



Intravo Responsible AI and Data Use Statement

SECURITY • PRIVACY • TRUST

Version: 1.0

Status: Published

Distribution: Public

Classification: Public

Policy owner: Adam Luz, Company Owner and Information Security Coordinator

Effective: September 24, 2026

Review cycle: At least annually and after a material legal, contractual, business, technology, vendor, risk, or security change

Public

Purpose

Describe Intravo Corp's public commitments for responsible use of artificial intelligence, including human accountability, data protection, security, transparency, and regional processing.

Scope

This statement covers AI features and AI-assisted internal workflows used in delivering Intravo services. It does not expand customer data uses beyond contracts, notices, or documented customer instructions.

Policy requirements

- AI use must have a defined business purpose, accountable owner, approved data classification, and documented risk assessment proportionate to impact.
- Confidential, customer, or personal data may be provided only to approved AI systems with appropriate contracts, access controls, retention settings, regional processing, and documented authorization.
- Customer content is not used to train general-purpose models unless a contract and explicit authorization permit that use.
- People remain accountable for consequential decisions. AI output must be reviewed for accuracy, bias, confidentiality, intellectual property, safety, and suitability before use.
- Intravo prohibits unlawful discrimination, deceptive impersonation, covert surveillance, unauthorized biometric categorization, and uses prohibited by applicable law or customer agreement.
- AI systems are monitored for security, quality, drift, misuse, and material changes. Significant changes trigger renewed assessment and approval.
- EU-origin data must follow Intravo's EU processing path. An approved contract alone does not override a stricter customer residency commitment.

Roles and responsibilities

- **Company Owner and Information Security Coordinator:** Approves this document, assigns control owners, resolves material risk decisions, and ensures appropriate resources and oversight.
- **System, service, process, and data owners:** Implement applicable requirements, maintain records, test controls, and remediate deficiencies.
- **Managers:** Grant work and access only to trained, authorized personnel and escalate exceptions, incidents, and overdue actions.
- **All personnel:** Follow this document, protect information and systems, complete required training, and report suspected failures promptly.
- **Vendors and contractors:** Meet applicable contractual requirements and provide requested assurance evidence.

Operating procedure

1. AI use cases are inventoried and categorized before production use.
2. Higher-impact uses require documented testing, human oversight, rollback or disablement capability, and legal or privacy review when applicable.
3. AI-related concerns may be reported to security@intravo.com or privacy@intravo.com and are handled through established incident and privacy procedures.

Monitoring and evidence

Control owners retain evidence in approved systems according to the Document Retention Policy. Evidence includes:

- AI use-case inventory.
- AI impact assessments.
- Model and vendor approvals.
- Evaluation results.
- Human-review records.
- Change and incident records.

Material deficiencies, missing evidence, repeated failures, and overdue corrective actions are recorded in the risk or remediation register and reported to the Company Owner.

Exceptions and enforcement

Exceptions require a documented business need, exact scope, risk assessment, compensating controls, owner, approver, expiration date, and review schedule. An exception does not waive legal, contractual, or customer obligations. Violations may result in access restriction, corrective action, contract remedies, or discipline up to termination of employment or engagement.

Related standards

- NIST AI Risk Management Framework
- NIST AI 600-1 Generative AI Profile
- ISO/IEC 42001:2023
- EU AI Act Regulation (EU) 2024/1689

Document control

The controlled copy and revision history in the Intravo compliance portal are authoritative. Printed or downloaded copies are uncontrolled after export. This document does not, by itself, represent a SOC 2 attestation, regulatory certification, or legal opinion.

Version 1.0 — Effective September 24, 2026. Comprehensive 2026 review, current brand, current control framework, and publication-ready organization.