Tungsten Automation: Our Commitment to Responsible AI and Compliance

May 2026

Proprietary and Confidential © 2026 Tungsten Automation Corp. All rights reserved.

TUNGSTEN AUTOMATION

Table of Contents

Tungsten Automation: Our Commitment to Responsible AI and Compliance 3
Document Purpose 3
Executive Summary 3
Our Approach to AI Governance and Compliance 4
Ongoing Compliance Efforts 4
AI Safety 4
Transparency and Trust 5
Responsible AI 5
Embedding Responsible AI Across Our Organization 5
Tungsten Automation's Responsible AI Principles 5
Building a Responsible AI Compliance Program 6
Continuous Learning and Ethical AI 7
Tungsten Automation Trust 8
Highlights of Tungsten Automation's Security Approach 8
Security Best Practices and Certifications 8
Global AI Legislation 9
Understanding the EU AI Act (AIA) 9
Understanding US Federal AI Policy 10
Understanding California's AI Transparency Laws 10
AB 2013: Artificial Intelligence Training Data Transparency 10
SB 942: California AI Transparency Act 11
Conclusion 12

© 2016-2026 Tungsten Automation. All rights reserved. Tungsten Automation is a trademark of Tungsten Automation Corporation (Formerly known as Kofax Inc), registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Tungsten Automation. This document is for informational purposes only and is not intended as a legally binding document.

Tungsten Automation: Our Commitment to Responsible AI and Compliance

Last updated: May 2026

Document Purpose

This document serves as a declaration of Tungsten Automation's commitment to fostering trust and transparency in the deployment of artificial intelligence (AI) technologies.

This document outlines our proactive initiatives, guiding principles, and future commitments to uphold responsible AI usage, reflecting our dedication to navigating the complexities of AI governance with integrity and foresight.

Executive Summary

As a global leader in business automation solutions, we understand the importance of trust and transparency in the use of emerging technologies such as artificial intelligence (AI) and recognize the imperative of aligning with emerging regulatory frameworks, including the EU AI Act (now in phased enforcement) and current U.S. federal AI policy, to ensure the safety, security, and compliance of our AI systems.

Our customers are central to our mission, and we are dedicated to exceeding regulatory requirements and customer expectations through the applications of ethical AI practices, and applying the highest standards of AI safety, security, and compliance. In the rapidly evolving regulatory landscape for Artificial Intelligence, with the EU AI Act now in phased enforcement and U.S. federal AI policy evolving under Executive Order 14179, we continue to align our practices with enacted and emerging regulations.

While compliance with these frameworks is an ongoing journey, Tungsten Automation is committed to responsible AI use and is actively working to meet all regulatory requirements. This statement outlines our guiding principles, current initiatives, and forward-looking guidance regarding AI regulation and compliance.

Our Approach to AI Governance and Compliance

We are continuously working towards meeting all compliance requirements, proactively engaging with regulatory bodies, industry groups, and AI ethics experts to stay ahead of the evolving standards.

As part of our commitment to building AI systems that are both effective and trustworthy, we have adopted a comprehensive approach to AI governance. Below, we outline key areas of our ongoing efforts to ensure that our AI systems meet the highest standards of safety, transparency, and fairness.

Ongoing Compliance Efforts

We understand that compliance is not a one-time achievement but a continuous process. As regulations continue to evolve, we remain committed to assessing and improving our AI systems to meet the latest compliance standards. Our ongoing efforts include:

- Conducting regular AI risk assessments and internal audits to ensure our systems remain compliant with EU and U.S. regulatory frameworks and any other global standards.
- Collaborating with industry groups, regulators, and academic institutions to stay informed about the latest developments in AI ethics and governance.
- Ensuring transparency by keeping our customers informed about our progress towards full compliance with the EU AI Act and current U.S. federal AI policy.

AI Safety

Establishing Robust AI Systems Through Rigorous Evaluation and Validation: We are dedicated to ensuring that every AI system we develop undergoes comprehensive evaluation, verification, and validation prior to deployment. Tungsten's commitment includes continuous testing of AI models using advanced methodologies, such as systematic measurement techniques. Where appropriate, we provide key stakeholders with detailed summaries of these evaluations, ensuring transparency and trust.

