ACCESS CONTROL POLICY

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

CLASSIFICATION: INTERNAL

Attention: The information is intended for the private use of Collation.ai. By viewing this document, you agree to keep the contents in confidence and not copy, disclose, or distribute this without written request to and written confirmation from Collation.ai. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document is prohibited.

Document Management Information

Ver. No.	Ver. date	Author	Reviewed By	Approved By	Changes
1.0	01.08.2023	CTO	CISO	CEO	Initial Version
1.1	31.01.2024	CTO	CISO	CEO	Minor Edits
1.1	31.05.2025	CTO	CISO	CEO	Minor Edits

Table of Contents

1. 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	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 includes, 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 of capturing, storing or transporting data
Users (of 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
ISF	Information Security System
SIRT	Security Incident Response Team
IT	Information Technology
ISMF	Information Security Management Forum
PDCA	Plan – Do – Check – Act (the Deming cycle)
CISO	Chief Information Security Officer

2. Purpose

To support Collation.ai business functions and ensure information security, the company provides access to information assets to all the employees only on need basis. Inappropriate access would expose Collation.ai Information assets to risks leading to business loss. The purpose of this policy is to define access controls to information systems and other resources.

3. Scope

This policy covers Collation.ai's cloud environment (including development, staging, testing and production – both instances), applications, systems, end-user devices, equipment and data.

4. Policy Statement

This policy is intended to protect the security, integrity of Collation.ai's information processing facility through access control.

5. General Use and Ownership

5.1 Use Boundaries of Access Control

Access Control is to be practiced on the following but not limited to:

- Facilities of the company
- All the desktops and end user devices
- Mobile devices (Laptops, Desktops and Mobile phones)
- Network Devices
- Applications
- Databases

5.2 General Policy Clauses

- All employees will be provided the access to information they need to have to carry out their responsibilities in an effective and efficient manner.
- Access to information, facility, functionality, assets, and resources of the company will be limited to authorized persons after appropriate approvals.
- Access is given through the establishment of a unique account. Users are expected to become familiar with and abide by the company's policies and procedures for appropriate and acceptable usage of the networks, systems and other resources of the company.
- Every user must maintain the confidentiality of information assets even if technical security mechanisms fail or are absent.
- Users are obligated to report instances of non-compliance.

5.3 Access Control (For Employees)

- Access Control should be deployed. For physical security Biometrics must be used and for email and system access, IT should configure after intimation from HR. The critical system / administrative access is provided on a need to know basis after appropriate approvals.
- Collation.ai employees are currently connecting to AZURE (Microsoft Azure Cloud Service) on a need basis using cryptographic key exchange methods (Public and Private key).
- In addition to the above step, devs can only connect to required infrastructure via the bastion method.

- Access to any systems and other network devices and areas are to be strictly adhered to by a role based access control policy and should be limited to authorized personnel only.
- Access to the AZURE network and its services are currently restricted only to Administrators of AZURE.
- All sensitive information shall be protected via logical access controls to ensure that unauthorized access, disclosure, modification, deletion of information is prevented.
- All users shall have their identity verified with a unique login id and a secret password issued by the IT Team prior to being permitted to use company resources. 2-factor authentication has been enabled on all systems.
- The authority to grant access to company information shall be provided only by the owner of the information or their delegate.
- Access to systems software shall be restricted to authorized users only.

5.4 Operating System Access Control

- System utilities should be restricted to minimum. Only required system administrators should have access to system utilities.
- Access to program source code shall be restricted and provided only on a need-to-know basis.
- Access rights of the users who have left the organization or moved to another department shall be revoked/adjusted.

5.5 User Access Management

Information Access Restriction:

- Access to applications by default should be ‘denying all’.
- Upon intimation from HR, IT should configure email and system and through biometric physical access should be provided to the premises.
- Access rights of the users who have left the organization should be removed or blocked.
- Access to application system functions shall be restricted in accordance with the access control procedure.
- Any application data shall be accessible only through application. Direct network access to the application data should not be allowed.
- The user access shall be reviewed quarterly.

5.6 User Access Provisioning & Revocation

- Authorization from the owner of the information system for the use of the information system should be obtained.
- The IT and Admin team should ensure the restriction and availability of information in regard to his/her roles and duties only after prior approvals are received.
- Any special rights or information required should have a special approval required apart from the default information applicable to his/her roles.
- The IT team should maintain a record of the access rights and services that are being provided at user level.

- The IT team shall remove/ block user IDs on receipt of email from HR on separation of employees.
- Any access to information or rights should not be activated without email prior authorization and approval.
- The IT team should ensure the blocking or removal of any information to any user if found being misused or modify the access as per role modification upon a proper mail communication exchange.

