Encryption and Cryptographic Control Policy

collation.ai

263 Tresser Blvd Floor 9,
Stamford,
CT 06901
United States

CLASSIFICATION: INTERNAL

Document Management Information

Ver No.	Ver. date	Author	Reviewed By	Approved By	Changes
1.0	01.08.2023	CTO	CISO	CEO	Initial Version
1.0	31.01.2024	CTO	CISO	CEO	reviewed
1.1	29.04.2025	CTO	CISO	CEO	Corrections
1.2	03.09.2025	CTO	CISO	CEO	Corrections

Table of Contents

• Definitions and Acronyms

Definitions

Term	Explanation
Information Asset	Anything that has value to the Organization and is either a form of information itself or creates, stores, transmits or manages information.
Information Security	Preservation of Confidentiality, Integrity, and Availability; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved
Information Security Management System	The system designed, implemented and maintained for assuring a coherent framework of processes and systems; for effectively managing information accessibility, thus ensuring the confidentiality, integrity, and availability of information assets and minimizing information security risks.
Collation.ai Employee	The person hired to perform a job or service for Collation.ai, and one who is directly employed or hired on a contract basis
Customers	All the clients of the organization who avail services or products provided by the Collation.ai.
Vendors	All third parties which include, but is not limited to vendors, volunteers, contractors, consultants, temporaries, and others who have access to, support, administer, manage, or maintain Collation.ai's information or physical assets
External Storage Media	All storage devices like USB drives CDs, DVDs, camera phones, external hard disks, or any other device which has the ability to capture, storing or transporting data
Users (of the Information system of Collation.ai)	The meaning of Users in this policy refers to all employees of the organization, (permanent as well as temporary), third parties, contractors, vendors, consultants, volunteers, interns, etc., who use or deal with information assets or other assets of Collation.ai.
Authorized Persons	Are defined as people who have established a need and received the necessary authorization from Collation.ai.
ISF	Forum started to strategize, develop, practice, implement, guide, measure and continuously improve Information security posture at Collation.ai to effectively manage the threats and risks to Collation.ai is termed as Information Security Forum.

Acronyms

Acronym	Full Name
AR	Asset Register
ISMS	Information Security Management System
SIRT	Security Incident Response Team
IT	Information Technology
ISF	Information Security Forum
PDCA	Plan – Do – Check – Act (the Deming cycle)
CISO	Chief Information Security Officer
CTO	Chief Technology Officer

• Scope

This policy is applicable to all Employees, Contractors, and Vendors of Collation.ai and others who have the authorization to access or use Collation.ai's information processing facility, data, applications, etc.

• Policy Statement

Encryption must be applied wherever possible to the information stored or transmitted as appropriate for the information classification and business requirements.

• Purpose

The policy aims to

1. Improve the security and confidentiality of information, wherever possible.
2. Reduce the risk of unauthorized access, loss of and damage to information.

• Policy Sections and Clauses

5.1 Encryption Requirements

The decision on requirements of information encryption must be made considering the following criteria:

- Applicable legal requirements or storing and transmission of information.
- Risks in transmitting information internally and externally.
- Risk in storing information and access control.
- Proven, standard algorithms must be used as the basis for encryption technologies.

5.2 Encryption Key Management

- Encryption key management is in place to support the organization's use of cryptographic techniques.
- Appropriate care is taken to generate encryption keys.
- Keys length and encryption algorithms are decided considering applicable legal requirements and identified risks in Risk assessment.
- All encryption keys are loaded into either Azure vault (only if used to encrypt Azure Cloud resources) and the local copy is securely erased.
- All-access to encryption keys is only via the key management services ensuring all access is properly logged and recorded.
- No Collation.ai staff has access to encryption/decryption keys. Encryption as a service provided by vault is consumed to encrypt/decrypt files without providing physical access to the key basis role assumed by staff.
- Vault's root token is split amongst a minimum of 5 different individuals using Shamir's secret sharing algorithm and the original copy securely erased.

5.3 Approved Cryptographic Algorithms

- The recommended key size is 128 bits for symmetric keys.
- The wireless network of Collation.ai is encrypted by WPA2 encryption with the AES-128-bit encryption algorithm.
- For password hashing, SHA-1/ SHA-2 or equivalent is used.
- TLS 1.2 or above is used for protecting HTTPS resources in-transit. The following cipher suites are recommended for use:
  - ECDHE-ECDSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-ECDSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-ECDSA-CHACHA20-POLY1305
  - ECDHE-RSA-CHACHA20-POLY1305
  - DHE-RSA-AES128-GCM-SHA256
  - DHE-RSA-AES256-GCM-SHA384
- All web servers are HSTS (http strict transport security) enabled
- For encrypting data at rest, AES-256 or equivalent symmetric encryption standards are used.

• Enforcement

Necessary disciplinary action will be taken against any employee not following the policies and procedures laid down by the Collation.ai. Similarly, action will be taken against those employees encouraging/observing such activity and not reporting the same to the concerned authority. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as per Collation.ai HR policies.

• Special situations and exceptions

Collation.ai's top management, Singapore government, or any other regulatory body or bodies norms override Collation.ai's Encryption and Cryptographic Policy at a particular point in time

• ISO 27001:2013 References

- A.10.1 Cryptographic controls
- A.10.1.1 Policy on the use of cryptographic controls
- A.10.1.2 Key management

–