Tungsten's proprietary AI models are built in compliance with our **Responsible AI Principles**. Customers can also train their own models with our tools; in which case the customer is responsible for the provenance and quality of the training data.

Tungsten Automation manages machine learning training data using the same operational processes as other source code assets to ensure the highest levels of security, accountability, and

reproducibility. Any data samples used to train AI models undergo specific scrubbing to remove or redact any/all PII data prior to their inclusion in the training data set.

Adopting Reliability and Safety Protocols: Tungsten's AI systems are designed with a multi-layered safety-by-design approach, ensuring that models and applications operate securely and remain under human oversight. Tungsten Automation continuously refine and improve these practices to meet the most stringent reliability and safety standards, thereby safeguarding the integrity and dependability of our AI solutions.

Transparency and Trust

We believe that transparency is key to building trust with our customers. As we continue to work towards full compliance with the EU AI Act and other upcoming regulations on AI, we remain committed to openly communicating our progress and sharing relevant updates with our customers. Our goal is to ensure that our AI solutions not only meet regulatory requirements but also exceed customer expectations for safety, security, and fairness.

Responsible AI

As a global leader in business automation solutions, we have long understood the transformative potential of artificial intelligence (AI) for both our organization and the broader industry. Equally critical, however, is the imperative to develop, design, and deploy AI responsibly. Our leadership recognized early on that if not managed ethically, AI could lead to significant adverse consequences, such as algorithmic bias, inaccurate outputs, workforce displacement, or even cyber vulnerabilities.

With AI's rapid evolution and its potential to redefine business operations, we set out to address a fundamental challenge: How can we govern AI in a way that harnesses its value, mitigates its risks, and builds enduring trust among our customers, employees, and shareholders.

Embedding Responsible AI Across Our Organization

To ensure the responsible and ethical scaling of AI technology, we are dedicated to implementing a comprehensive Responsible AI Compliance Program. This program is designed to safeguard our organization while also fostering trust with clients, partners, and the general public.

Our Responsible AI initiative enables us to leverage AI effectively, while ensuring that it is used ethically, with risk mitigation at the forefront.

Tungsten Automation's Responsible AI Principles

Our Responsible AI framework is guided by key principles that we apply to our internal operations,

as well as to our work with clients, partners, and suppliers:

- **Human-Centric Design**: We prioritize understanding the impact of AI on people and proactively manage any associated risks.
- **Fairness**: We are committed to ensuring that all AI models treat individuals and groups equitably. We take deliberate actions to identify and eliminate biases.
- **Transparency, Explainability, and Accuracy**: Our AI practices are built on transparency. We disclose the use of AI and ensure that our models' outputs and decision-making processes are clear and comprehensible to stakeholders.
- **Safety**: We rigorously assess potential safety concerns and take necessary measures to mitigate risks when deploying AI systems.
- **Accountability**: We maintain robust, documented governance structures across the organization, ensuring clear roles, policies, and responsibilities for accountable AI deployment.
- **Compliance, Data Privacy, and Cybersecurity**: Our AI systems are designed to comply with all relevant legal requirements. We also ensure that our systems are safeguarded against cyber threats and that data privacy is rigorously protected.
- **Sustainability**: AI deployments are conducted with sustainability in mind, and we actively seek to minimize any environmental impact resulting from AI system usage.

Building a Responsible AI Compliance Program

While guiding principles provide a foundation, they alone are not sufficient to ensure ethical AI usage. To reinforce these values, we are dedicated to build a Responsible AI Compliance Program, supported by four core pillars:

- **Establishing AI Governance and Principles**: We have heightened leadership awareness regarding the risks and opportunities of AI, created governance frameworks, implemented comprehensive policies and standards, and formed a multi-disciplinary team to oversee AI initiatives.
- **Conducting AI Risk Assessments**: Our compliance program includes systematic risk assessments to identify potential threats from AI deployment. We also review evolving regulatory frameworks to ensure our practices remain compliant and mitigate risks before they materialize.
- **Systematic Enablement for Responsible AI Testing**: We are dedicated to institutionalizing our approach to responsible AI, embedding ethical standards and compliance mechanisms

across all relevant technologies, processes, and systems. We have also developed tools for testing and trained our personnel in the best practices for responsible AI deployment.

