboarding.
- Appropriate Onboarding & Offboarding workflows and checklists are implemented as per the Access Control Policy for new and terminated employees.
- Elevated and privileged access is granted only for limited durations and special approvals.
- Veranda Learning's access control policy also applies to all third-party contractors and vendors also

Strong passwords & login control

Strong passwords for an application are the first line of defense against malicious actors; hence Veranda Learning password policies establish rules of how employees can maintain strong and secure passwords when using multi-factor authentication and how all information systems can enforce best practices for strong passwords.

Strong password policy

- Strong, complex passwords are enforced for all applications
- MFA is enforced for all users of critical and crucial applications
- All administrative users should have MFA enabled.

Access audit and logging

- All user access to information systems is logged.
- All logs are stored for at least 60 days.

Asset management

Veranda Learning maintains an inventory of all its information systems. All assets have owners and custodians assigned.

Acceptable use Policy

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 disposition Policy

Employees, Contractors should return organization assets upon termination of their employment, contract, or agreement. Assets are disposed of and recycled as per the data retention and disposition policies.

Encryption Policy

All critical and sensitive data in databases is encrypted. This includes but is not limited to

- Customer data in production environments
- Application data in production environments
- Document / Object stores such as S3 buckets
- Audit logs and application logs

All data in transit is encrypted. All data flowing in and out of the Company shall use SSL, TLS, and IPSec for transmission.

The encryption policy requires the use of strong and latest encryption algorithms. Standards are set for cryptography key management, such as all keys must be rotated every six months.

Data Classification policy

Information in Veranda Learning is classified based on legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification. The classifications are based on the value of information and impact on business due to loss or theft of that information identified during risk assessment.

The following sections outline the data classification level in Veranda Learning of the data and information across different information types and systems in Veranda Learning.

All sensitive information is labeled with the appropriate classification label when shared internally or externally. Whenever not known, the lowest and most restrictive level data classification is used. The labeling is applied to information and data in

- Paper documents
- Emails
- Electronic documents
- Application data
- Electronic media

Restricted: Restricted information is highly valuable, highly sensitive business information, and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need. All data are to be assigned one of the following four sensitivity levels:

Confidential: Confidential information is highly valuable sensitive business information, and the level of protection is dictated internally by Veranda Learning.

Internal Use: The internal Use information is information originated or owned by Veranda Learning, or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact on the Company's business interests.

Public: Public information is information that has been approved for release to the general public and is freely sharable both internally and externally.

Data retention policy

Veranda Learning maintains a data retention policy that specifies what data to retain and how long it is retained.

For example-

- Customer data is retained for the duration set in the contracts and SLAs.
- Application data

- Will be maintained during the full duration of the relationship
- Will be maintained till 45 days after the duration of the relationship
- Will be maintained during the duration of the trial
- Will be deleted between 7- 14 days after the trial or the relationship ends

Backup Policy

The purpose of the Backup Policy is to maintain data integrity and availability of the Veranda Learning's information system, to prevent loss of data, and to facilitate the restoration of the information system and business processes.

Loss of data is prevented by performing regular backups to meet the RPO (Recovery Point Objective) and RTO (Recovery Time Objective). Refer to the Data Retention Policy for RTO and RPO.

Backup schedules are maintained for all information systems centrally.

For Veranda Learning data for critical information systems must be backed up at least 2 times a day.

All data backups should be kept for at least 30 days and after that it could be moved to archives for data retention and legal purposes

All backup data must be stored encrypted with the AES-256 symmetric encryption algorithm.

Backup copies are tested every quarter for recovery capability.

Availability Policy

All Information systems have defined, documented, and agreed upon SLAs for availability for all customers.

Unique availability SLAs for customers are documented and agreed upon formally in writing.

All critical systems have redundant databases.

Tests of backup data are conducted twice per year.

Tests of configurations must be conducted twice per year.

Backups and associated media are maintained for a minimum of thirty (30) days and retained per legal and regulatory requirements.

The network infrastructure that supports critical resources must have system-level redundancy (including but not limited to a secondary power supply, backup disk array, and secondary computing system).

Critical core components (including but not limited to routers,

Risk Management Policy

Risk assessment is a critical 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 it is for a threat to exploit it, 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.

Logging

To measure an information system's level of security through confidentiality, integrity, and availability, the system collects audit data that provides critical insights into system performance and activities. This audit data is collected in the form of system logs. Logging from critical systems, applications, and services provides information that can be a starting point for metrics and incident investigations. This policy provides specific requirements and instructions for how to manage such logs.

Event logs with user activities, exceptions, faults, and information security are produced, kept, and regularly reviewed. The organization utilizes automated audit trails for system components to reconstruct events.

Monitoring

Automated tools are deployed in Veranda Learning Inc to monitor abnormal behavior intrusion detection logs. System alerts are set up to alert the system owners if malicious activity is detected in real-time. Resource usage is logged, and alarms are triggered if unusual activity is detected outside the threshold of normal operations.

Incident Response Policy

Security incidents happen, and the best thing an organization can do for its customers is to be best prepared for them. Incident Management policy outlines the procedures for managing security incidents at Veranda Learning. It outlines the processes in place to ensure that

- Proper controls are in place to monitor and alert when security incidents happen.
- The right team is identified, trained, and available to investigate and resolve the security incidents.
- Proper communication channels and SLAs are in place with the customer to inform the customer of the incident.
- Right learnings and corrective actions are captured and iteratively applied to improve incident response procedures.