5.7 Management of Privilege Access Rights

- Collation.ai IT teams must ensure the privilege information and rights should be role specific and not allowed to every individual. In case of any special requirement it should have a mail approval.
- A proper authorization process and it's tracker should be maintained.
- Granting of the privilege access rights should not be provided until the authorization process is completed and approved.
- Any change in access to these rights should undergo a proper change management process.
- Periodic monitoring of these rights should be done to assess the level of their execution by the user.
- Collation.ai IT team should maintain and record as to whom the rights are being given, what is the purpose and the tenure of the rights. Also, this should be carried out over an evidence-based communication medium.
- Users of Collation.ai need to maintain strong confidentiality while accessing these rights and the IT team must enforce a strong password policy.

5.8 Management of Secret Authentication Information of Users.

- Collation.ai IT team should ensure the authenticated information is being accessed to the user only after a proper mail communication is established seeking for access.
- User's should provide receipt of acknowledgement for receiving the authenticated information via electronic or paper document.
- User's should be made to sign an agreement with the usage of any secret authentication information for its sole discretionary use only and any misuse / violation to that should hold disciplinary actions.
- Collation.ai users should be provided with a temporary authentication mechanism which needs to be forcefully changed after their first login.
- Temporary secret authentication information should be given to the users in a secure manner.
- Temporary secret authentication information should be unique to an individual.
- Secret authentication information should be kept confidential and one should avoid keeping a record of the secret authentication information.

5.9 Review of User Access Rights

- The Collation.ai IT team should review the access rights at regular intervals for any addition/deletion/modification of the user's roles and his duties.
- The Collation.ai IT team should also keep a track of any privilege rights that are being provided to users and its authorization should be reviewed frequently.
- User’s actions using his/her role specific and privilege rights should be kept under a logging monitor with periodic checks.
- Collation.ai IT team must ensure that unauthorized privilege rights are not provided to any user apart from the communicated individual and strong reviewing for the same shall be done frequently.

5.10 Removal or Adjustment of Access Rights.

- Collation.ai’s IT team must revoke every access to information or rights of an employee departing from the organization.
- Any assets or information of value as to be surrendered to the Admin team as per the checklist of assets and rights provided to him at the time of hiring and during the employment.
- Any special rights or privileges, access card numbers, RSA tokens, OTP devices will be revoked, modified or suspended by the IT team post mail exchanges and approvals.
- Collation.ai IT and admin team should cover all the aspects of documenting and reviewing of the information such as the type of rights the user exercised, the last date of his/her employment exercising those rights, disabling of any rights post his/her reliving, changing of password on the last day and surrender of any critical/authenticated information to the SPOC in case of Vendor and to the HR in case of employee.

5.11 Use of Secret Authentication Information

- Collation.ai’s secret information such as password and authentications should be held confidentially with the user and should strictly ensure to avoid leakage.
- Authenticating mechanisms such OTP tokens and devices should not be held in use with anybody other than self.
- Temporary secret authentication information should be given to the users in a secure manner.
- Temporary secret authentication information should be unique to an individual.
- Passwords should not be an easy guess, dictionary word or personal information and should be having a strong combination of letters, special characters and numbers.
- Passwords for new users should have a force change on the first login approach.
- Secret authentication information should be kept confidential and one should avoid keeping a record of the secret authentication information or passwords in any hard / soft copy.
- The IT team should enforce a password lock out policy after 3 attempts.
- Users must ensure that the provided secret authentication is not shared with any individual authority nor shared between business and non-business reasons.

5.12 Use of privileged utility programs

- The IT team of Collation.ai should whitelist a list of utility programs that are allowed for users to use.
- The allowed utility programs should not hamper the day to day business applications and softwares and should have controlled access as to which features are to be allowed.
- Downloading & logging of utility programs should be restricted & monitored by means of physical, logical and virtual controls.
- Authorization levels & it’s duration should be listed and tracked in respect to the access of the utility programs.
- The IT team should keep a record of all the utility programs that are currently being used in the organization, its access rights, its tenure and its purpose.
- Any utility programs which are no longer required should be immediately informed to the IT team for its removal from the business.
- The IT team must ensure the access of utility programs to any role specific user should be limited and granted with proper approval if required.

6. 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 an 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.

7. Special situations and exceptions

Collation.ai’s top management, USA government, or any other regulatory body or bodies norms overrides Collation.ai’s Secure Development Policy at a particular point in time.

8. ISO 27001:2013 References

- Annexure A.9.1 – “Business requirements of access control”
- Annexure A.9.2 – “User access management”
- Annexure A.9.3 – “User responsibilities”
- Annexure A.9.4 – “System and application access control”