- **Ongoing Monitoring and Compliance**: We conduct continuous post-deployment monitoring of AI systems to ensure they align with our Responsible AI principles. This includes quality assurance protocols and mechanisms for evaluating the ongoing effectiveness of our compliance efforts.

Continuous Learning and Ethical AI

We recognize that the responsible use of AI is an evolving journey, and continuous learning is essential to staying at the forefront of ethical AI practices. To this end, we provide ongoing responsible AI training and AI security training for our employees, equipping those most directly involved in AI development with the latest tools and frameworks to make informed and ethical decisions. Furthermore, we have implemented mandatory ethics and AI training for key personnel to ensure that ethical considerations are embedded throughout every stage of our AI development and deployment process.

By embedding responsibility and ethics into every level of our AI systems, we are confident that we will not only unlock the transformative potential of AI but also ensure that its use remains aligned with the highest ethical standards.

Tungsten Automation Trust

Tungsten Automation takes building and maintaining the trust of our customers seriously. Tungsten Automation provides robust security, compliance, and privacy programs that carefully consider data protection matters across our suite of products. The Tungsten Automation Trust site ensures you have the latest security, compliance, ESG, and privacy information at your fingertips.

Highlights of Tungsten Automation's Security Approach

- **Data Security:** Industry standard physical and technical measures to protect you and your data.
- **Product Testing:** Robust data and privacy compliance testing and threat and vulnerability management programs.
- **Risk Management:** 24/7/365 network security monitoring procedures to keep you running.
- **Organization and Management:** Dedicated teams of SMEs across privacy, information security, and compliance.
- **Audits and Attestations:** Significant investment in maintaining globally recognized certifications and attestations.
- **Communications:** Proactive incident response management and communications on security incidents.

Security Best Practices and Certifications

All products and services are implemented in accordance with Tungsten Automation's Secure Software Development Lifecycle Policy (more details of which can be provided on request).

The Tungsten Automation Secure Software Development Lifecycle process consists of a series of activities to address various aspects of security as it relates to the software development process. These activities apply to all phases of the development process, from Planning through Design and Implementation phases, and finally through Quality Assurance, Release and Maintenance.

Tungsten Automation maintains a comprehensive set of compliance certifications and attestations that demonstrate our commitment to protecting customer data and following regulatory and industry standards. Certifications may vary by product; please contact your Tungsten Relationship Manager for more information.

Global AI Legislation

The global landscape of AI regulation is rapidly evolving, with an increasing recognition of the need for comprehensive governance frameworks to manage the risks and benefits associated with AI technologies. The European Union has taken a pioneering role with the AI Act, the first legal framework addressing AI risks, which categorizes AI systems into four risk levels and imposes strict obligations on high-risk applications.

This approach is setting a global precedent, potentially influencing international standards, nevertheless countries worldwide are developing their own AI national strategies and ethics policies.

The following sections detail our approach to key announced and upcoming global legislation.

Understanding the EU AI Act (AIA)

The EU Artificial Intelligence Act (EU AI Act) represents the first comprehensive regulatory framework aimed at governing the deployment and use of AI technologies within the European Union.

Adopted by the European Parliament, the Act categorizes AI systems based on a risk-based approach, aiming to protect individuals' fundamental rights while fostering innovation.

The Act outlines four levels of risk associated with AI systems:

- Unacceptable risk
- High risk
- Limited risk
- Minimal risk

Systems that fall under the unacceptable risk category—such as AI used for subliminal manipulation, biometric surveillance, or social scoring—are prohibited outright. High-risk AI systems, including those used in critical areas such as education, employment, law enforcement, and healthcare, are subject to stringent requirements. These systems must comply with specific obligations, including rigorous risk management, transparency, accountability, and human oversight.

Enforcement is now underway in phases: prohibitions on unacceptable-risk AI (e.g., social scoring, real-time biometric surveillance) have been in force since Feb 2, 2025; governance requirements for general-purpose AI models (GPAI) took effect Aug 2, 2025; high-risk AI system obligations are imminent (Aug 2026); and requirements for pre-existing legacy systems follow in Aug 2027. We are committed to ensuring that none of our AI applications fall under the prohibited use cases, and we continue to assess our portfolio against the high-risk classification criteria as enforcement milestones approach.

