INTERNATIONAL
WELDING BUREAU

IWB SECURITY & COMPLIANCE OVERVIEW - POWERED BY REVCORD

IWB SECURITY & COMPLIANCE OVERVIEW - POWERED BY REVCORD

1. INTRODUCTION

This paper details Revcord's final security posture for government and public-safety customers, replacing all prior versions. It integrates:

- TRG datacenter physical controls and certifications,
- Revcord's zero-trust logical architecture and 320 GB dual-cluster AI capacity,
- Vanta continuous compliance validation and Trust Center transparency, and
- A hardened AI layer using only closed, proprietary LLMs operated on Revcord-owned GPU infrastructure.

2. THE REVCORD SECURITY PLATFORM

Purpose

Protect restricted, confidential, and sensitive data (CJIS, PHI/PII/PCI) while preserving operational efficiency for PSAPs and government agencies.

Employee Requirements

- Security awareness training; adherence to Acceptable Use.
- MFA-protected SSO for all corporate and production access.
- No external email/file sharing for sensitive data; use approved encrypted channels only.
- Device encryption and EDR required for all endpoints.
- Joiner/Mover/Leaver off-boarding with credential revocation and asset return.

Corporate Security Policies and Procedures

- Access Control, Password, Remote Access
- Data Protection & Encryption
- Vulnerability and Patch Management
- Incident Response & Business Continuity / DR
- Vendor & Risk Management
- Audit & Logging; Secure Software Development

Product-Specific Security Protocols

- **RevSync** – TLS 1.2+ transport, encrypted storage, RBAC, tamper-evident logs, tokenized APIs.
- **IQ3** – Encryption at rest, TLS, MFA for admins, role-based permissions, full auditable workflow history.
- **RevCell** – End-to-end encryption, device tokens, inactivity locks, remote wipe, device encryption enforced.
- **RevGuard** – Continuous configuration/health checks, alerting, tamper-evident logs, MFA for admins.
- **RevWatch** – HTTPS+MFA, role-segmented visibility, immutable model/threshold change logs.
- **RevView** – HTTPS playback, export watermarking, granular permissions, session-scoped URLs.
- **MMS (Logger)** – Encryption at rest, TLS services, comprehensive RBAC and audit trails, encrypted backups.

the company's existing alignment under NIST 800-171, CJIS, and HIPAA frameworks.

Continuous monitoring and evidence automation are performed through Vanta, which validates Revcord's internal controls for encryption, access management, endpoint posture, and audit readiness while referencing TRG's certified infrastructure as the hosting boundary of record.

3. ARCHITECTURE

Revcord Data Center and Physical Security (TRG)

Revcord's cloud infrastructure is hosted at TRG Datacenters (Houston) — a modern, audited facility engineered for resilience, security, and uptime. TRG provides the first defensive perimeter (power, cooling, physical access, network diversity), while Revcord layers logical, application, and AI controls above it.

Facility Highlights

- Location: 2626 Spring Cypress Rd., Spring, TX 77388
- Power: Dual-path 2(N+1) with indoor generators; UPS-backed
- Connectivity: 15+ carriers; carrier-neutral cross-connects
- Uptime: Documented 100% track record during recent severe weather events
- Compliance (facility level): FISMA-capable, HIPAA-capable, SSAE/SOC, PCI, NFPA-110

Network & Infrastructure Security

- Tier-4-style redundancy across power/cooling/network
- Edge: FortiGate NGFW with VLAN segmentation (Prod / SecOps-Mgmt / DMZ)
- Cloudflare WAF/DDoS/TLS edge; HSTS enforced
- Core: 10 Gb aggregation, FS3900 switching
- Storage: TrueNAS (ZFS snapshots) + Synology HA clusters for recordings/archives
- AI Clusters: Two GPU clusters totaling 320 GB VRAM (closed-model inference/training)

Physical & Environmental Security

- 24×7 staffing and video surveillance; man-trap options
- Built for 185+ MPH wind loads; outside 500-year floodplain; raised slab
- Intrusion detection, segmented cages/cabinets available

4. Network Ports and Firewalls

All customer-to-Revcord cloud communications are outbound-only from customer networks.
Below tables mirror the final required set.

RevShield / RevGuard

Port	Proto	Service	Description	TLS	Direction
443	TCP	HTTPS	RevGuard API	Yes	Outbound → revwatch.revcord.com
444	TCP	WSS	Remote Control	Yes	Outbound
8441	TCP	WSS	Remote Config	Yes	Outbound
8451	TCP	WSS	Remote Audio	Yes	Outbound

Additional inbound on Logger (from workstations/admin): VodServer 4510; RealTime 4520; Revwsserver (local) 8181; IIS 80 (optional/legacy).

