Security Overview

Version: 2.0
Last Updated: 1st September 2026
Classification: Public

Security Overview

This document describes the information security program supporting the Concord platform — the administrative, technical, and organizational safeguards protecting customer information and the secure delivery of the Services. Read together with the Trust Center Guide, Information Security Schedule, Data Processing Addendum, and applicable contractual documents.

Security Governance

Concord maintains a documented information security program covering security responsibilities, risk management, regulatory compliance support, and continuous improvement of controls. Security risks are periodically reviewed and prioritized by business impact and exposure.

Secure Software Development

Security is incorporated throughout the development lifecycle: secure design review, secure coding standards, peer code review, automated code quality and dependency-vulnerability scanning, secrets detection, Infrastructure-as-Code review, security testing before production deployment, and controlled production releases. See the Secure SDLC & Vulnerability Management Overview.

Identity and Access Management

Access to production systems follows least-privilege principles: role-based access control, multi-factor authentication for privileged access, periodic access review, timely provisioning/deprovisioning, and administrative access controls. See the IAM Overview.

Encryption

Data in transit — all traffic between users, applications, and platform services is protected using TLS 1.2 or later.

Data at rest — customer information is encrypted at rest by the underlying cloud infrastructure. Sensitive fields, such as MFA secrets, carry an additional application-layer encryption pass beyond the platform default. Encryption keys are managed using cloud key management services with access controls appropriate to their sensitivity.

Infrastructure Security

Concord runs on Google Cloud Platform with network segmentation, firewalled and private networking, managed secrets storage, infrastructure monitoring, and secure configuration management. Compute is containerized and centrally deployed rather than managed per-instance, which keeps configuration consistent across the fleet.

Vulnerability Management

Concord identifies, assesses, prioritizes, and remediates vulnerabilities through automated dependency and infrastructure scanning, security advisory monitoring, and risk-based prioritization, with critical findings receiving prioritized attention.

Logging and Monitoring

Authentication events, administrative actions, infrastructure changes, application events, API activity, and availability are monitored for operational visibility and incident detection. Application errors are tracked with cloud-native error reporting tied to the specific code version that produced them, rather than through a separate third-party error-tracking

subprocessor. Audit logs affecting customer-visible governance activity are append-only, enforced at the database level rather than by application convention.

Incident Response

Concord maintains documented incident response procedures covering detection, impact assessment, containment, root-cause remediation, service recovery, customer communication where appropriate, and post-incident review. Where contractually required, customers are notified of confirmed security incidents without undue delay.

Business Continuity and Disaster Recovery

Concord maintains backup and disaster recovery procedures designed to support service resilience. See the BCDR Summary for detail, and the applicable Service Level Agreement for specific recovery commitments.

Vendor Risk Management

Third-party providers supporting service delivery are evaluated for security and privacy posture before use and subject to contractual security obligations and ongoing monitoring. See section subprocessors of privacy data protection overview.

Security Testing

Security validation includes automated application security testing, dependency scanning, infrastructure and configuration review, and vulnerability assessment. Penetration testing, where performed, may be conducted internally or by qualified third-party specialists; detailed reports are not publicly distributed but may be made available to customers under confidentiality arrangements.

Physical Security

Concord's production infrastructure is hosted on Google Cloud Platform, primarily in the Canada (Toronto, northamerica-northeast2) region. Physical security — facility access control, video surveillance, environmental monitoring, redundant power, and fire suppression — is managed by Google as the underlying cloud provider.

Shared Responsibility

Concord is responsible for: platform security, infrastructure management, secure software development, service monitoring, incident response, platform availability, and encryption.

Customers are responsible for: managing user accounts and access permissions, protecting user credentials, endpoint security, customer-managed integrations, and governance of their own AI workflows and data.

Reporting Security Concerns

Customers who identify a potential security concern should report it promptly through their designated Customer Success or support contact. Reports are investigated under our documented incident response procedures.

Additional Information

Available on request, subject to applicable confidentiality obligations: Information Security Schedule, Data Processing Addendum, architecture documentation, AI governance documentation, subprocessor information, and Service Level Agreement.
