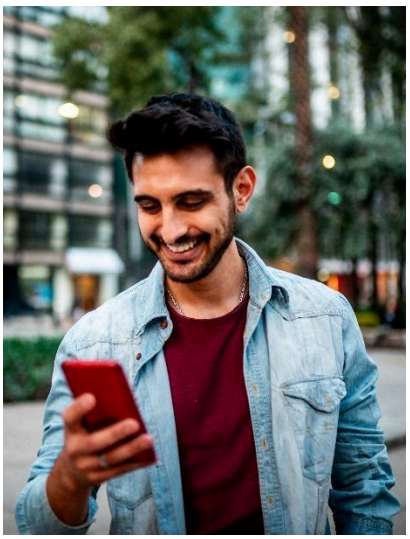
RingCentral Artificial Intelligence Transparency Whitepaper



At RingCentral, customer trust is a priority and we have created this document to describe RingCentral's approach to trustworthy artificial intelligence (AI). The purpose of this document is to help our customers and partners understand RingCentral's approach to AI and how our products use and feature AI. This whitepaper may be helpful for customers in performing AI reviews or security and privacy impact assessments of RingCentral products and services.

RingCentral services and AI

RingCentral leverages proprietary and trusted third-party AI technologies to provide services and features to our users. These include AI and automation features, such as conversational intelligence, productivity and efficiency enhancements, sales intelligence, and call handling enhancements for businesses. For example, RingCentral can generate summaries and highlights from recorded calls, and create action items and next steps, providing a seamless experience for call participants and RingCentral users. For our events-focused services, RingCentral leverages AI to assist event hosts in creating descriptions of the events and organizing questions and answers during live events.

RingCentral AI governance program

RingCentral has developed an AI governance program to support and develop trustworthy AI while fostering customer-centric innovation. RingCentral's program includes a cross-functional AI governance council and an internal AI policy. The internal AI policy is based on the NIST AI Risk Management Framework. This framework is focused on core AI principles for development and deployment of AI solutions that further the responsible and ethical use of AI. RingCentral continuously evaluates its AI-enabled products to ensure they align with regulatory standards and global best practices.

Below are the core RingCentral principles for trustworthy AI and how we align with each:

- **Safe:** At RingCentral, we believe AI-enabled systems should not endanger human life, property, privacy, or the environment.
- **Secure:** AI-enabled systems should maintain confidentiality, integrity, and availability through protection mechanisms that prevent unauthorized access and use.
- **Transparent:** Information about AI-enabled systems and their outputs should be available to users interacting with the systems.
- **Explainable and interpretable:** AI-enabled systems should enable the provision of information that describes how they function.
- **Privacy enhanced:** AI-enabled systems should be developed and used in compliance with privacy laws and RingCentral privacy policies.
- **Fair:** Development and use of AI-enabled systems at RingCentral should consider equality and equity by addressing issues such as harmful bias and discrimination.

AI models and customer data

RingCentral may use proprietary and/or third-party AI models to provide RingCentral's AI features. RingCentral does not use customer data to train its AI model, nor do we allow our third-party vendors to use RingCentral customer data to train their AI models. If the service or feature allows, customers may use their data to customize their experience when using AI within their account. For example, customers may use their own data to fine-tune the AI models within their environment. Choosing this option may enhance their experience and increase efficiency when using the service.

Third-party AI systems

When RingCentral uses AI systems procured from third-party vendors to provide AI functionalities or features, we apply a thorough third-party risk management framework to assess a vendor's AI development and compliance practices. Additionally, we ensure that proper contractual guarantees are provided by the vendor. Prospective vendors are required to complete an AI-specific questionnaire which includes questions regarding their AI development. This includes the methodology used to mitigate or eliminate bias and discrimination, risk assessments, and usage of customer data in their AI models. We contract only with third-party vendors that provide appropriate levels of data protection, security, and that align with our AI principles. Once a third party AI system is implemented into our products, RingCentral applies guardrails to monitor and assess our product(s) which mitigate and limit risks such as hallucination and bias.

The third-party AI models and systems used may depend on the service or feature, and include third parties such as Microsoft Azure OpenAI, OpenAI, Google, and AWS. Please see the RingCentral Subprocessor List, which identifies and describes third-party subprocessors, including AI vendors, as they are changed or added.

How our services align with AI laws and regulations

RingCentral is committed to supporting customer compliance with AI laws and regulations. RingCentral continuously monitors the evolving legal landscape to implement legal requirements for RingCentral products and services.

Transparency

RingCentral ensures transparency through several methods, including through this whitepaper. We also host a dedicated space on the RingCentral Trust Center focused on AI. There, our customers and partners can find information about our AI practices and policies, including our commitment to transparency, and more information about our AI products and features.

