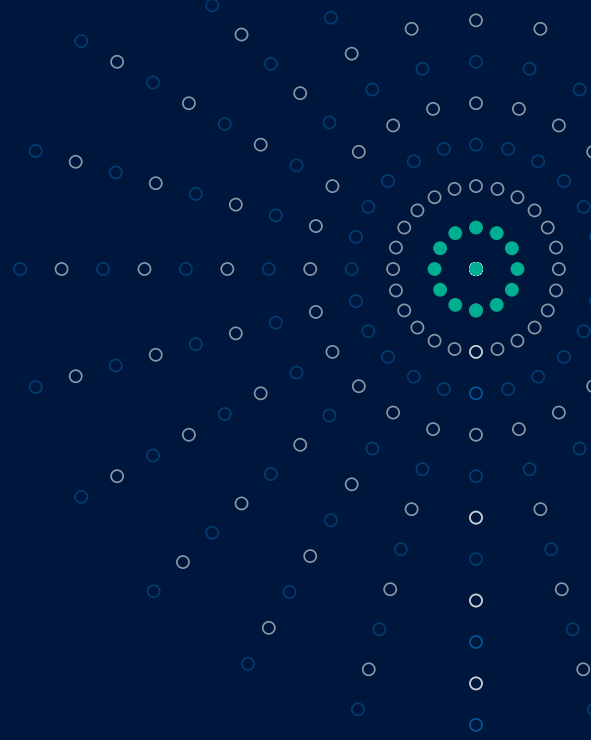




MASTER SPECIFICATION

YourSixOS

Master A&E Specification

Unified direct-to-cloud physical security platform

PROJECT NAME

PROJECT LOCATION

REVISION

September 2026

WE'VE GOT YOUR BACK.

PART 1

General

1.1 System description

A. General requirements

1. The specified solution shall be a commercially available, manufacturer-supported Physical Security as a Service (PSaaS) platform designed for commercial and industrial 24/7/365 use.
2. The platform shall provide centralized, cloud-managed physical security functions from a single software environment, including video surveillance, access control, IP audio, sensors, peripherals/I/O, analytics, health monitoring, event management, and professional monitoring integrations.
3. The platform shall use a direct-to-cloud architecture and shall not require an onsite application server, VMS server, database server, or cloud gateway appliance for normal supported device connectivity.
4. The platform shall support geographically distributed organizations, sites, devices, users, identities, credentials, events, and recordings from a centralized browser-based interface.
5. The solution shall support cloud, edge, and hybrid recording architectures for supported video devices.
6. The platform shall be YourSixOS by YourSix, Inc., or an approved equal meeting all requirements of this specification.

B. Related requirements

1. 28 05 00 - Common Work Results for Electronic Safety and Security.
2. 28 05 11 - Cyber Security Requirements for Electronic Safety and Security.
3. 28 05 19 - Storage Appliances for Electronic Safety and Security; 28 05 21 - Network Attached Storage for Electronic Safety and Security; and 28 05 23 - Storage Area Network for Electronic Safety and Security, where applicable.
4. 28 20 00 - Electronic Surveillance; including applicable video surveillance, analytics, and interface requirements.
5. 28 10 00 - Electronic Access Control and Intrusion Detection, where access control is included. Coordinate IP audio, sensors, I/O/peripherals, and monitoring interfaces with applicable Division 28 project sections.

1.2 Abbreviations and acronyms

ACAP	AXIS Camera Application Platform	API	Application Programming Interface
DNS	Domain Name System	FPS	Frames Per Second
HTTPS	Hypertext Transfer Protocol Secure	I/O	Input/Output
MFA	Multi-Factor Authentication	NTP	Network Time Protocol
OAK	Owner Authentication Key	OSDP	Open Supervised Device Protocol
PSaaS	Physical Security as a Service	PTZ	Pan/Tilt/Zoom
REX	Request-to-Exit	SAML	Security Assertion Markup Language
SLA	Service Level Agreement	SOC	System and Organization Controls
SSO	Single Sign-On	TLS	Transport Layer Security
VMS	Video Management System	WebRTC	Web Real-Time Communication

1.3 Quality assurance

1. Installing contractor or security subcontractor shall be qualified to install and service IP-based physical security systems of similar scope and complexity.
2. Installation, configuration, programming, and commissioning shall be performed by personnel trained on the specified platform and supported endpoint devices.
3. Software provider shall maintain a production service level commitment of 99.99% uptime.
4. Software provider shall maintain a current SOC 2 Type 2 attestation and shall conduct independent security audits and penetration testing as part of its cybersecurity program.

