ENCRYPTION 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 Acceptable Encryption Policy establishes requirements for the use of cryptographic controls and cryptographic keys to protect the confidentiality, integrity, authenticity, and nonrepudiation of information in **Veranda Learning**.

Scope

The Encryption Policy applies to following

- All computers/laptops
- Network systems
- Data at rest and data in motion
- Databases and data storage systems
- All system admins and applications

Background

Encryption policy defines the high-level objectives for the use of cryptography to encrypt data at rest and in motion. It is vital that the organization adopts a standard approach to cryptographic controls across all work centers in order to ensure end-to-end security, while also promoting interoperability. This document defines the specific algorithms approved for use, requirements for key management and protection, and requirements for using cryptography in cloud environments.

Policy

Encrypting data at rest

All critical and sensitive data in databases must be 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

Encryption of data in transit

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

Encryption Algorithm Requirements

- Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IPSec.
- Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.
- Ciphers in use must meet or exceed the set defined as AES-compatible" or "partially AES-compatible" according to the Ciphers in use must meet or exceed the group described as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2 or any superseding documents according to the date of implementation. The Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.
- Algorithms in use must meet the standards defined for use in NIST publication.

Cryptography key management and standard requirements

- Cryptographic keys must be generated and stored securely to prevent loss theft (see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2) or compromise.
- Key generation must be seeded from an industry-standard random number generator (RNG).
- Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman IKE or Elliptic curve Diffie-Hellman (ECDH).
- Public keys used to establish trust must be authenticated before use. Examples of authentication include transmission via cryptographically signed messages or manual verification of the public key hash.
- All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.
- All servers and applications using SSL or TLS must have the certificates signed by a known trusted provider.

Key Rotation

- All cryptography keys should be rotated as per established best practices of every six months.
- The rotation period shall also be based on the information management system and data for which the key is used.

Mapping to Industry Standards

This policy addresses the following risks related to Acceptable Encryption Policy and Information Security standards, frameworks:

Risk	Mapping to ISO 27001:2022
Loss of CIA (Confidentiality, Integrity, and Availability)	8.24 Use of cryptography 8.13 Information backup 8.11 Data masking
Information Leakage	8.24 Use of cryptography
Theft	8.24 Use of cryptography
Data Breach	8.24 Use of cryptography 8.26 Application security requirements
Legal and Regulatory non-compliance	8.24 Use of cryptography 5.31 Legal, statutory, regulatory and contractual requirements

Enforcement

Infosec team is responsible that all internal and vendor applications follow the best practices for encryption mentioned in the 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.