RevShield / RevGuard

Port	Proto	Service	Description	TLS	Direction
443	TCP	RevSync	Websocket	Yes	Outbound → revcloud.revcord.com
8431	TCP	RevSync	Livestream	Yes	Outbound
8441	TCP	RevSync	Secure FTP	Yes	Outbound

MMS, IWB App User, IWB Participants

Port(s)	Proto	Service	TLS	Direction
443	TCP	MMS (Logger)	Yes	Inbound (from user LAN/VPN)
443	TCP	License/3rd party (mt.revcord.com, Zoho, softwarekey)	Yes	Outbound
8181	TCP	MMS (local)	-	Inbound (LAN)
8431/8441	TCP	Websocket/FTP (RevSync)	Yes	Outbound
1935/8086/8087/9443	TCP	Streaming (Wowza)	Mixed	Outbound
10000–20000	UDP	Media (Twilio/Wowza)	Yes	Outbound

RevAgent

MonitorService 10998, DB 1433, FTServer 10999, CTI 4530, FT Server License 11000

5) ENCRYPTION AND SECURE COMMUNICATION

Data Protection: In Transit and At Rest

- TLS 1.2/1.3 everywhere; WSS for real-time streams
- Encrypted outbound SSL telemetry for logs/health/auth
- Encryption at rest for all Revcord-managed environments (CJIS/HIPAA aligned)

DSF + AES-256 Dual-Layer Protection

Layer 1 — Logical (DSF):

- Proprietary Digital Storage Format; unplayable outside Revcord apps
- File-bound hashes; checksum enforcement; DB linkage; tamper-evident

Layer 2 — Physical (AES-256):

- TrueNAS/Synology volume encryption; off-device key vault; annual rotation

Combined Effect: Even if copied, files are unusable (DSF). Even if disks are removed, data is unreadable (AES-256). Meets/exceeds CJIS, NIST 800-171, HIPAA confidentiality/integrity expectations.

Closed, Proprietary LLMs (ReVI)

- ReVI uses only closed, Revcord-controlled LLMs; no public cloud AI or third-party inference.
- All AI runs inside TRG on Revcord GPU clusters (320 GB VRAM total).
- Built on a licensed foundation and fine-tuned by Revcord for PSAP/LE use; updates validated internally; data never leaves custody.
- Automatic redaction (PII/PHI/PCI/CJIS), dual-transcript handling, sentiment/QA aligned to APCO/NENA best practices.

6. REVSYNC & REMOTE OPERATIONS SECURITY

RevSync Security (Outbound-Only)

- Customer logger initiates all sessions (no inbound exposure)
- Outbound ports: 443, 8431, 8441; TLS/WSS enforced
- Triple-redundant storage (primary + mirror + off-site encrypted archive)
- Cloud failover: two-way sync; immediate continuity during local outages

Remote Access: RevGuard / RevWatch

- RevGuard remote viewer never requires inbound openings; connects via secure broker

- Access granted only by CJIS-certified Revcord admins; all sessions audit-logged
- Auto-updates and support actions over encrypted outbound channels

7. COMPLIANCE STANDARDS & VANTA VALIDATION

Frameworks in Scope (Revcord)

- SOC 2 Type II (controls live; external attestation target 2026)
- NIST 800-171 (self-attested; Vanta-validated evidence and SPR readiness)
- CJIS (tech controls; agency addenda in flight)
- HIPAA (BAA available; encryption/redaction controls enforced)
- PCI-DSS (out of scope for storage/processing; vendor reliance as applicable)
- ISO 27001 (ISMS mapped; certification target 2026)

Vanta as a Validation Platform

- Vanta continuously monitors and validates Revcord controls (MFA, EDR, encryption, backups/DR, SIEM coverage, access reviews). Customer-facing Vanta Trust Center provides curated audit artifacts, policies, diagrams, and live posture indicators under NDA.
- Facility Certifications (TRG)
- TRG maintains audited/attested SOC/SSAE, ISO 27001, HIPAA/PCI-capable operations with Tier-style redundancy—forming the physical boundary of trust for Revcord workloads.

8. REVSYNC NETWORK ARCHITECTURE AND DATA FLOW (OVERVIEW)

- Single outbound egress from customer LAN → Revcord Cloud (TRG)
- Two-way RevSync: secure archive/failover; RevWatch for health/alerts
- Remote users access via HTTPS/MFA; media delivered via secured streams

8. FAQ

Can anyone use Revcord to get into my network?

No. We never require inbound access. Support and updates use encrypted outbound brokered sessions with full audit trails.

Where does AI processing occur?

Exclusively inside TRG on Revcord GPU clusters (closed models). No third-party AI providers are used.

Do you encrypt my recordings twice?

Yes. DSF (logical) + AES-256 (storage). Copies are unusable; disks are unreadable.

How do I verify compliance?

Request access to Revcord's Vanta Trust Center for live control status, policies, and reports; ask for TRG certificates applicable to your scope.

10. DISCLAIMER

This document describes Revcord's current security controls. Nothing herein amends any written agreement, SLA, or warranty between Revcord and its customers.