AiDANT Cybersecurity and Data Privacy

AiDANT Intelligent Technology

Unit 125 - 10451 Shellbridge Way, Richmond, BC, V6X 2W8, Canada

1. Authentication & Access Control

At AiDANT Intelligent Technology, we prioritize a "Security by Design" approach. Our applications are deployed as ACAPs, meaning they run natively within the AXIS camera's internal environment. Instead of maintaining a separate, external authentication silo, our software inherits the robust, hardened security framework of the AXIS Edge vault. By relying on AXIS's native authentication and access control protocols, we ensure that your data is protected by the same enterprise-grade standards that govern the hardware itself. This integration eliminates common vulnerabilities associated with third-party software bridges and ensures a single, secure point of management for your security administrators.

Key Access Control Features (AXIS Hardware):

- Encrypted Communication: Support for HTTPS/TLS, ensuring that management sessions and data streams are encrypted from the camera to the client.
- Role-Based Access Control (RBAC): Granular user levels (Administrator, Operator, Viewer) to ensure users only have the permissions necessary for their role.
- Network-Level Defense: Support for IEEE 802.1X (port-based network access control) and IP address filtering to prevent unauthorized devices from communicating with the camera.

- Brute-Force Protection: Built-in mechanisms to delay or block login attempts after multiple failed tries, neutralizing automated password attacks.
- Hardware-Rooted Trust: Use of Secure Boot and Signed Firmware to ensure that only authenticated AXIS software—and by extension, your ACAP—can run on the device.

2. Data Privacy and Encryption

Actionable intelligence should never come at the cost of individual privacy. Our ACAPs are built on a "Privacy by Design" framework, meaning they do not collect, process, or store Personally Identifiable Information (PII).

Our software operates entirely at the "edge" within the AXIS camera environment. When our analytics detect an activity, the system generates a simple event notification rather than transmitting raw video data. For sensitive environments, we offer built-in anonymization tools to mask individuals within the field of view, ensuring total compliance with global privacy standards. Any historical reporting data—such as aggregate people counts or traffic flow—is stored locally on the device as anonymous numerical metadata. This information can be securely accessed via VAPIX or MQTT protocols, but because we only store numbers and never identities, your organization’s data footprint remains lean, secure, and fully private.

- Zero PII Collection: Our applications are engineered to process metadata only. No names, faces, or biometric signatures are ever linked to individuals or stored by the ACAP.
- Edge-Based Processing: Analysis happens entirely on the camera's processor. No raw video or sensitive imagery is transmitted to an external server for processing.
- Event-Driven Notifications: The system only communicates when a specific rule is triggered, sending a notification rather than a continuous stream of data.
- Dynamic Anonymization: Optional privacy masking can be enabled to blur or anonymize individuals within the field of view in real-time.
- Numeric Metadata Storage: Reporting data (such as occupancy levels or people counts) is strictly numerical.
- Secure Transport Protocols: Data retrieval from the camera is handled via VAPIX or MQTT, ensuring industry-standard encryption for all outgoing numbers.

3. Third-Party Protocols

We maintain a strict "Zero-Sharing" policy. Your data should remain exactly that: yours. Our ACAPs are engineered to be self-contained; they do not transmit "telemetry" or metadata back to AiDANT, and we have no technical means to access the information generated on your cameras.

We do not partner with third-party data brokers, and we never monetize the insights generated by our applications. Any integration with external platforms—such as a Video Management System (VMS) or local reporting server—is entirely at the discretion of your internal IT team and is executed through secure, user-defined protocols. When you deploy an AiDANT ACAP, you aren't just getting an intelligent analytics tool; you're getting a closed-loop system where data privacy is enforced by architecture, not just by promise.

- No Third-Party Sharing: We do not sell, trade, or share any metadata or event logs with outside vendors, partners, or advertisers.
- Total Data Sovereignty: All data generated by our ACAPs belongs exclusively to the end user and remains within their managed network.
- No "Phone Home" Features: Our applications do not maintain background connections to AiDANT servers or third-party cloud environments for data harvesting.
- Decentralized Architecture: Because our software runs at the edge, there is no centralized AiDANT database where user information is stored or accessible to our staff.
- Customer-Controlled Integrations: Any data transmission to third-party systems (like a VMS or an MQTT broker) is explicitly configured and controlled by the user, not AiDANT.

4. Vulnerability Management

We believe that security is synonymous with control. Our ACAP software is engineered to be Internet-Independent, meaning it can operate in a strictly offline or LAN-only environment without any loss of core functionality. This architecture ensures that your security network remains isolated from the public internet and protected from remote external threats.