Additionally we provide our customers with detailed information on how AI uses their data and for which purposes for each service in the relevant RingCentral Product Datasheet on our Trust Center and in the RingCentral Data Processing Addendum.

Risk assessment framework

As part of the product development lifecycle, RingCentral conducts risk assessments of AI products and features early in the design and development process. These risk assessments evaluate and identify possible risks across the various stages of development and deployment. This process allows us to gain a thorough understanding of the anticipated customer experience and identify any potential risks.

RingCentral relies upon the core AI principles for trustworthy AI above as the foundation for product development, deployment, and monitoring. Included in the framework are processes for reviewing the third-party AI models and systems; ensuring data governance, record-keeping, and explainability of AI systems; and assessing unintended consequences of outputs, such as

algorithmic discrimination. The risk assessment process includes considering the intended purpose of the AI system and the customer experience, mitigating possible misuse, and assessing alignment with applicable laws. The framework is designed to be adaptive and agile to the evolving landscape of AI laws and regulations.

Customer choices

RingCentral empowers account owners to make informed decisions about their selection of RingCentral AI enabled systems by way of clear notices of generative AI features. Additionally, at the individual user level, we provide user autonomy to leverage generative AI tools. For example, our products provide a feature for transcribing calls and meetings only after a user has affirmatively enabled transcription.

Automated decision-making and human review

Customers should review outputs for accuracy and should not use outcomes or metrics generated by the service to make decisions, for instance, concerning employment, creditworthiness or insurability. Please see RingCentral's Terms of Service, Product Service Terms, and Acceptable Use Policy for more information about customer obligations to comply with applicable law in connection with using the services.

Prevention of bias

Assessing potential bias in our AI systems is a critical component of our development process. Our AI feature development is balanced across demographic groups, accessible to individuals with disabilities, and should not exacerbate existing disparities or systemic biases. RingCentral evaluates our AI features for potential bias and undesirable outputs and tests for equality and accessibility of the tools across various demographics. Each AI feature and service is reviewed by our legal team and relevant stakeholders to assess the inclusiveness for all customers.

AI literacy

RingCentral provides AI training to employees and contractors who are involved in product development and deployment of AI systems.

Security

RingCentral is committed to security and maintains technical, organizational, and contractual safeguards to protect customer data processed by our services, including with AI capabilities. We implement industry informed, AI-specific development and integration standards designed to specifically address challenges and risks in the use of AI in safeguarding customer data

RingCentral's approach to AI and security focuses on these tenets:

- AI development and integration standards for RingCentral product development
- AI use restrictions by RingCentral personnel, including engineering, architecture, and product teams
- Training model secure design restrictions to ensure separation of tenant level data and security from potential data poisoning attempts
- Operational security for access and management of the AI models

RingCentral's AI use requirements and restrictions cover proper licensing of AI solutions, what types of data may be used as inputs, scope of usage for AI system outputs internally, and use of source code from generative AI systems. With respect to training model restrictions, RingCentral's AI systems development standards set forth restrictions around AI model training, including data used for training, proper recordkeeping, storage, and access restrictions. Furthermore, RingCentral implements operational security and testing for access to and management of backend resources to prevent access to data by unauthorized personnel or modifications

without permission.

Please see our Security Addendum and our Trust Center for information on the general commitments we make to our customers about security.

Shared responsibilities

Implementation of AI is a shared responsibility with our customers. While RingCentral has based the development of our services on the core principles for trustworthy AI as described above, customers also share a responsibility to use the products safely, securely, in compliance with applicable laws. Additionally, customers must ensure human oversight into how the services are being used within their organization, including reviewing outputs generated by AI. RingCentral Services are not designed to make decisions based solely on automated processing, particularly those that produce legal effects on individuals.

RingCentral is responsible for the architecture and security of the service and the physical and environmental security of the infrastructure employed to deliver our service. Customers likewise have responsibilities, including managing their configuration settings, account policies, granting the correct roles and permissions to users; properly implementing security features, such as MFA/SSO; tracking administrative changes made on their RingCentral account; and working with RingCentral to identify suspicious activity. Ultimately, just as RingCentral is responsible for preventing disclosures of customer account information and call data, users are also responsible for preventing disclosures of their settings and their information.

Customers are responsible for ensuring that AI features and functionalities are used in compliance with our Terms of Service, Acceptable Use Policy, Product Service Descriptions, and applicable laws.

Contact us

Should you find an answer to your question missing from our various resources, feel free to contact us.

About this white paper

The information provided in this white paper does not constitute legal or professional advice, warranty of fitness for a particular purpose or compliance with applicable laws. RingCentral reserves the right to update this white paper from time-to-time.