Security Policy

I. Purpose

This Security Policy sets forth the information security program and policies that Collibra will meet and maintain in order to protect Customer Data from unauthorized use, access or disclosure, during the term of Customer's Agreement with Collibra. Collibra may modify the terms of this Security Policy from time to time, provided that such modified terms shall be no less protective of Customer Data as those currently in effect.

The terms of this Security Policy are incorporated by reference in the agreement between Collibra and Customer pursuant to which Collibra provides Customer with access to Collibra's cloud products and services ("**Agreement**"), and capitalized terms not defined herein shall have the meanings ascribed to them in the Agreement.

II. Information Security Program

Collibra implements, and maintains an approved information security program designed to protect and secure Customer Data from unauthorized access, disclosure, or use. Collibra's information security program is documented and updated based on changes in applicable legal and regulatory requirements related to privacy and data security practices, and industry standards applicable to Collibra. The program is based on industry standards including those from ISO, NIST, and the Cloud Security Alliance. Collibra's ability to meet and maintain the security standards and obligations in this Security Policy is subject to Customer accepting and promptly implementing all releases, upgrades, patches, fixes and any other corrective actions and procedures provided by Collibra.

III. Standards

Collibra incorporates commercially reasonable and appropriate administrative, technical, and physical safeguards to protect the security, confidentiality, and availability of Customer Data. Collibra will, at a minimum, adhere to applicable information security practices as identified in International Organization for Standardization 27001 (ISO/IEC 27001) (or a substantially equivalent or replacement standard).

IV. Independent Assessments

Collibra will, at a minimum, undergo an audit of Collibra's information technology general controls with respect to the Service (including, but not limited to information security, confidentiality, and availability controls), performed by an independent third-party audit firm based on a recognized audit standard (SOC 2 Type II report or equivalent). Upon Customer's written request, Collibra will make available to Customer for review, its SOC 2 Type II report after the report's publication by the independent audit firm. Customer agrees to treat such audit reports as Confidential Information of Collibra. Collibra maintains certification to ISO 27001 and will make the certificate of registration available to Customer upon written request. Collibra undergoes penetration testing from independent third parties on an annual basis, including at minimum, of its network and applications in connection with the Service.

V. Information Security Policies

Collibra implements, maintains, and adheres to its internal information security and privacy policies that address the safeguards and the roles and responsibilities of Collibra's employees, who have direct or indirect access to Customer Data in connection with the Service. Collibra's information security policies are regularly documented, and reviewed and approved by management at least annually.

VI. Information Security Infrastructure

a. Access Controls

Collibra will ensure that appropriate access controls (physical, technical, and administrative) are in place and will maintain such access controls in accordance with Collibra's policies and procedures. Access to the Service by Collibra employees and contractors is protected by authentication and authorization mechanisms, and only accessible to those whose role requires such access. Access privileges are based on job requirements using the principle of least privilege access and are revoked upon termination of employment or transfer. Access entitlements are reviewed by management regularly.

b. Data Encryption

Collibra implements industry standard encryption for all encryption within the Service. At a minimum, Collibra will use the Advanced Encryption Standard (AES) algorithm with a minimum key size of 256 bits for at-rest encryption and Transport Layer Security (TLS) 1.2 or greater for in-transit encryption.

c. Cloud Security

Collibra has cloud security protections in place that are standard with a Software-as-a-Service organization. Cloud native tools such as virtual private clouds, security groups (which function like a firewall), endpoint detection and protection, and infrastructure as code may be implemented to ensure the Collibra cloud network has appropriate protections in place.

d. Vulnerability Management

Collibra uses commercially reasonable efforts to ensure that Collibra's operating systems and applications associated with its organization, the Service, and those that host Customer Data, are subject to vulnerability management assessment and controls.

e. Host Security

1. Systems and applications are hardened in accordance with Center for Internet Security (CIS) Benchmarks to mitigate the impact of security vulnerabilities. Industry standard processes and tools are used to automatically implement secure baselines for relevant systems and to detect any deviations from these established baselines.
2. Host systems and Collibra endpoints are deployed with (i) anti-malware or equivalent controls, that are updated at regular intervals, and (ii) host-based intrusion detection controls.

f. Data Management

Collibra will destroy, delete, or otherwise make irretrievable Customer Data upon the disposal or repurposing of storage media containing Customer Data. The Service logically separates Customer Data of each Collibra customer.

g. Monitoring

Collibra implements monitoring in its cloud environment for the Service to ensure continuous security monitoring of events. Relevant logs are centrally collected, secured to prevent tampering, monitored for evidence of any security incident, and stored up to a year to support analysis and investigation as needed.

h. Human Resources Security

1. *Background checks*

   Upon commencement of the employment process for all prospective candidates, Collibra undertakes appropriate background checks and screenings. Subject to per-country and jurisdiction restrictions, these include criminal, employment, financial, citizen status, and government watch lists.

2. *Non-disclosure and policy agreements*

   As a condition of accepting employment, Collibra employees are required to sign a non-disclosure agreement and review and confirm their understanding of relevant Collibra policies. Collibra employees are contractually required to observe adherence to Collibra policies as a condition of continued employment.

3. *Security Awareness Training*

   Without exception, all Collibra employees are required to undergo annual general security awareness training. Completion of mandatory security training is monitored.

Notwithstanding the foregoing, Customer understands and acknowledges that Customer will be solely responsible for implementing and maintaining access and security controls on its own systems and users of Collibra services and products.

VII. Secure Software Development Life Cycle

Collibra's Secure Software Development Life Cycle (SSDLC) methodology governs the development, configuration, maintenance, modification and management of infrastructure and software components for the Service. Collibra's secure software development policies and procedures are aligned with industry standards such as the OWASP Top Ten (or a substantially equivalent standard). Vulnerabilities and patches are remediated in accordance with Collibra's vulnerability management standards that follow industry leading practices.

VIII. Security Incident Management

a. Notice

Collibra will respond promptly to, contain and remediate Security Incidents (as defined below). Collibra shall notify Customer of a confirmed Security Incident promptly and in accordance with applicable law. Collibra will cooperate with Customer's reasonable requests for information regarding any such Security Incident, and Collibra will provide regular updates on the Security Incident and the investigative and corrective actions taken. "Security Incident" means unauthorized access to, acquisition, or use of unencrypted Customer Data that has the potential to cause identity theft or financial harm to Customer's employees or participants.

b. Remediation

In the event that Collibra knows or has reason to know of a Security Incident, Collibra will, at its own expense: (1) investigate the Security Incident; (2) provide Customer with a remediation plan to address and mitigate the Security Incident, and reasonably prevent any further such incidents; (3) remediate the effects of the Security Incident in accordance with such remediation plan; and (4) reasonably cooperate with Customer and any law enforcement or regulatory official investigating such Security Incident.

IX. Contingency Plan

Collibra implements and maintains a business continuity plan to minimize the impact to its provision and support of the Service from an extended business disruption. Additionally, Collibra (i) maintains a technical disaster recovery plan; (ii) provides for appropriate backup technology that will permit transition of the Service in the event of an incident; and (iii) tests the disaster recovery plan regularly.

X. Certifications, Assessments and Standards

To continue to provide transparency in its secure cloud products and services, upon Customer's written request, Collibra will provide an executive summary of independent third-party penetration test reports. Collibra maintains a list of externally validated certifications, assessments and standards, which can be found at the Collibra Trust Center.