ORDR

ORDR IQ · POLICY

Enterprise AI Security & Confidentiality Policy

Overview

ORDR is committed to delivering AI that meets the highest standards of security, privacy, and enterprise readiness. ORDR IQ works with any large language model that offers enterprise-grade licensing with strong guarantees around data protection, confidentiality, and zero data retention. Customers can bring their own LLM or AI infrastructure and configure it directly through the ORDR UI.

ORDR IQ uses secure, enterprise-grade AI capabilities to deliver intelligence and automation across your environment while keeping your data private, protected, and fully under your control. All AI processing is handled with strict confidentiality, and customer data is never used to train external models.

Security Architecture

Access Control

- Access is restricted to authorized ORDR personnel and designated customer users only
- Integrated Single Sign-On (SSO) with strong identity verification
- Role-based access controls consistent with enterprise governance policies

Infrastructure

- ORDR IQ operates in an isolated private-cloud environment
- Segmented from public-facing networks
- Hosted on enterprise-grade, SOC 2 Type II–certified infrastructure
- Built with industry-standard AI security protocols

© 2026 ORDR, Inc.

Data Protection

Zero Data Retention

- Zero Data Retention (ZDR) is always enabled
- No prompts, responses, or metadata are stored by the AI provider
- No data is used for AI model training —ever

Confidential Processing

- All input is processed in real-time only
- Data is immediately deleted after computation
- No persistent storage of sensitive information
- Data is never shared with third parties or used outside the customer environment

Confidentiality & Compliance Guarantees

Data Lifecycle

- Data exists only during active processing
- Automatic, instant deletion post-processing
- No long-term logging, caching, or replication

Compliance Alignment

- Supports enterprise security and governance frameworks
- Aligns with customer regulatory requirements (HIPAA, PCI, SOX, NERC, etc.)
- Detailed audit logs available for access, usage, and administrative actions

Risk Mitigation Controls

- No exposure to external or unapproved APIs
- End-to-end encrypted data transmission
- Continuous monitoring and security telemetry
- Periodic internal and external security assessments

© 2026 ORDR, Inc.

AI Actions, Access Controls, and Human Oversight

ORDR IQ operates strictly in an advisory capacity and is not authorized to execute actions or make changes to any system.

No Autonomous Actions

IQ cannot independently execute policies, modify configurations, or initiate enforcement actions.

No System Credentials

IQ is not provided with credentials or privileged access to log into ORDR or any external systems to perform actions.

Human Oversight and Control

All decisions and actions remain under explicit human control. IQ may generate policy recommendations, suggest configurations, and provide actionable insights, but cannot implement them.

Manual Policy Implementation

Any policies generated by IQ must be explicitly reviewed, approved, and manually transferred to the ORDR platform by an authorized user for implementation.

THE POWER OF ORDR IQ

ORDR IQ turns deep device intelligence into clear, actionable guidance. By pairing ORDR's visibility into every connected device with enterprise-grade AI, IQ helps security teams understand risk faster, prioritize what matters most, and build effective policies with confidence.

© 2026 ORDR, Inc.