1.4 Software, support, and updates

1. Platform software updates, feature updates, cybersecurity patches, and supported device management capabilities shall be provided for the duration of an active subscription.
2. The cloud platform shall not require customer-managed application software, databases, or thick-client software for browser-based administration and operation.

3. Manufacturer support shall be available for active subscriptions in accordance with the provider's current support policies.
4. Supported endpoint firmware shall be remotely manageable, and the platform shall provide firmware/patch management functions for supported devices.
5. The software provider shall maintain a publicly accessible platform changelog/version archive documenting material software releases, feature changes, and platform updates. Customers and partners shall have a means to subscribe to applicable update communications.
6. The software provider shall maintain a publicly accessible service-status page providing current operational status, incident and maintenance communications, historical uptime information, and a means to subscribe to service-status updates.

1.5 Submittals

1. Product data sheets and current supported-device documentation.
2. Network and firewall requirements, including required outbound connectivity and FQDN allowlisting guidance where applicable.
3. System architecture and recording design identifying cloud, SD card, NAS, or hybrid recording locations.
4. Access control door/barrier schedule where access control is included.
5. Sensor and gateway schedule where sensors are included.
6. Subscription schedule identifying Base Device Subscriptions, cloud storage subscriptions by stream and retention period, and any solution-specific subscriptions.
7. Training and commissioning plan.

PART 2

Products

2.1 Unified physical security platform

A. Manufacturer and platform

1. Platform: YourSixOS.
2. Architecture: direct-to-cloud, serverless/cloud-managed PSaaS with limited onsite infrastructure beyond supported endpoint devices, networking, and optional edge/NAS storage.
3. The platform shall provide multi-tenant capabilities suitable for integrators, enterprise organizations, and professional monitoring workflows.
4. Customer accounts, users, and sites shall support scalable deployment; user access shall be governed by role/scope and granular permissions.

2.2 Compatible products and device connectivity

A. Supported endpoint categories

1. AXIS network cameras, including supported fixed, PTZ, multisensor, panoramic, modular, and thermal devices.
2. Supported AXIS video door stations.
3. Supported AXIS network speakers and audio devices.
4. Supported AXIS door controllers, including A1210, A1610, and A1601 models meeting current minimum firmware requirements.
5. Supported system devices including I/O/relay modules, radar products, encoders, recorders, gateways, and peripherals.
6. Supported native environmental sensors, including AXIS D63-series devices, and supported Modbus RTU sensors through a compatible gateway.

B. Connectivity

1. Primary cloud communications shall use outbound TCP port 443 and DNS. No inbound port forwarding or NAT rules shall be required for normal operation.
2. Peer-to-peer video streaming shall use WebRTC where available; outbound UDP ports 30000-40000 shall be permitted when P2P streaming is required.

3. Basic proxy support shall be available. Required platform FQDNs shall be allowlisted when outbound network traffic is filtered.
4. Recommended upload bandwidth shall be a minimum of 0.5 Mbps dedicated per camera for cloud storage and viewing, subject to actual scene, stream, and use requirements.
5. Supported devices shall meet the minimum AXIS OS/firmware requirements published by YourSix.

2.3 Client and user interface requirements

1. Administrative and end-user access shall be browser based using current supported versions of Google Chrome, Mozilla Firefox, or Microsoft Edge.
2. The web client shall not require a locally installed thick client for standard platform operation.
3. The platform shall support current supported Microsoft Windows and macOS environments in accordance with manufacturer support policies.
4. Native mobile applications shall be available for supported Android, iPhone, and iPad devices.
5. Mobile applications shall support current supported Android and iOS versions and shall be available through the applicable public application stores.
6. The web platform shall support centralized navigation across organizations, sites, devices, video, barriers, peripherals, sensors, events, and alarm groups.
7. Native mobile applications for supported iOS and Android devices shall provide authorized users secure remote access to applicable YourSixOS functionality.
8. Mobile functionality shall include live video viewing, recorded-video playback, video export, mechanical and digital PTZ control, site and device health monitoring, notifications including mobile push notifications, I/O control, and audio talkdown.
9. The mobile application shall provide a feedback function capable of supplying application logs to YourSix Technical Support for troubleshooting.
10. Mobile application users shall maintain a current supported application version. When an application update is available, it should be installed within two weeks to maintain proper application functionality.

