



# Intravo Security Privacy and Compliance Policy Manual

SECURITY • PRIVACY • TRUST

Version 2.1

**Status:** Published

**Distribution:** Public

**Portal version:** 2.1

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

**Effective:** October 14, 2026

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

Public

## Purpose and decision

Intravo Corp adopts this manual as the governing baseline for information security, privacy, resilience, responsible artificial intelligence, and compliance operations. It is designed to support a SOC 2 control environment, the EU General Data Protection Regulation where applicable, customer commitments, and the company security standards described below.

This manual does not itself create a SOC 2 attestation or prove GDPR compliance. Intravo demonstrates operation of these requirements through deployed controls, retained evidence, periodic review, testing, remediation, and independent assessment where required.

## Scope

This manual applies to all Intravo Corp directors, officers, employees, interns, contractors, temporary personnel, systems, software, cloud environments, endpoints, networks, vendors, subprocessors, and information used for company business. It applies regardless of location, ownership, or hosting model.

Customer contracts and applicable law may impose stricter requirements. The stricter requirement controls unless the Company Owner and Information Security Coordinator documents a lawful exception.

## Control framework

Intravo organizes its security and privacy program around:

- The AICPA Trust Services Criteria for Security and, when included in the audit scope, Availability, Confidentiality, Processing Integrity, and Privacy.
- GDPR principles and controller or processor obligations, including Articles 5, 25, 28, 30, 32, 33, 35, and 44 through 49 where applicable.
- NIST Cybersecurity Framework 2.0 functions: Govern, Identify, Protect, Detect, Respond, and Recover.
- CIS Benchmarks Level 1 as the default secure configuration baseline for supported operating systems, servers, cloud services, and databases. Level 2 controls are evaluated for higher-risk systems and tested before enforcement.
- Customer contracts, data processing agreements, business associate agreements where applicable, and other documented commitments.

The Company maintains a control matrix that maps these requirements to control owners, systems, evidence, review frequency, exceptions, and remediation items.

## Governance and accountability

Adam Luz, as Company Owner and Information Security Coordinator, is accountable for the security and privacy program, risk acceptance, policy approval, control oversight, incident coordination, vendor-security review, and management reporting. Operational responsibilities may be delegated, but accountability remains assigned and documented.

System Owners are responsible for inventories, access, secure configuration, patching, backup, recovery, logging, vendor dependencies, and evidence for their systems. Data Owners determine authorized use, classification, residency, retention, and disclosure. Workforce members must follow policy, complete training, protect credentials and devices, and report suspected incidents promptly.

Intravo reviews the security program at least quarterly. The review covers material risks, incidents, exceptions, vulnerability and patch performance, access reviews, vendor status, device compliance, monitoring coverage, privacy requests, retention failures, and progress against the remediation register.

## Risk management

Intravo maintains a risk register as the authoritative record of identified security, privacy, operational, vendor, and compliance risks. Material technology, vendor, data-flow, regional-processing, and contractual changes require a documented risk assessment before production use.

Each risk has an owner, affected assets, inherent and residual ratings, existing controls, treatment decision, target date, evidence, approval authority, and review date. Critical risk acceptance requires written owner approval,

compensating controls, and a time-bound remediation plan. High risks affecting customer data are reviewed at least quarterly and may not remain accepted indefinitely.

## Asset and data inventory

Intravo maintains inventories of production systems, cloud accounts, endpoints, applications, repositories, service identities, vendors, subprocessors, information assets, and significant data flows. Inventories identify the owner, environment, region, classification, retention, recovery objective, dependencies, and monitoring source.

Unknown, unsupported, or unowned assets may not process customer or confidential data. Discovery of an unowned production asset requires prompt assignment of ownership or removal from service.

## Information classification and handling

Information is classified as Public, Internal, Confidential, or Restricted. This is Intravo's only approved classification scheme. It applies to all information and to every system that stores, processes, or transmits it, including email, chat, documents, files, and the compliance portal. The Intravo Asset Management and Data Classification Policy defines the minimum handling for each label.

