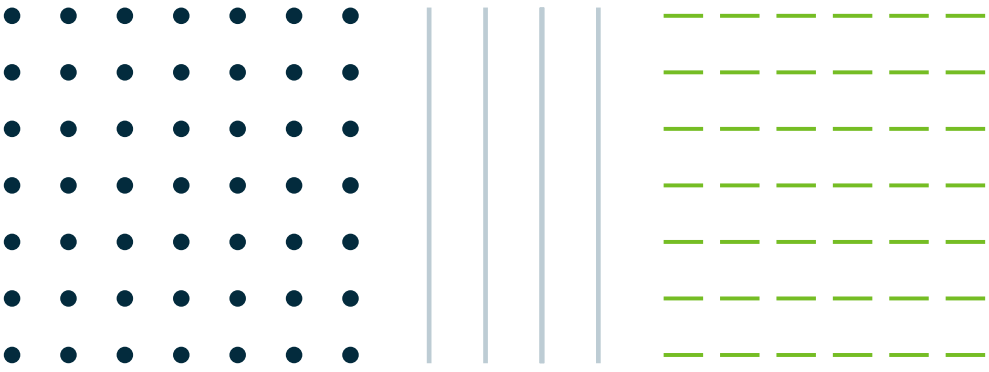
Collibra

Security and compliance overview

Collibra is committed to the security of our software and infrastructure. Security plays a vital role in our organizational structure, software delivery, training programs, and hiring processes. It is also a cornerstone of account controls, audits, and the services we provide to customers.



Security culture

Employee background checks

Collibra screens all employees prior to hiring through third party experts. Background screening includes criminal, education, employment, financial, and where applicable, drug screening.

Security training for all employees

All employees have access to security training and job specific security training by role.

Collaboration with the security research community

We participate in the Cloud Security Alliance Security Trust Assurance and Risk (STAR) program which works to incorporate security standards in Cloud Security. Companies who use STAR indicate best practices and validate the security posture of their cloud offerings.

Operational security

Operational practices

As a global organization, Collibra must comply with various international privacy regulations. One of the ways we comply with international privacy regulations is by maintaining a comprehensive, written information security program that contains technical and organizational safeguards designed to prevent unauthorized access to and use or disclosure of customers' data.

Vulnerability management

We scan our code for vulnerabilities and complete a peer code review before code is committed.

Incident management

We have a formal security incident response plan in place. This involves all aspects of Collibra's team including CloudOps, Development, Support, Legal, Finance, and Executives. Customers are asked to direct all security requests to Support.

Security at the core of technology

Audits

We exclusively audit against the ISO 27001 standard. We have also implemented over 200 compensating controls that map to leading national and international security standards: including FedRAMP Security Controls, PCI DSS, and AICPA Trust Service Criteria (SOC 2SM Report).

Security

We create and maintain a rigorous control security framework built around regulatory, legal, and statutory requirements as well as industry best practices.

Certification

ISO 27001 is a globally recognized, standards-based approach to security that outlines requirements for an organization's information security management system. We have achieved and maintain certification against ISO 27001. Certification is achieved following an independent assessment of conformity to the ISO standard. ISO recertification occurs every three years, and to maintain certification, we undergo surveillance audits. This ISO certification affirms our commitment to privacy and security and demonstrates that our controls are operating effectively. The ISO certificates are available for customer review.

Collibra has been authorized as a Moderate Impact Cloud Service Provider under the Federal Risk and Authorization Management Program (FedRAMP). By achieving the FedRAMP Moderate certification, Collibra is now officially recognized by the US Government for meeting some of the most stringent cloud security requirements in government today.

Collibra is compliant with the Health Insurance Portability and Accountability Act (HIPAA). Collibra's HIPAA compliance intentions are established through the design and implementation of administrative, technical, and physical controls throughout the infrastructure and supporting processes.

Cloud architecture

Our cloud architecture is designed to segregate and restrict data access based on the customer and on the customer's business need. The architecture of the cloud environment used by Collibra provides logical data separation and role-based access privileges, all controlled on a customer-specific level. Production and testing environments are separated.

Identity and access management

We control and restrict access to our software to ensure appropriate identity, entitlement, and access management. We support industry identity federation standards such as SAML and integration with customers' single sign-on (SSO) solutions.

Encryption

Collibra implements encryption for data at rest using the Advanced Encryption Standard (AES) algorithm with a key size of 256 bits and Transport Layer Security (TLS) for data in transit.

Network

We implement proactive security procedures, such as perimeter defense and network intrusion prevention systems. Vulnerability assessments and penetration testing of the Collibra network infrastructure are also evaluated and conducted on a regular basis by both internal Collibra resources and trusted third-party security professionals.

Reliability

Backups

The cloud architecture used by Collibra includes independent hardware restore and recovery.

Business continuity

We have established and maintain disaster recovery and business continuity plans so that the Collibra software is reliable and recoverable. We test for resiliency across our cloud provider and implement and test backup and restore procedures.

Privacy and GDPR

The General Data Protection Regulation (GDPR), a European Union (EU) regulation, took effect in all EU member states on May 25, 2018, and simplifies and harmonizes current data protection laws in all EU member states. The GDPR applies to

companies in the EU as well as all companies that process or store the personal data of EU citizens, regardless of their location. Collibra is a data processor as defined under the GDPR. We continuously evaluate GDPR requirements and have implemented numerous privacy and security practices. We understand the importance of GDPR for our global customers and continue to monitor guidance from supervisory authorities and industry best practices.

Ongoing commitment to security and privacy

We remain committed to delivering a secure product and platform and privacy practices that ensure trust and control of customer data. This strategy includes evaluating industry standards, assessments and authorizations, and targeting compliance with those that ensure a rigorous, flexible, and scalable security and privacy strategy.

The security of customers is a primary concern of Collibra infrastructure, product, and personnel operations. Our connection with the security research community enables us to address vulnerabilities quickly or prevent them entirely.

We believe that our investment in security and making security the core of our setup will help our customers to securely store and access their metadata between cloud and on-premises or between cloud instances.

More information

For additional detail, please see the Cloud Security Alliance Star Registry for Collibra cloudsecurityalliance.org/star/registry/collibra or a copy of our Standardized Information Gathering (SIG) is available upon request.

For additional questions, contact us at:

United States
+1 646 893 3042

United Kingdom
+44 203 695 6965

All other locations
+32 2 894 79 60

By email
info@collibra.com