Customer Trust Center Guide

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

Customer Trust Center

Welcome

Welcome to the Concord Customer Trust Center.

Trust is fundamental to every customer relationship. Organizations entrust Concord with information relating to their business operations, governance activities, compliance programs, and artificial intelligence initiatives. Protecting that information takes more than technology — it takes a comprehensive approach to security, privacy, operational resilience, and responsible AI governance.

This Trust Center provides an overview of the safeguards, governance practices, and operational controls that support the Concord platform, to help customers evaluate our security posture, privacy practices, and AI governance framework during procurement, vendor risk assessments, and ongoing due diligence.

Additional supporting documentation is available on request, subject to applicable confidentiality obligations.

About Concord

Concord is an enterprise SaaS platform that helps organizations govern AI agents through their software delivery lifecycle, with confidence. The platform helps organizations:

- Govern AI agents throughout their CI/CD lifecycle
- Manage AI governance and compliance obligations
- Maintain AI inventories and risk registers
- Automate governance workflows

- Monitor AI-related risks and controls
- Produce audit-ready evidence for internal and external stakeholders
- Support compliance with evolving regulatory and organizational requirements

Concord is designed for regulated industries and organizations that require strong governance, transparency, and accountability for AI-enabled business operations.

Our Trust Principles

Security by Design — security safeguards are integrated into platform design, development, testing, deployment, and operations, not added after the fact.

Privacy by Design — we collect and process only the information reasonably necessary to provide the Services and support our customers.

Responsible AI — AI should enhance human decision-making, not replace it. Our AI capabilities are designed to support transparency, accountability, human oversight, and responsible governance throughout the AI lifecycle.

Transparency — we aim to communicate clearly about how customer information is processed, how AI capabilities operate, how security controls are implemented, and how operational incidents are managed.

Continuous Improvement — security, privacy, and AI governance are ongoing commitments; we continually review and enhance our controls, processes, and platform capabilities.

Security Program

Concord maintains an information security program covering identity and access management, encryption, secure software development, vulnerability management,

infrastructure security, logging and monitoring, incident response, business continuity, disaster recovery, and vendor risk management. See the Security Overview for detail.

Privacy and Data Protection

Concord processes customer information in accordance with applicable privacy and data protection laws and contractual commitments, including a Data Processing Addendum, data minimization, retention and deletion procedures, cross-border transfer controls, subprocessor governance, and support for customer data-subject rights. See the Privacy & Data Protection Overview.

Responsible AI Governance

Responsible AI is central to the Concord platform. Our AI governance program supports human oversight, transparency, explainability, accountability, AI risk management, governance workflows, AI inventory management, regulatory readiness, and ongoing monitoring. Concord does not knowingly use identifiable customer prompts or customer data to train publicly available foundation AI models without customer authorization. See the AI Governance & Responsible AI Overview.

Platform Reliability

Concord is designed with operational resilience in mind — business continuity planning, disaster recovery procedures, backup management, incident response, operational monitoring, and change management. Service commitments are described in the applicable Service Level Agreement. See the BCDR Summary.

Compliance Alignment

Concord designs its security, privacy, and AI governance practices with reference to widely recognized industry frameworks, including ISO/IEC 27001, the NIST Cybersecurity Framework, OWASP, PIPEDA, GDPR, and the NIST AI Risk Management Framework. Unless expressly stated, references to these frameworks indicate alignment objectives and control mappings — not claims of certification or formal regulatory approval. See Compliance Mapping.

Shared Responsibility

Security is a shared responsibility. Concord is responsible for securing the platform; customers remain responsible for the appropriate use of the Services, including user administration, identity management, endpoint security, and governance of their own data and AI-enabled business processes.

Customer Due Diligence

Concord supports reasonable customer due diligence, including security questionnaire responses, vendor risk assessment documentation, subprocessor information, a Data Processing Addendum, security architecture information, and AI governance documentation. Some information may require an NDA or other confidentiality arrangement.

Contact Us

Customers with questions regarding security, privacy, compliance, or responsible AI should contact their designated Customer Success representative, or the contact information provided in their Order Form or Master Services Agreement.

Document Maintenance

This document is reviewed periodically and updated to reflect improvements to our security, privacy, operational, or AI governance programs.