- Public information is approved for external disclosure.
- Internal information is intended for the Intravo workforce and approved partners.
- Confidential information includes customer information, contracts, source code, business records, nonpublic operational data, credentials metadata, security records, employee information, and personal data.
- Restricted information includes secrets and private keys, authentication material, sensitive personal data, regulated data, security investigation details, and information contractually designated for heightened protection.

Customer and internal information is treated as Confidential unless a Data Owner approves another classification. Restricted information requires explicit authorization, encryption in transit and at rest, restricted administration, enhanced logging, and documented retention.

Classification labels configured in any system, including Microsoft Purview sensitivity labels used in Outlook, Teams, SharePoint, and OneDrive, must use these four names. No other label set may be configured or used. The former Highly Confidential label is retired; information previously marked Highly Confidential is handled as Restricted.

## Privacy and GDPR

Intravo processes personal data lawfully, fairly, transparently, and only for specified purposes. Collection and use must be limited to data that is relevant and necessary. Personal data must be accurate where accuracy matters, retained only as long as required, protected according to risk, and handled so Intravo can demonstrate accountability.

Before a new or materially changed processing activity begins, the owner must document its purpose, categories of data and data subjects, legal basis or customer instruction, recipients, processors, region, retention, security controls, and deletion method. Intravo maintains records of processing activities appropriate to its controller and processor roles.

Intravo uses privacy by design and by default. Systems default to the least data, least access, shortest defensible retention, restricted disclosure, and secure deletion. A data protection impact assessment is required before processing likely to create high risk to individuals, including large-scale monitoring, sensitive data, biometric or voice-derived processing, or material automated decision-making.

Intravo supports applicable rights requests, including access, correction, deletion, restriction, objection, portability, and notice rights. Requests are logged, identity is verified, deadlines are tracked, applicable exceptions are documented, and customer instructions control when Intravo acts as a processor.

Intravo designates a Privacy Lead for program administration. Use of the statutory title Data Protection Officer requires a documented legal determination that appointment is required or a deliberate voluntary appointment with the independence and resources required by law.

## **Data residency and international transfers**

The Intravo Data Residency and International Transfer Standard is mandatory. EU-origin customer content and personal data must remain in approved EU production, storage, backup, recovery, logging, analytics, and support paths unless a documented exception is approved before transfer.

US-origin data may be hosted in an approved EU region when customer commitments and applicable law permit it. EU-origin data must not be routed to a US service merely because that service has a DPA, BAA, SOC 2 report, or encryption. Contractual and technical residency controls are separate requirements.

## **Identity and access management**

Every user receives a unique identity. Shared interactive accounts are prohibited except for documented emergency-access accounts. Multifactor authentication is required for workforce and administrative access. Legacy authentication is blocked where supported.

Access is based on least privilege, need to know, role, device posture, and environment. Privileged access uses separate administrative roles or identities where feasible and is reviewed at least quarterly. Service identities are noninteractive, narrowly scoped, inventoried, monitored, and rotated according to risk.

Access is approved before provisioning, reviewed after role changes, and removed promptly after separation or loss of business need. Emergency-access accounts are tightly limited, monitored, tested on a defined schedule, and excluded from controls only where necessary to preserve recoverability.

Applications handling Confidential or Restricted information must enforce authorization server-side on every request. Authentication alone is not authorization.

## **Endpoint and BYOD security**

Company-managed endpoints must be enrolled in the approved management platform, encrypted, protected by endpoint detection and response, configured with firewall and antimalware controls, patched, locked automatically, and reported compliant before accessing restricted company applications.

Intravo may use Conditional Access to require a compliant managed device. An application may perform an additional compliance check at sign-in, but application checking does not replace identity-provider enforcement.

Personal mobile devices may access approved company data only through approved applications protected by mobile application management. Intravo may require enrollment on a company-managed device for higher-risk roles, customer commitments, development access, administrative access, or systems that cannot be adequately protected through application management alone.