2.4 Cybersecurity, data protection, and business continuity

A. Compliance and assurance

1. The software provider shall maintain a current SOC 2 Type 2 attestation.

2. The software provider shall perform penetration testing at least annually. A remediation plan shall be developed and changes implemented to remediate identified vulnerabilities in accordance with established service-level commitments.
3. The software provider shall perform control self-assessments at least annually to gain assurance that controls are in place and operating effectively, with corrective actions taken for relevant findings.
4. The software provider shall perform risk assessments at least annually. The assessment process shall identify relevant environmental, regulatory, and technological threats and changes, formally assess associated risks, and consider the potential for fraud.
5. The software provider shall maintain a documented risk-management program addressing identification of potential threats, assessment of the significance of identified risks, and mitigation strategies.

B. Access and infrastructure security

1. Access to production applications and systems shall be restricted to authorized personnel.
2. User access to in-scope system components shall be based on job role and function or require a documented access request and manager approval prior to provisioning.
3. The software provider shall maintain documented access-control procedures governing the addition of new users, modification of existing users, and removal of user access.
4. Authentication to applicable systems, applications, and production network resources shall use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.
5. Remote access to production systems shall be limited to authorized personnel using a valid multi-factor authentication (MFA) method.
6. Remote access to production systems shall use an approved encrypted connection.
7. The software provider shall use network firewalls configured to prevent unauthorized access.
8. The software provider shall maintain processes for granting, changing, and terminating physical access to company data centers based on authorization from control owners.
9. Access to data centers shall be reviewed at least annually.

C. Data protection and privacy

1. Platform and customer data shall be encrypted in transit and at rest as applicable to the service architecture.

2. The software provider shall maintain formal data-retention and disposal procedures governing the secure retention and disposal of company and customer data.
3. The software provider shall purge or remove customer data containing confidential information from the application environment, in accordance with established procedures and best practices, when customers leave the service.
4. The software provider shall maintain a data-classification policy designed to ensure confidential data is appropriately secured and restricted to authorized personnel.
5. Portable and removable media shall be encrypted when used for company information.
6. Electronic media containing confidential information shall be securely purged or destroyed in accordance with established procedures and best practices.

D. Incident response and business continuity

1. The software provider shall maintain documented security and privacy incident-response policies and procedures and communicate them to authorized personnel.
2. The software provider shall maintain Business Continuity and Disaster Recovery plans, including communication plans intended to maintain information-security continuity during the unavailability of key personnel.
3. Management roles and responsibilities for the design and implementation of information-security controls shall be defined.
4. Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information-security controls shall be formally assigned.

E. Security commitments and governance

1. The software provider's security commitments shall be communicated to customers through applicable contractual documents, including Master Service Agreements (MSA) or Terms of Service (TOS).
2. The software provider shall maintain defined objectives supporting the identification and assessment of risks related to its service commitments.

2.5 Live video and viewing

1. Live view shall support single-camera, split-view, full-screen, and multi-view configurations.
2. Live view shall support up to 20 cameras or up to 40 supported widgets, subject to viewing-station performance and configuration.

3. Supported live actions shall include device-dependent mechanical/digital PTZ, PTZ presets, digital zoom, I/O control, live talkdown, microphone control, snapshots, resolution controls, lens wiper controls, barrier controls, and peripheral controls.
4. Live video shall support H.264 (MPEG-4 Part 10/AVC) with AXIS Zipstream where supported.
5. Live resolution shall be device dependent, with support up to 4K for applicable devices.
6. Remote/cloud and direct peer-to-peer live streaming shall support up to 8 fps under the current platform specification.
7. Manual or automatic stream-quality selection shall be available to balance bandwidth and image quality.
8. AXIS Corridor Format and supported panoramic/dewarped views shall be supported where applicable to the device.
9. The platform shall support secure WebRTC peer-to-peer (P2P) live video streaming between supported endpoint devices and viewing clients.
10. Where a direct P2P connection can be established, live video shall be capable of traveling directly from the endpoint device to the viewing client without requiring the live stream to traverse the YourSixOS cloud.
11. When the endpoint device and viewing client are on the same network and network configuration permits direct communication, P2P streaming shall be capable of maintaining the live video stream locally.
12. The platform shall automatically determine whether a direct P2P or cloud streaming path is available. If a P2P connection cannot be established or is interrupted, the platform shall automatically fall back to cloud streaming to maintain live video access.
13. The user interface shall identify when an applicable live video stream is using a P2P connection, and users shall have the ability to force an applicable stream through the YourSixOS cloud.
14. P2P streaming shall support Standard quality at approximately 720p, or the closest resolution supported by the device, and High quality at approximately 1080p, or the closest supported resolution, at 8 frames per second. Additional available device resolutions may be accessed through cloud streaming.
15. Use of P2P live streaming shall not alter or interrupt configured video recording. Recording shall continue independently of the live-video delivery path.
16. Successful P2P operation shall be subject to the WebRTC and network requirements specified in Section 2.20, Network Architecture and Dataflows.