Furthermore, we do not utilize "Push" or automatic updates. We recognize that in professional security environments, software changes must be predictable and scheduled. Therefore, the responsibility for software maintenance lies with the user. All security patches and feature enhancements must be manually downloaded and installed by an authorized administrator. This "Pull-only" update model ensures that no code enters your network without your explicit action and oversight, allowing for rigorous change-management protocols.

- Internet Independence: Our ACAPs are designed to function entirely within a Local Area Network (LAN). No external internet connection is required for the software to operate, analyze data, or trigger events.
- No Automatic Updates: To ensure system stability and prevent "surprise" changes to your security environment, our applications never update automatically.
- User-Initiated Maintenance: The end user retains full sovereignty over the software versioning. Updates must be manually downloaded from our secure portal and uploaded to

the AXIS camera via the standard management interface.

- Reduced Attack Surface: By eliminating outbound "phone-home" update checks, we significantly reduce the potential attack vectors usually associated with IoT and edge software.

5. Regulatory Alignment

AiDANT Intelligent Technology is an agile, edge-focused organization, our software is built from the ground up to align with the core principles of global privacy frameworks such as GDPR, CCPA, and HIPAA.

- Data Minimization (GDPR/CCPA): Our ACAPs strictly adhere to the principle of data minimization. By processing all analytics at the edge and storing only anonymous numerical metadata, we ensure that no Personally Identifiable Information (PII) is ever generated or transmitted.
- Privacy by Design: Our "LAN-only" and "No-PII" architecture means that your organization can deploy our analytics in highly regulated environments without expanding your compliance footprint or triggering complex Data Processing Agreements (DPAs).
- HIPAA & Sensitive Environments: Because our software can be configured to anonymize individuals in real-time and does not store video or patient records, it is ideally suited for healthcare environments where patient privacy is paramount.
- Sovereignty & Control: Unlike cloud-based AI providers, AiDANT never has access to your data. You retain 100% sovereignty over your information, which is a key requirement for SOC2 and ISO 27001 internal audits.

Note: AiDANT provides the technical tools to maintain a compliant environment; however, the end user remains responsible for ensuring their overall deployment meets specific local legal requirements.

6. Reporting a Concern

If you discover a potential vulnerability or suspect a security issue related to an AiDANT ACAP, please contact our technical team immediately. Reports should be submitted via our Technical Support Form at: http://AiDANT.ai/contact

Our Response Process

- Acknowledgment: Upon receiving a report, our security team will acknowledge receipt within 24–48 business hours.

- Investigation & Validation: We will conduct a thorough internal review to determine the scope and impact of the reported issue.
- Remediation: If a vulnerability is confirmed, we will develop a software patch.
- Communication: Since our software does not "phone home," we cannot push updates automatically. We will notify registered administrators of the availability of a critical update via email and our official website, providing clear instructions for manual installation.

We believe in "Responsible Disclosure" and work closely with our partners and customers to ensure that any security findings are addressed before they can be exploited.

7. User Best Practices for Maximum Security

Physical & Hardware Hardening

- Physical Access Control: Ensure cameras are mounted at heights or in housings that prevent physical tampering with the SD card or reset button.
- Cable Protection: Use conduits for all cabling to prevent unauthorized "man-in-the-middle" physical network taps.

Account & Authentication Hygiene

- Unique Credentials: Never use default passwords. Use unique, complex passwords for every camera (minimum 12–15 characters, following NIST/AXIS OS 13 complexity standards).
- The Principle of Least Privilege: Create a specific "Operator" or "Viewer" account for daily monitoring. Reserve the Root/Admin account strictly for software updates and configuration changes.
- Rename the Admin Account: If the firmware allows, rename the default "root" account to something non-obvious to thwart brute-force scripts.
- Network Configuration (The LAN Environment)
  VLAN Segmentation: Place all security cameras and AiDANT ACAPs on a dedicated, isolated VLAN separate from the general office or guest Wi-Fi traffic.
- Disable Discovery Protocols: Since your system is LAN-only, disable UPnP, mDNS (Bonjour), and SNMP (unless active monitoring is required) to make the cameras "invisible" to unauthorized scanning tools.
- NTP Time Sync: Even in an offline LAN, ensure your cameras are synced to a local NTP server. Accurate timestamps are critical for the integrity of AiDANT's event logs and reporting data.
- Proactive Maintenance
  Firmware Lifecycle: Regularly check the AXIS website for "Long-Term Support" (LTS)

firmware tracks. Only install Signed Firmware to ensure the hardware's root-of-trust remains intact.

- Audit Log Reviews: Monthly, export and review the camera’s internal access logs to ensure no unauthorized login attempts have occurred.