Lost, stolen, compromised, rooted, jailbroken, unsupported, or noncompliant devices must be reported immediately and may be blocked or selectively wiped.

## **Cryptography and key management**

Confidential and Restricted information is encrypted in transit using current approved protocols and at rest using approved platform controls. TLS 1.0 and 1.1 are prohibited. New systems use TLS 1.2 or later, with TLS 1.3 preferred where supported.

Secrets, private keys, tokens, certificates, and encryption keys are stored in approved secret or key management services rather than source code, tickets, chat, or unprotected configuration files. Access is restricted and logged. Keys are generated with approved methods, assigned an owner, rotated according to risk and provider capability, revoked after compromise or loss of need, and recoverable only through controlled procedures.

Production and nonproduction credentials are separate. Customer-specific keys are segregated when required by contract or risk.

## **Server cloud and network security**

Production infrastructure uses approved regions, private networking where feasible, least-privilege security groups, encrypted storage, encryption in transit, centralized logging, monitored administrative access, and documented backup and recovery.

Supported CIS Level 1 benchmarks are the default hardening target. Exceptions are tested, justified, recorded in the risk register, and reviewed. Internet-exposed services use a documented edge-security design, rate limiting where appropriate, vulnerability monitoring, and origin restrictions that prevent bypass of the intended access layer.

Production, staging, development, and administrative environments are logically separated. Direct database access is restricted to authorized administrative paths. Public access, wildcard principals, legacy protocols, default credentials, and unused services are prohibited unless a documented exception exists.

## Vulnerability and patch management

Intravo continuously identifies vulnerabilities through platform findings, endpoint and cloud security tools, dependency scanning, code scanning, vendor advisories, penetration testing, and responsible reports.

Findings are risk-ranked using exploitability, exposure, asset criticality, data sensitivity, customer impact, and available compensating controls. Target remediation times are:

| Severity                        | Default target                                                                     |
|---------------------------------|------------------------------------------------------------------------------------|
| Critical and actively exploited | Contain immediately and remediate as soon as practicable, normally within 72 hours |
| Critical                        | 14 calendar days                                                                   |
| High                            | 30 calendar days                                                                   |
| Medium                          | 90 calendar days                                                                   |
| Low                             | 180 calendar days or documented acceptance                                         |

Exceptions require a documented risk decision, compensating controls, owner, expiration, and re-evaluation date. Remediation is verified through rescanning or equivalent evidence.

Operating systems, browsers, applications, firmware, cloud services, libraries, and container images are patched according to risk. Emergency changes may use an expedited path but must be documented and reviewed after implementation.

## Secure development and change management

Security and privacy requirements are defined during design. Material changes require threat modeling or documented security review when they alter authentication, authorization, cryptography, data flow, regional processing, external exposure, AI processing, or vendor dependencies.

Source changes use version control, peer review, automated testing appropriate to risk, secret scanning, dependency and code security analysis, and protected release workflows. Valid security findings are resolved or formally accepted before release. Production deployments are attributable to an approved change and include verification and rollback procedures.

Emergency changes are limited to urgent restoration or risk reduction, use the narrowest safe scope, retain evidence, and receive retrospective approval.

## Logging monitoring and audit trails

Intravo logs security-relevant authentication, authorization, administrative, configuration, deployment, data-access, deletion, incident, and vendor-management events appropriate to system risk. Logs include actor, timestamp, source, action, target, and outcome where feasible.

Logs must not unnecessarily contain secrets, full prompts, transcripts, payment details, or other sensitive content. Security telemetry is classified and routed according to the Data Residency and International Transfer Standard.

Critical log pipelines are monitored for delivery failure. Alerts have owners, response procedures, severity, and tested notification routes. Server and cloud security logs are retained for at least one year unless a longer period is required. Endpoint logs are retained for at least six months. Where indexed retention is shorter, protected archival storage is used and restoration is tested.

