The Cisco Responsible AI Framework

Trustworthy AI by Design

At Cisco, we appreciate that Artificial Intelligence (AI) can be leveraged to power an inclusive future for all. We also recognize that by applying this technology, we have a responsibility to mitigate potential harm. That is why we have developed the six Principles for Responsible Artificial Intelligence of Transparency, Fairness, Accountability, Privacy, Security and Reliability – all necessary for promoting and enabling safe and trustworthy AI.

To implement these principles, we have a Responsible AI Framework that can be applied to the development, deployment and/or use of AI by Cisco, whether in developing a product or model for our customers and partners to use, integrating and building upon a third-party model for unique offerings, or providing AI tools or services for our own, internal operations. In practice, we strive to bring these principles to life by combining Security by Design, Privacy by Design, and Human Rights by Design to surface and mitigate risks to provide AI that is responsible and trustworthy.

The Responsible AI Framework

Guidance and Oversight	• Provide leadership oversight through a Responsible AI Committee of senior executives across Cisco engineering, sales, privacy, security, human rights, legal, government affairs, human resources, and other functions. • Advise Cisco on Responsible AI practices and oversees Responsible AI Framework adoption. • Review sensitive or high-risk uses of AI proposed by our business units and incident reports for bias or discrimination.
Controls	• Incorporate security, privacy, and human rights principles into AI design, leveraging the existing Cisco Secure Development Lifecycle. • Require assessments for relevant AI use cases, models, and functions to identify, prevent, and mitigate potential risks, including risks to privacy, security, and human rights that meet or exceed assessment standards in the markets in which we operate.
Incident Management	• Leverage security, data breach, and privacy incident response system to manage reported AI incidents. • Assign and report incidents to the AI Governance Team to analyze and engage relevant team for resolution. • Track and report AI incidents and share findings and remediation steps to the original submitter or a broader group of stakeholders, customers, employees, and partners.
Industry Leadership	• Establish AI governance practices with specific focus on proactively supporting and leading Cisco to deliver AI in a responsible and trustworthy manner. • Participate in leading industry forums, including those involving open source and other technology standardization bodies to advance the responsible use of AI.
External Engagement	• Work with governments and regulatory bodies to understand global perspectives on AI's benefits and risks. • Monitor, track, and influence AI-related legislation, emerging policy, standards, and regulations when and as appropriate. • Partner with cutting-edge research institutions, industry associations, and civil society organizations to develop best practices for AI development and governance from technical, organizational, social, and design perspectives.

Cisco is committed to continuing internal focus and collaboration with our external partners and stakeholders to improve our collective understanding of the societal and human rights impact of AI. We work to continuously improve our framework to support fair, explainable, and transparent results of the AI systems we develop and use.

Learn more about our approach to Responsible AI at the Cisco Trust Center.