Business Continuity Policy

Veranda Learning continuously aims to preserve critical business operations and essential functions to deliver essential products and services. This policy outlines how Veranda Learning ensures this continuity.

- This policy puts a structure and authority to ensure business resilience of operations and information systems.
- This policy puts a plan to manage business operations through the disaster period and the effort it will take to get back to normal operations.

- This policy defines a disaster recovery plan containing a set of human, physical, technical, and procedural resources to return to a normal level of operation, within a stipulated time and cost, in case of an emergency or disaster.

Vulnerability Management Policy

At Veranda Learning a vulnerability scan and assessment of all critical information systems are conducted at least once every 6 months. The scan includes

- Network scan
- Application scan
- Server and computer scans
    - o A third-party vendor conducts the scan
    - o The scan tries to find vulnerabilities that are related to
- Known vulnerabilities
- Application vulnerabilities
- Invalid configuration vulnerabilities
- Others from the CVE database

Vendor Management Policy

The organization's overall security is highly dependent on the security of its contractual relationships with its IT suppliers and partners. This policy defines requirements for effective management and oversight of such suppliers and partners from an information security perspective. The policy prescribes minimum standards a vendor must meet from an information security standpoint, including security clauses, risk assessments, service level agreements, and incident management. Veranda Learning assesses vendors to determine if their IT security controls are adequate. Veranda Learning also ensures that vendors implement mechanisms to identify and remediate deficiencies or vulnerabilities on an ongoing basis to ensure the continued effectiveness of IT security controls.

- All supplier relationships are vetted by the Information Security Council (ISC). Where possible, a written contract shall exist between all parties involved, and Veranda Learning will hold an original signed by all parties, which will be held electronically.
- A detailed risk assessment is conducted for vendors by the Infosec team where enough information about controls and policies is not available.
- All vendors and third-party contractors are required to adhere to Veranda Learning's security policy.

Remote access and work from home

The objective is to secure remote work environments and prevent loss, damage, theft, or compromise of assets and interruption to the Company's operations. Accidental or intentional exposure of confidential data within a company's network by not following proper procedure to connect to it is a huge risk faced by information security teams today. Hackers and other bad actors frequently use vulnerabilities on personal devices and home networks to conduct massive hack attacks on the Company's network.

Veranda Learning -

- Establishes usage restrictions and implementation guidance for each allowed remote access method
- Monitors for unauthorized remote access to the system
- Authorizes remote access to the system before connection and
- Enforces requirements for remote connections to the system.

Physical security

Physical security is a must to protect employees, contractors, and other personnel within the office premises from unlawful and harmful acts by malicious external actors. Proper physical security also prevents bad actors from having easy access to data, information, and other organization-owned assets. This policy outlines all measures at Veranda Learning to avoid such incidents. For example,

- Physical badges or electronic key cards are required for employees to access physical office facilities.
- All visitors are required to log their visit in the office's visitor log.
- Access cards are not allowed to be shared or used by other than the person to who the card was issued.
- The clean desk policy guides employees to keep their desks and offices clean of confidential information.

Mapping with Industry Standards

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

Risk	Mapping to ISO 27001:2022
Loss of CIA (Confidentiality, Integrity, and Availability)	5.1 Policies for information security 5.12 Classification of information 5.13 Labelling of information 5.15 Access control 5.16 Identity management 5.17 Authentication information 5.18 Access rights 5.34 Privacy and protection of PII
Unauthorized Access	5.1 Policies for information security 5.2 Information security roles and responsibilities 5.15 Access control 5.16 Identity management 5.17 Authentication information 5.18 Access rights 5.34 Privacy and protection of PII C 5.1 Leadership and commitment C 5.2 policy C 5.3 Organizational roles and responsibility C 7.1 Resources

Risk	Mapping to ISO 27001:2022
	C 7.5 Documented information
System Failure/Data Loss	5.1 Policies for information security 5.5 Contact with authorities 5.9 Inventory of information and other associated assets 5.12 Classification of information 5.13 Labelling of information 5.15 Access control 5.18 Access rights 5.23 Information security for use of cloud services 5.24 Information security incident management planning and preparation 5.25 Assessment and decision on information security events 5.26 Response to information security incidents 5.27 Learning from information security incidents 8.13 Information backup 8.14 Redundancy of information processing facilities, 8.16 Monitoring activities C 9.3 Management review C 10.1 Continual improvement
Data Breach	5.24 Information security incident management planning and preparation 5.25 Assessment and decision on information security events 5.26 Response to information security incidents 5.27 Learning from information security incidents 5.37 Documented operating procedures 5.34 Privacy and protection of PII 8.12 Data leakage prevention C 6.2 Information security objectives and planning to achieve them C 10.1 Continual improvement

Enforcement

InfoSec team, along with senior management of Veranda Learning is responsible for the success of the Information Security program. The senior management is accountable for implementing, enforcing, and reviewing security controls.

All employees, contractors, and other individuals subject to the organization's information security policy must read and acknowledge all information security policies.

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.