The EU AI Act's timeline for enforcement spreads over two years from the date of its adoption. Many obligations for most AI systems will become effective 24 months after its entry into force, giving organizations the time to align their practices and technology to the regulatory requirements. However, for pre-existing AI systems that fall under the general-purpose AI category and have not undergone substantial modifications, the compliance deadline is extended to 36 months from the Act's entry into force, providing a longer window for certain systems to become compliant.

Understanding US Federal AI Policy

On January 23, 2025, President Trump signed Executive Order 14179, “Removing Barriers to American Leadership in Artificial Intelligence,” which revoked the prior administration’s Executive Order 14110 and directed federal agencies to update AI governance policies to prioritize U.S. competitiveness, innovation, and national security. The new order emphasizes removing unnecessary regulatory barriers to AI development while maintaining safeguards aligned with American values. We monitor U.S. federal AI guidance on an ongoing basis and align our internal practices accordingly.

Our AI governance framework is designed to remain adaptive and compliant regardless of evolving federal policy direction. We maintain ongoing dialogue with legal and regulatory counsel to ensure our practices keep pace with the current U.S. federal AI policy landscape, including applicable NIST guidance and sector-specific federal requirements.

Understanding California’s AI Transparency Laws

On September 29, 2024, California enacted two critical AI laws, **AB 2013: Artificial Intelligence Training Data Transparency, effective January 1, 2026, and SB 942: California AI Transparency Act, whose operative date was deferred to August 2, 2026 by AB 853 (signed October 13, 2025)**. These regulations aim to increase transparency in AI development, ensuring the public has insight into how AI systems are built and how AI-generated content is identified. We have completed our initial compliance assessment and are aligning with applicable requirements across our product portfolio.

AB 2013: Artificial Intelligence Training Data Transparency

AB 2013 focuses on transparency regarding the training data used to develop AI systems. Under this law, developers must provide a summary of the datasets used to train any AI system that generates synthetic content, such as text, images, video, or audio.

Key provisions include:

- Posting a publicly accessible summary of the datasets used, detailing sources, content types, and ownership, and noting whether the data contain personal information or are synthetic.

- Requiring transparency for any generative AI systems available to Californians, even if developed before 2026.

Our Approach: As our AI tools generate text and code outputs, without creating or modifying images, audio, or video, AB 2013's requirements do not apply to our products. Nevertheless, we are creating product-specific summaries with relevant information pertaining to the AI and Machine Learning technologies used within each product, within the bounds of proprietary and legal constraints. This commitment reflects our dedication to transparent practices, enhancing customer trust and understanding of our AI tools.

SB 942: California AI Transparency Act

SB 942 targets generative AI systems that produce images, audio, and video, mandating additional transparency for these outputs. While this law primarily affects providers with more than 1 million monthly users and those producing audiovisual content, its provisions promote industry-wide practices for disclosing AI-generated content.

Key requirements include:

- Offering a detection tool for users to verify if content was AI-generated.
- Embedding latent disclosures within AI-generated images, video, or audio to help users identify them as such.

Our Approach: Tungsten Automation's AI services generate only text and code outputs and do not produce images, audio, or video. As such, we fall outside SB 942's current scope. However, as an industry leader, we continuously assess our products and user reach to ensure compliance with both the spirit and letter of evolving AI transparency standards. We also implement internal measures to ensure transparency in our AI content generation practices.

Conclusion

In conclusion, our dedication to AI safety, security, and compliance remains steadfast. As the EU AI Act moves through its phased enforcement timeline and U.S. federal AI policy continues to evolve, we are proactively aligning our systems and practices with enacted obligations and emerging standards. Our AI governance framework now incorporates EU AI Act compliance obligations, current U.S. federal policy alignment, ISO/IEC 42001:2023 guidance, and best practices for agentic AI systems. We are committed to continuously monitoring the regulatory environment, adapting our processes, and maintaining transparency with our customers.

Your trust is paramount to us. We are dedicated to ensuring that our AI systems are not only safe, reliable, and ethical, but also fully compliant with all applicable regulations worldwide. As an intelligent automation leader, we view responsible AI governance as a competitive differentiator and a core commitment to our customers, partners, and the communities we serve.