



Intravo Security and Privacy Overview

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

Provide customers and partners with a clear description of Intravo Corp's security, privacy, resilience, and governance commitments without exposing sensitive implementation details.

Scope

This overview applies to Intravo-hosted services, corporate operations, personnel, approved subprocessors, and the US and EU service regions used to deliver contracted services.

Policy requirements

- Identity is centrally managed. Multifactor authentication, risk-based Conditional Access, least privilege, and periodic access review are required for company systems.
- Company endpoints must be enrolled in approved management, encrypted, protected by endpoint security, patched, and compliant before they may access protected services.
- Data is encrypted in transit and at rest using approved protocols and managed keys. Secrets are stored outside source code and rotated based on risk and lifecycle events.
- Production changes require authorization, testing, rollback planning, and retained evidence. Secure development includes peer review, dependency management, and security testing proportionate to risk.
- Security-relevant events must be centrally logged and investigated. Intravo requires incident-response, business-continuity, backup, and recovery procedures and risk-based testing.
- Vendors and subprocessors are risk reviewed before use and periodically thereafter. Contractual privacy, security, confidentiality, and incident-notification obligations are required where appropriate.
- Intravo's regional-processing standard requires separate US and EU service paths and restricts EU-origin customer content and identifiable telemetry to approved EU processing paths.

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. Customers may request current security documentation, relevant subprocessor information, and reasonable assurance evidence subject to confidentiality and contractual limits.
2. Security concerns may be reported to security@intravo.com. Intravo triages reports, contains confirmed incidents, preserves evidence, and provides legally or contractually required notices.
3. This overview is reviewed at least annually and after a material change to services, law, risk, or security architecture.

Monitoring and evidence

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

- Controlled policies and revision history in the Intravo compliance portal.
- Access reviews, device-compliance reports, vulnerability and patch records, change tickets, incident exercises, vendor reviews, and continuity-test 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

- AICPA Trust Services Criteria
- NIST Cybersecurity Framework 2.0
- CIS Controls v8.1
- ISO/IEC 27001:2022

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.