

RevWorks Platform Security Statement

Updated May 2026

- Overview..... 1
- Architecture..... 1
- Access Control 2
- AI Security 2
- Data Handling 5
- Operational Security 6
- Compliance 6
- Salesforce ISV Partnership 7
- Frequently Asked Questions 7
- Contact 10

Overview

This document provides a comprehensive overview of the security architecture, data handling practices, access controls, AI security model, and compliance posture of Akoonu RevWorks — a forecasting and pipeline intelligence platform built natively inside Salesforce.

Akoonu is designed for enterprise revenue teams that require complete confidence in how their data is handled. The fundamental principle is simple: your data stays in Salesforce. Akoonu never exports, copies, or stores your data outside your Salesforce org. There is no Akoonu database. There is no external cloud infrastructure. Every feature — from pipeline views to AI-generated insights — operates directly on your live Salesforce data, within your existing security boundary.

Akoonu has been a **Salesforce ISV Partner since 2017**, has passed Salesforce's mandatory AppExchange security review, maintains a **5.0 AppExchange rating**, and has delivered **zero breaking changes** for customers across eight years and every Salesforce release cycle.

Architecture

Akoonu is built inside Salesforce, not connected to it. This is a fundamental architectural distinction from external revenue intelligence platforms, which sync CRM data to their own servers for processing and analysis.

Akoonu is installed from the Salesforce AppExchange as a managed package. All application code runs within the Salesforce platform using Apex, Lightning Web Components (LWC), and SOQL and other platform technologies. The application reads and displays Salesforce data in real time. It never exports data to an external system, never replicates data to an external database, and never stores customer data outside the Salesforce org.

Because Akoonu operates entirely within the Salesforce platform, there are no Akoonu-side external API connections to manage, no Akoonu-side credentials to rotate, and no Akoonu-side integration points to monitor. Users authenticate through their standard Salesforce login. There is no separate Akoonu login, no Akoonu API key management, and no Akoonu OAuth configuration required.

This architecture eliminates an entire category of security concerns that arise with external platforms: data in transit to external servers, data at rest in third-party databases, credential

management for external integrations, and the ongoing maintenance burden of keeping sync connections operational and secure.

Access Control

Akoonu inherits your Salesforce org's access control model completely. It does not implement its own permission system, does not maintain its own user directory, and does not require any access configuration beyond what you've already built in Salesforce.

Specifically, Akoonu respects your org's sharing rules, role hierarchy, and field-level security. When a user opens Akoonu, they see exactly what Salesforce allows them to see — nothing more, nothing less. A sales rep sees their own pipeline. A manager sees their team. A VP sees their region. These boundaries are enforced by Salesforce's native security layer, not by Akoonu's application logic.

Access to Akoonu is granted through standard Salesforce permission sets. There is no custom security model to learn, configure, or maintain. End users do not require system administrator access. The managed package operates within the permissions framework your Salesforce admin has already built.

Akoonu works with both Salesforce role hierarchies and territory management. Whichever access structure your org uses, Akoonu inherits it automatically. If you restructure territories or change reporting relationships in Salesforce, those changes are immediately reflected in Akoonu without any additional configuration.

AI Security

Akoonu's AI capabilities — including the Daily Advisor, Oonu conversational BI, opportunity insights, forecast analysis, and sales methodology suggestions — are designed with security as a foundational requirement. The AI processes your Salesforce data to generate insights, but it does so within a framework that gives your admin full control over what the AI can access and where processing occurs.

AI Features Are Opt-In

AI Features are disabled by default. Your admin must affirmatively enable AI Features and select an AI Processing Mode through the Services' configuration before any AI processing of your Salesforce data occurs. Disabling AI Features at any time returns the Services to the no-AI baseline.

AI Processing Modes

When AI Features are enabled, your admin selects one of three AI Processing Modes. Each has a distinct contractual posture, and each fits different security requirements.

Customer Agentforce Mode. AI processing is performed using Salesforce Agentforce or other AI capabilities native to your Salesforce Org. All AI processing occurs under your agreement with Salesforce, and Salesforce's terms govern handling of your data by the underlying AI models. Akoonu has no contractual relationship with the AI model provider in this mode.

Customer BYOK (Bring Your Own Key) Mode. AI processing is performed by a third-party AI provider (such as OpenAI or Anthropic) under your own agreement with that provider. You provide the API credential, which is stored in your Salesforce Named Credentials. Akoonu's code, executing within your Salesforce Org, makes the AI request authenticated by your credential. Your agreement with the AI provider governs the handling of your data by that provider.

Akoonu-Provided AI Mode. AI processing is performed by an AI provider with which Akoonu maintains a direct contractual relationship (currently Anthropic). Akoonu provisions a per-Customer API credential, which is stored in your Salesforce Named Credentials. Akoonu's code, executing within your Salesforce Org, makes the AI request authenticated by the Akoonu-provisioned credential. In this mode, the AI provider acts as Akoonu's sub-processor with respect to data submitted to the AI Features. See the AI Schedule at akoonu.com/legal/ai-schedule for current details.

