Scrut Automation

Your Questions Answered

Responsible AI at Scrut Automation

The purpose of this document is to help provide answers to common questions our team gets from customers regarding our AI systems. Generally, our AI systems are subject to and abide by the same security program and rigorous requirements outlined and described in our Trust Vault: https://trust.scrut.io/ There are unique scenarios and circumstances when using AI systems and we are describing that here. What's described here is generally in addition to, not a substitute for our overall security program and practices.

Data Usage and Privacy

1. How will you use my data?

Scrut Automation Automation processes your inputs solely for the purpose of delivering the AI services you've opted for.

2. Will my data be used to train models for other customers?

No. We do not use customer data to train, fine-tune, or update any Scrut Automation AI models for other customers. Your data is processed in a secure, isolated environment and is never shared with or exposed to other customers.

3. Do you store my data? If so, for how long?

We store your data only for the duration necessary to process your requests or as mandated by your agreement for our AI systems the same as all of our systems. Data retention policies are clearly outlined in our terms of service, and you can request data deletion at any time in accordance with any ongoing legal requirements.

Security and Safeguards

4. Achieving ISO 42001 certification, the latest AI management system standard

We are one of the first companies to pursue and achieve ISO 42001 certification, ensuring that we've received thorough external 3rd party review of our processes on a regular and ongoing basis. Through this process we have integrated additional assurance processes into our compliance program alongside other international standards, including ISO 27001, ISO 27701 and SOC 2, to name a few. You can review the full list of international standards we comply, attest, and certify to please visit our Trust Vault.

5. **What security measures are in place for the AI systems?**

   We have strict input and output guardrails in place. We have full control over how customer provided inputs are sent to the LLMs to ensure inputs are not in violation of the acceptable use of the application and continuously monitor what comes out of the generative models.

   Our systems are protected by end-to-end encryption, secure APIs, and robust access control measures. Regular vulnerability assessments and compliance with ISO 42001 enhance our system's resilience. To review the full scope of measures we are taking, please visit our Trust Vault.

6. **What precautions are taken to prevent data breaches for your AI systems?**

   We have a comprehensive security program that spans people, process, and technology, described both in this document and in our Trust Vault [link here] including, but not limited to security monitoring, intrusion detection systems, and regular external penetration testing.

Responsible AI Use

7. **How do you ensure your AI systems operate responsibly?**

   Our AI modules are designed to follow established ethical AI principles including certifying to ISO 42001, the international standard for AI management systems, including fairness, accountability, and transparency. We are continuously carrying out extensive testing with experts in the field to ensure that the outputs are trustworthy. We have version control and rollback mechanisms in place for safety.

   We provide our customers the option to opt-in to AI features if they'd like, we don't enable these by default.

8. **Are your AI applications and data processing practices audited by 3rd parties?**

   Yes, we are committed to transparency and are actively pursuing 3rd party ISO 42001 certification.

General Concerns

9. **How do you address ethical concerns related to AI?**

   We have an internal Responsible AI committee that reviews ethical implications of our AI modules. As part of our Artificial Intelligence Management System - for which we are pursuing ISO/IEC 42001:2023 certification - we encourage feedback from external parties..

10. **How often are your AI modules updated or reviewed?**

    We review our AI modules at least quarterly and at major releases to ensure they remain secure, free of unlawful bias, and aligned with ISO 42001 and other regulatory standards.

11. **What technologies does Scrut Automation's AI systems use?**

    We primarily use AWS Bedrock hosted LLMs and Langsmith and are constantly evaluating the best combination of tools and technologies to deliver our customers the outcomes they require in the most efficient and effective fashion.