Instant Systems Sweden AB

AI Issa – Security & Compliance Statement

Document Version: 1.0
Date: June 02, 2026
Prepared by: Instant Systems

---

1. Introduction

This document outlines the security, data protection, and architectural measures implemented for **AI Issa**, Instant Systems' AI assistant. It is designed to provide customers with full transparency regarding data handling, isolation, and compliance practices.

Instant Systems is committed to the highest standards of data security and privacy. AI Issa has been developed with a **privacy-by-design** and **security-by-design** approach.

---

2. Key Security & Architecture Principles

- **Complete Separation from Production Systems** AI Issa has **no direct access** to production databases, live data sources, or the customer's operational environment. All data used by Issa is copied to a dedicated, isolated database infrastructure that is physically and logically separated from production systems.
- **Read-Only Operation** Issa operates exclusively in **Read-Only mode**. It has no technical capability to create, update, modify, or delete any records in the customer's systems.
- **Data Isolation & Confidentiality** Each customer instance of Issa works exclusively with that customer's own data. There is **zero data sharing** between customers for training, fine-tuning, or any other purpose.
- **No Sensitive Data Exposure** Issa does not process GDPR-protected personal data or other highly sensitive information unless explicitly and selectively copied for legitimate business use (with customer approval).

- **Local & Sovereign Infrastructure** Issa runs entirely within Instant Systems' own secure infrastructure. We use proprietary models hosted on GPUs in our own server park. No external third-party AI models or cloud AI services are used for core functionality.
- **No Additional Data Collection** No additional data is collected, processed, stored, or transmitted outside of Instant Systems' infrastructure as part of Issa's operation.
- **No Impact on Existing Systems** Implementation of AI Issa requires **no changes** to your existing integrations, APIs, database schemas, reporting structures, or production environment.

---

3. Frequently Asked Questions (FAQ)

Q1: What data sources does AI Issa have access to within the platform? Issa does not have access to production databases or live data sources. Data relevant for Issa is copied to a separate, isolated database infrastructure. She has no access to GDPR data or other sensitive data. Your Issa instance only has access to **your data**. No sharing of data between customers occurs for fine-tuning or any other purpose.

Q2: Does AI Issa operate on a read-only basis or can it create, update, modify, or delete records? As of today, Issa operates strictly in **Read-Only mode** and has no access to production data or data sources. It cannot create, update, modify, or delete any records.

Q3: How does AI Issa interact with the underlying database structure and application layer? Issa does not interact with your product environment or application layer. Only selected data is copied to a separate, secure database infrastructure.

Q4: Is any additional data being collected, processed, stored, or transmitted as part of the AI functionality? No additional data is collected, processed, stored, or transmitted outside of Instant Systems' infrastructure for Issa.

Q5: Are AI-generated outputs based solely on existing platform data or are external models/services involved? Issa operates solely within Instant Systems' infrastructure. We use our own locally hosted models running on GPUs in our own server park.

Q6: What impact does AI Issa have on data governance, security, permissions, audit trails, and data integrity? Security is our main concern. We have implemented strong isolation and technical controls to ensure that Issa does not affect your data governance, security policies, permissions, audit trails, or data integrity.

Q7: Does the introduction of AI Issa require any changes to existing integrations, APIs, reporting structures, or database schemas? No changes are required on your end. Your production database, APIs, BI tools, and data tables remain completely unaffected. Issa runs in a fully separate environment.

Q8: What controls are in place to ensure that AI interactions cannot inadvertently alter historical records, master data, or transactional data? Issa has no access to the production database and only has read-only permissions to the copied dataset in its isolated environment. This architectural separation makes any modification of live data technically impossible.

---

4. Conclusion

AI Issa is designed to deliver powerful AI capabilities while maintaining the highest levels of security, compliance, and data protection. By keeping Issa completely isolated from production systems and running it on our sovereign infrastructure, Instant Systems ensures that your operational data integrity and security are never compromised.

We remain fully committed to transparency and will update this document as the solution evolves.