Choosing Customer Agentforce Mode

Customer Agentforce Mode is recommended for organizations that want all AI processing governed by their existing Salesforce agreement. Whether data leaves Salesforce's infrastructure depends on which model the customer configures Agentforce to use: Salesforce-hosted models (such as Anthropic in Agentforce) keep inference on Salesforce infrastructure, while externally-hosted models accessed through Salesforce's Einstein Trust Layer (such as OpenAI or Gemini) send inference requests to the external provider under Salesforce's contractual relationship with that provider. In either case, Salesforce's terms govern the

handling of customer data, and Akoonu has no contractual relationship with the AI model provider.

AI Credentials Stay In Your Org

When AI Features are enabled in Customer BYOK Mode or Akoonu-Provided AI Mode, the AI provider API key is stored in your Salesforce Named Credentials. In BYOK Mode, you provide your own key under your own agreement with the AI provider. In Akoonu-Provided AI Mode, Akoonu provisions a per-customer key under Akoonu's agreement with Anthropic and delivers it to your Named Credentials at provisioning. In both cases, the key is stored inside your Salesforce Org. Akoonu does not maintain a credential store on external infrastructure. There is no Akoonu-side credential store that could be compromised.

Data Usage and Training

Your data is not used to train AI models. In Akoonu-Provided AI Mode, this is contractually required of Akoonu's AI provider under Anthropic's commercial terms, as further described in the AI Schedule at akoonu.com/legal/ai-schedule. In Customer Agentforce Mode and Customer BYOK Mode, the no-training commitment is established by your own agreement with the AI provider (Salesforce, OpenAI, or Anthropic), which Akoonu does not control. In every mode, AI processing is used exclusively for inference — generating insights and analysis for your team in real time.

Configurable AI Context

Admins control exactly which Salesforce objects and fields the AI has access to. Akoonu provides multiple detail levels — from standard (core opportunity and forecast fields) to detailed (extended object access including custom objects, products, and account hierarchies). This allows your admin to balance AI insight quality with data exposure based on your organization's comfort level.

MCP Integration (Optional)

Akoonu includes an optional Model Context Protocol (MCP) server that enables secure integration with external AI clients such as Claude Desktop, ChatGPT, and Slack. When enabled, the MCP server provides controlled access to Akoonu data and functionality, governed by the same Salesforce permissions that control all other access. MCP is disabled by default and must be explicitly enabled by your admin.

Geographic Considerations

If your organization has geographic data processing requirements, Customer Agentforce Mode configured with a Salesforce-hosted model (such as Anthropic in Agentforce) keeps all AI processing on Salesforce infrastructure. For other configurations, you can choose an LLM provider that meets your data residency requirements. The choice of provider and configuration is entirely within your admin's control.

Data Handling

Understanding exactly what Akoonu stores and what it does not store is essential for any security evaluation. This section provides a clear accounting.

What Akoonu Stores in Your Salesforce Org

Akoonu creates custom objects within your Salesforce org to store its own application data. This includes configuration settings, saved view definitions, formula definitions, forecast submission history, AI-generated insights and digests, cadence settings, and cached data used for performance optimization. All of this data lives inside your Salesforce org as standard Salesforce custom objects, subject to your org's backup, retention, and security policies.

What Akoonu Does Not Store

Akoonu does not copy or store your core Salesforce data. Your opportunities, accounts, contacts, leads, forecasts, pipeline data, activity history, and any other standard or custom object data remain exactly where they are in Salesforce. Akoonu reads this data live when a user opens a view, runs an analysis, or interacts with the AI. It is never replicated to an external system, never written to an Akoonu-owned database, and never cached outside your org.

Clean Uninstall

If your organization decides to remove Akoonu, the uninstall process is clean and complete. Your Salesforce data — opportunities, accounts, forecasts, and all other standard and custom objects — remains completely untouched. Only Akoonu's own custom objects and configuration data are removed. There is no data held hostage, no export required before uninstall, and no residual dependencies that affect your Salesforce org after removal.

Operational Security

Because Akoonu runs natively inside Salesforce, the operational security burden is fundamentally different from external platforms. There is no integration to monitor, no sync to maintain, no webhook to configure, and no external service to keep running.

Akoonu includes an internal master scheduler that manages all background automation jobs — including AI insight generation, sales methodology analysis, and opportunity scoring. This scheduler is designed to operate within Salesforce’s platform limits without consuming your org’s scheduled Apex capacity. Your admin has full visibility into all background jobs through the Akoonu Setup tab, including job status, last execution time, and any errors.

When Salesforce formula fields need to be used as forecasting type amount fields (a scenario where Salesforce requires a non-formula field), Akoonu provides a field mirroring tool that syncs values from formula fields to static fields on the opportunity or opportunity product object. This mirroring occurs entirely within Salesforce, with no external processing.

Compliance

Akoonu’s compliance posture is built on a simple principle: because Akoonu runs entirely within your Salesforce org and stores no data externally, your Salesforce org’s compliance posture is your Akoonu compliance posture.