Datadog is a monitoring and evidence platform, not a substitute for governance, response, or retention. Intravo owns monitor configuration, review, response, data minimization, regional routing, and retained evidence.

## **Incident response and breach notification**

Suspected security or privacy incidents must be reported immediately. Intravo triages, contains, preserves evidence, investigates, eradicates, recovers, communicates, and performs a lessons-learned review proportional to severity.

The incident record identifies the timeline, systems, data, people, regions, customers, vendors, decisions, notifications, containment, recovery, evidence, and follow-up actions. Legal counsel is engaged when appropriate.

Potential personal-data breaches are assessed promptly. Where GDPR applies and notification is required, Intravo supports notice to the competent supervisory authority without undue delay and, where feasible, within 72 hours after awareness. When Intravo acts as a processor, it notifies the controller without undue delay according to contract and law. Notification to affected individuals is based on legal risk thresholds and customer direction.

Intravo tests the incident response plan at least annually and after material changes. High-severity incidents receive a documented post-incident review and tracked corrective actions.

## **Vendor and subprocessor management**

Vendors are risk-assessed before receiving Confidential or Restricted information or becoming a production dependency. Diligence considers security controls, privacy terms, data location, subprocessors, breach duties, retention, deletion, availability, financial viability, sanctions where relevant, and independent assurance such as SOC 2 or ISO certification.

Required contracts, DPAs, BAAs where applicable, Standard Contractual Clauses or other transfer mechanisms, service descriptions, and customer notices are completed before restricted processing begins. A generic agreement does not establish that every product is in scope.

Material vendors and subprocessors are recorded in the vendor register, reviewed at least annually, and monitored for material changes. Current assurance reports and bridge letters are retained. Exit plans address data return, deletion, continuity, credential revocation, and replacement.

## **Business continuity backup and recovery**

System Owners define recovery time and recovery point objectives based on business impact. Backups are encrypted, access-controlled, regionally compliant, monitored, protected from routine production compromise, and tested through restoration.

Intravo maintains continuity and disaster-recovery procedures for critical services, including identity, communications, customer production systems, source control, monitoring, and security operations. Exercises occur at least annually and after significant architectural changes. Test results and corrective actions are retained.

## **Artificial intelligence**

Only approved AI services may process company information. Public, synthetic, or non-identifying content may be used within approved tools. Confidential, personal, customer, or proprietary information requires documented Information Security authorization, a reviewed vendor and data flow, contractual coverage, defined retention, regional compliance, and a business purpose.

AI access is limited to authorized users on compliant devices where the risk requires it. Systems must minimize prompts, prohibit training on Intravo content unless expressly approved, avoid logging sensitive prompt content, validate outputs before use, and prevent model output from taking consequential action without an approved control.

EU-origin data may use AI only when processing, storage, logging, analytics, and support paths meet the Data Residency and International Transfer Standard. If a provider cannot make the required regional commitment, the EU data path must be blocked or served by an approved EU-hosted alternative.

## Retention deletion and legal holds

Data Owners define retention based on business need, contract, law, and risk. Systems implement deletion as a default lifecycle control, not solely as a manual task or a successful completion callback. Retention timers, deletion jobs, backups, archives, caches, and derived data are included.

Legal holds suspend ordinary deletion for specified records. Holds are authorized, documented, access-controlled, reviewed, and released in writing. When a vendor or system is retired, Intravo verifies return or deletion of company data and revokes access.

## Security awareness personnel and acceptable conduct

Workforce members complete security, privacy, incident reporting, phishing, acceptable use, and role-specific training at onboarding and at least annually. Developers and administrators receive training appropriate to their access and responsibilities.

Background screening is performed where lawful, relevant to the role, authorized, and consistent with applicable notice and employment requirements. Confidentiality, acceptable-use, security, and post-employment obligations are documented.

## Exceptions enforcement and review

Policy exceptions must identify the requirement, reason, scope, risk, compensating controls, owner, approval, expiration, and review date. Exceptions do not waive legal or contractual requirements.

