Security Incident Response 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
1.1	31.01.2024	CTO	CISO	CEO	Minor edit and reviewed
1.2	30.04.2024	CTO	CISO	CEO	Corrections

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 was 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	A 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

2. Scope

This policy governs Collation.ai's general response, documentation, and reporting of incidents affecting Collation.ai's assets, such as theft, intrusion, misuse of data, other activities contrary to the Collation.ai's Acceptable Use Policy, denial of service, corruption of software, computer and electronic communication-based violations, and other incidents reported to Incident response team of Collation.ai by Collation.ai employees, vendors, business entities and related stakeholders. This policy does not include damage to personal assets owned by an employee unless those assets contribute to the Incident defined by the parameters identified below.

3. Policy Statement

Collation.ai's Security Incident Response Policy mandates that requisite action is taken for identifying, tracking, responding, reporting, and recording security incidents.

4. Purpose

The purpose of this policy is to ensure proactive response and proper remediation to the security incidents to protect Collation.ai's assets integrity, availability, and confidentiality, to prevent loss of service. The document also aims to aid Collation.ai's employees for quicker remediation, information gathering and reporting of security incidents or events.

5. Policy Sections and Clauses

5.1 Identifying Security Incident

Subscribed Tools:

- Microsoft Azure Cloud Infrastructure will be monitored in real-time by Azure tools which we have subscribed to, namely – Microsoft Defender, Azure Web Application Firewall, Microsoft Purview, etc
- The above tools enable Collation.ai to monitor for possible security events/monitoring related to security, benchmark, Access & privileges, etc.

Manual:

- Any employee of Collation.ai may refer to a security event, activity or concern to the SIRT (Security Incident Response Team) via SD ticket.
- The SIRT can also identify an Incident through its proactive monitoring of information system activities.
- Once identified, SIRT will use standard internal procedures to log and track Incidents and, working with others as appropriate, take steps to investigate, escalate, remediate, refer to others or otherwise address as outlined in the remainder of this policy.

5.2 Types of incidents

- A security incident is a term related to exceptional situations or a situation that compromises Confidentiality, Integrity or Availability of Information and Information Systems. Also, violations of the existing security policies and

procedures of the Collation.ai shall be considered as an incident. A few examples of security incidents are as below.

- Unauthorized access to the secured area.
- Unauthorized modification or deletion of data.
- Hacking attempts from the external networks.
- Account lockouts because of invalid password entries.
- Virus infection to any desktop or server.

- Security weakness is a vulnerability in an information system, which could be exploited to compromise the Confidentiality, Integrity or Availability of the system. The following are examples of security weaknesses.
  - Malfunctioning of the access door to a secured area.
  - Access rights are given to those who do not perform their duties.
  - Virus definitions are not updated.
  - The latest service packs are not installed on desktops.
  - Improperly configured firewall rules.
- Software malfunction is any abnormal / deviation in the functioning of a software application. Examples of such incidents are
  - The inappropriate output from an application.
  - Displaying unexpected errors.
  - Corruption of data files.
- Non-IT Security Incidents
  - Theft
  - Human Errors
  - Natural Calamity or Disaster
  - Non-Compliance with ISMS Policies and Procedures

5.3 Reporting Incidents

- When any of the above incidents or other events occur, which breach the security policy of Collation.ai or may cause security weakness, should be reported immediately to the Head of department/members of SIRT / CISO / CTO.
- An incident reporter should provide as much detail as possible about the incident.

5.4 Incident Response Procedure

- When any of the above incidents are reported, the investigation/response should be started immediately or within 4 hours.
- All possible evidence should be collected and stored securely. Such evidence should be used for further investigating the incident and kept securely to produce in the court of law if required.
- Quick action should be taken to restore the system affected by the incident and normal operation should be restored.
- If it is a computer-related incident, the affected computer should be immediately removed/isolated from the network and should not be turned off until all required logs and other evidence are copied from the system.
- All affected systems should be monitored on a daily basis at least for a week and then twice a week for one month after the operations are normalized.
- During an Incident Investigation, information is shared on a strictly "NEED to KNOW" basis. Even after an incident is closed, participants may be advised to keep certain aspects of the investigation confidential, especially if Legal Action is being pursued.

- During an incident, nothing shall be created, modified or destroyed unless explicitly approved by the CTO.
- Incidents remain open until such time as the SIRT declares the issues to be resolved and the incident closed.
- An incident report should be prepared to specify all details about the incident, investigations carried out and corrective actions are taken.
- Where it is a feasible Incident reporter should be informed about the results of the incident handling process.
- ISF should review critical incidents in the ISF meeting.

5.5 Establishment of SIRT

- SIRT is established with 4 permanent members - Devops Lead, Engine Lead, Visualiser Lead, CTO and invited members.
- Invited members are invited to be consulted on a case to case basis as subject matter experts.
- CTO will be chosen to act as a point of contact in case of responding or coordinating in case of Incidents.
- SIRT will be responsible for Incident coordination and remediation of computer electronic communication -based resources affected by these incidents.

5.6 Documentation and Communication of Incident

- SIRT will ensure that Incidents are appropriately logged and archived with proofs or evidence if any.
- Wherever possible, documentation of such Incidents will cross-reference other event databases within Collation.ai, such as network monitoring systems, and reports if any.
- Any Incidents involving systems that are tracked will be cross-referenced in that database with the incident tracking log.
- SIRT head will be responsible for communicating the Incident to appropriate personnel and maintaining contact, for the purpose of update and instruction, for the duration of the Incident.
- SIRT head will be responsible for communicating the incident to appropriate client contacts as per the protocols laid out for communication and severity levels decided.

5.7 Learning from Incidents

- ISF should analyze all incidents and identify recurring and high impact incidents and malfunctions. Document and communicate the same to SIRT.
- The requirement of enhanced or additional controls should be identified and implemented.
- All security incidents should be used in future security training so as to train users about such incidents and avoid such incidents in the future.

5.8 Plans and Procedures

- SIRT will maintain standard procedures and plan for the response and investigation of each Incident, as well as securing the custody of any evidence obtained in the investigation.

- The application of these procedures will be governed by the classification matrix described in Section 6.7 in the Security Incident Procedure.
- The procedures will specify the location and method of custody for each incident if custody of evidence is required.

5.9 Incident awareness and training

- Collation.ai personnel are required to report Incidents to the Collation.ai's SIRT.
- The security awareness and training that is required will cover specific procedures for reporting security Incidents.

5.10 Help of Government officials

A response plan or remediation defined by this policy may be preempted as required or
at Collation.ai's discretion by the intervention of Government officials.

5.11 Incident Prevention

Wherever possible, Collation.ai's SIRT will undertake to prevent Incidents by monitoring and
scanning its own network for anomalies and developing clear protection procedures for
the configuration of its IT resources.

5.12 Policy revisions and modifications

This policy and its procedures will be reviewed at least annually to adjust processes, identify new risks and their remediation.

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 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 override Collation.ai's Incident Response Policy at a particular point in time.

8. Procedures

Collation.ai maintains internal procedures for Incident logging, tracking, and reporting, for evidence custody and related practices.

- Security Incident and Response Procedure

9. ISO 27001:2013 References

- A.16.1.1 Responsibilities and procedures
- A.16.1.2 Reporting information security events
- A.16.1.3 Reporting information security weaknesses
- A.16.1.4 Assessment and decision of information security events
- A.16.1.5 Response to information security incidents
- A.16.1.6 Learning from information security incidents
- A.16.1.7 Collection of evidence