Salesforce maintains an extensive set of certifications and compliance frameworks, including SOC 2 Type II, ISO 27001, GDPR, HIPAA, and FedRAMP. Your data, when processed through Akoonu, is protected by the same enterprise-grade encryption, network security, and continuous monitoring that Salesforce provides for all data within your org. For full details on Salesforce’s security infrastructure, visit trust.salesforce.com.

At the application level, Akoonu has passed the Salesforce AppExchange security review, which evaluates CRUD/FLS compliance, vulnerability testing, and code quality analysis. This review is a prerequisite for any managed package listed on the AppExchange and is re-evaluated periodically.

Akoonu's contractual data handling commitments are documented in the Akoonu Terms of Service (akoonu.com/legal/terms), the AI Schedule applicable to Akoonu-Provided AI Mode (akoonu.com/legal/ai-schedule), and the Data Processing Addendum (akoonu.com/legal/dpa).

Because Akoonu introduces no external data storage, no additional data residency requirements are created. Your data remains wherever your Salesforce org is hosted. No new geographic data processing locations are introduced. No additional compliance certifications are required beyond what your Salesforce org already maintains.

You retain full control over your security environment through Salesforce's native security tools — profiles, permission sets, sharing rules, field-level security, audit trails, and session management. Akoonu inherits every control you've configured. Changes to your security configuration in Salesforce are immediately reflected in Akoonu without any additional action.

Salesforce ISV Partnership

Akoonu has been a Salesforce ISV (Independent Software Vendor) Partner since 2017. This partnership includes passing Salesforce's mandatory security review, maintaining compliance with Salesforce's partner program requirements, and testing against every major Salesforce release cycle.

Over eight years of continuous partnership, Akoonu has delivered zero breaking changes for customers. When Salesforce releases platform updates (three major releases per year), Akoonu tests compatibility in advance and ensures that customers experience no disruption. This track record is reflected in Akoonu's 5.0 AppExchange rating.

Frequently Asked Questions

The following questions are commonly raised during security evaluations of Akoonu. They are provided here for reference.

Where does my data go?

Nowhere outside your Salesforce org. Akoonu never exports, copies, or stores your data externally. All data access occurs in real time within Salesforce.

Does Akoonu respect our sharing rules?

Yes, completely. Akoonu inherits your org's sharing rules, role hierarchy, and field-level security. Users see only what Salesforce authorizes them to see. Akoonu does not implement any access model beyond what Salesforce provides.

What happens during Salesforce releases?

Akoonu tests against every Salesforce release in advance. As an ISV Partner since 2017, Akoonu has delivered zero breaking changes for customers across eight years of Salesforce platform updates.

What if we want to remove Akoonu?

Uninstall is clean and complete. Your Salesforce data remains untouched. Only Akoonu's custom objects and configuration are removed. There is no data export required and no residual dependencies.

Does AI training use our data?

No. Your data is not used to train AI models. In Akoonu-Provided AI Mode, this is contractually required of our AI provider, Anthropic. In Customer Agentforce Mode and Customer BYOK Mode, the no-training commitment is established by your own agreement with the AI provider (Salesforce, OpenAI, or Anthropic), which Akoonu does not control. In every mode, your data is used exclusively for inference.

Do we need a separate security review for Akoonu?

Most security reviews are dramatically shorter because Akoonu has no external infrastructure. Platform-level questions (data centers, hosting, network security, encryption at rest, backup) resolve to Salesforce's own certifications. Akoonu has also passed the Salesforce AppExchange security review, which is Salesforce's mandatory evaluation for managed packages.

Can we restrict which data the AI can access?

Yes. Your admin configures exactly which Salesforce objects and fields the AI has access to, with multiple detail levels available. You control the scope of AI context based on your organization's requirements.

Can we run AI entirely within Salesforce?

Yes, depending on configuration. Customer Agentforce Mode keeps all AI processing under your Salesforce agreement. If you configure Agentforce to use a Salesforce-hosted model (such as Anthropic in Agentforce), inference runs on Salesforce infrastructure and data does not leave the Salesforce platform. If you configure Agentforce to use an externally-hosted model accessed through the Einstein Trust Layer (such as OpenAI or Gemini), data is sent to that provider under Salesforce's contractual relationship — Akoonu has no role in that relationship.

Is data sent to external LLMs?

Only if you enable AI Features. AI Features are off by default. In Customer Agentforce Mode, the answer depends on which model you configure Agentforce to use — Salesforce-hosted models (such as Anthropic in Agentforce) keep inference on Salesforce infrastructure, while externally-hosted models accessed through the Einstein Trust Layer (such as OpenAI or Gemini) send data to that provider under Salesforce's contractual relationship. In Customer BYOK Mode or Akoonu-Provided AI Mode, prompts containing your data are sent to OpenAI or Anthropic for processing under no-training terms, and the response comes back to your org. In every mode, prompts and outputs are stored in your Salesforce Org, not in Akoonu infrastructure.

Contact

For security-related questions, vendor assessment support, or to schedule a call with the Aכוןu team to discuss your organization's specific security and compliance requirements, please contact:

Email: security@akoonu.com

Web: www.akoonu.com/security