Violations may result in access restriction, corrective action, disciplinary action, contract remedies, or legal action, consistent with applicable law.

This manual is reviewed at least annually and after material change. Each review records the version, approver, effective date, changes, affected controls, required training or acknowledgment, and evidence updates.

## Existing policy disposition

Upon formal adoption, this manual governs common requirements that are duplicated across the legacy policy set. Detailed standards and procedures remain separately maintained where operational specificity is needed.

| Existing document                                 | Disposition after adoption                                              |
|---------------------------------------------------|-------------------------------------------------------------------------|
| Information Security Policy                       | Superseded by this manual and detailed standards                        |
| Risk Management Policy                            | Retained as a detailed procedure after terminology alignment            |
| Audit Trail Policy                                | Retained and updated as the Logging Monitoring and Audit Trail Standard |
| Cyber Incident Response Plan                      | Retained and rewritten as an operational plan                           |
| Personal Data Protection Policy                   | Retained and rewritten as the Privacy and Data Protection Standard      |
| Cybersecurity Supply Chain Risk Management Policy | Retained and updated as the Vendor and Subprocessor Risk Standard       |
| Secure Development Policy                         | Retained after control and evidence alignment                           |
| Change Management and Control Policy              | Retained after workflow and evidence alignment                          |
| Vulnerability and Patch policies                  | Consolidated into one standard with separate procedures                 |
| Key Management Policy                             | Retained and updated as the Cryptography and Key Management Standard    |
| Business Impact Analysis Policy                   | Retained with business continuity and disaster-recovery procedures      |

| Existing document                       | Disposition after adoption                                                 |
|-----------------------------------------|----------------------------------------------------------------------------|
| BYOD Policy                             | Rewritten for current MAM and managed-device models                        |
| AI Acceptable Use Policy                | Retained and updated for approved tools, regional processing, and evidence |
| Document Retention Policy               | Retained after schedule and automated-deletion validation                  |
| Wireless Network Security Policy        | Retained as a remote and network access standard                           |
| Code of Conduct                         | Retained with terminology and cross-reference review                       |
| Background Check Policy                 | Retained with jurisdiction-specific employment-law review before screening |
| Infection Prevention and Control Policy | Retained as a separate workplace policy                                    |

## References

- AICPA Trust Services Criteria and SOC 2 resources: <https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2>
- GDPR official text: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- European Data Protection Board international-transfer guidance: [https://www.edpb.europa.eu/topics/international-transfers-and-international-cooperation\\_en](https://www.edpb.europa.eu/topics/international-transfers-and-international-cooperation_en)
- NIST Cybersecurity Framework 2.0: <https://www.nist.gov/cyberframework>
- CIS Benchmarks: <https://www.cisecurity.org/cis-benchmarks>

## Approval record

| Role                                               | Name                   | Decision                                           | Date               |
|----------------------------------------------------|------------------------|----------------------------------------------------|--------------------|
| Company Owner and Information Security Coordinator | Adam Luz               | Approved for publication                           | September 24, 2026 |
| Company Owner and Information Security Coordinator | Adam Luz               | Approved version 2.1 for publication               | October 14, 2026   |
| Legal and privacy review where required            | Case-specific reviewer | Required before a qualifying activity or exception | Per review         |

## Revision history

| Version | Date               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.0     | September 24, 2026 | Consolidated current security, privacy, SOC 2, GDPR, regional-processing, AI, and evidence requirements into one governing baseline                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 2.1     | October 14, 2026   | Revised by Adam Luz, Company Owner and Information Security Coordinator. Adopted Restricted as the highest classification label, retired Highly Confidential, and designated Public, Internal, Confidential, and Restricted as the only classification scheme for all systems, including email and Microsoft 365 sensitivity labels. Reason: the Manual named the highest classification label Highly Confidential while the Asset Management and Data Classification Policy and the compliance portal named it Restricted, and no policy designated the scheme for email; conflicting policy requirements are not acceptable for SOC 2 |