17. The platform shall be designed for low-latency interaction with connected devices to support responsive live operations, including live video, PTZ control, audio talkdown, peripheral control, and other interactive functions.
18. Actual end-to-end latency shall be dependent on endpoint-device, network, Internet, and client conditions and shall not be represented as a fixed guaranteed latency unless separately stated in a project-specific service commitment.

2.6 Recording and storage

A. Recording architecture

1. Cloud recording shall be optional and licensed/subscribed per recorded video stream.
2. Edge recording shall support compatible SD card and/or NAS storage based on device capability and configuration.
3. Hybrid designs shall permit different recording locations and policies as required by the project.
4. Recording modes shall include continuous, schedule-based, motion/analytic/event-triggered recording as supported by the configured device and application.
5. Cloud recording shall support up to 720p or equivalent at up to 8 fps.
6. Edge recording shall support device-dependent resolution up to 4K and frame rates up to 30 fps.
7. Cloud video shall upload directly from supported devices to the cloud without requiring an onsite VMS recording server.

B. Retention

1. Cloud storage retention packages shall include 3, 7, 14, 30, 60, 90, 120, 180, 365, and 730 days, subject to currently offered subscriptions.
2. Edge retention shall depend on available storage capacity, scene activity, recording configuration, resolution, frame rate, and compression.
3. Retention shall be configurable by camera/stream as permitted by the subscribed storage option and recording design.

2.7 Playback, search, and export

1. Users shall be able to search recordings by device, date, time, and event type; events and recordings shall be represented on the playback timeline.
2. Playback shall support viewing recordings from up to 20 cameras, subject to client performance and recording configuration.

3. Cloud playback resolution shall correspond to the cloud recording configuration and shall be limited to the supported cloud recording specification.
4. Search shall include supported event, object, and access-event criteria across a selected timeframe and device set.
5. Object event search shall support people and vehicles and supported appearance attributes such as color and vehicle class when compatible analytics and devices are deployed.
6. Export shall support multiple video clips from up to eight cameras for a period of up to 24 hours.
7. Exports shall use MP4 video packaged in a ZIP container.
8. The software provider shall provide a validation utility for supported video exports that allows a recipient to check the authenticity and integrity of the exported video file.

2.8 Video analytics

1. The platform shall ingest and use supported AXIS edge-based analytics and ACAP-generated events.
2. Supported analytic events may include people/vehicle detection, motion, intrusion/crossline, loitering, audio detection, tampering, and other device-supported analytic events.
3. Analytics shall be usable as event sources for search, notifications, recording workflows, and other supported platform actions.
4. Where supported, object search shall allow investigation of human and vehicle events using available attributes.
5. Third-party or manufacturer-provided ACAP applications shall be supported only where specifically validated by YourSix and the endpoint manufacturer.
6. Object Appearance Search (OAS) shall provide forensic search across supported cameras and selected time ranges for human and vehicle appearances.
7. Supported OAS search criteria shall include object class (human or vehicle), vehicle class (car, truck, bus, or bike), vehicle color, and human upper- and lower-body clothing color.
8. OAS results shall be presented as thumbnails with timestamp, confidence score, and applicable appearance attributes. Users shall be able to open a result for an enlarged view, view associated video in the Matrix when a recording exists, and search for similar appearances.

9. OAS shall provide an adjustable confidence-score threshold, with higher settings applying stricter class and color matching.
10. OAS-capable devices shall use a supported system-on-chip, including ARTPEC-8, ARTPEC-9, or CV25, shall run AXIS OS 11.11 or newer, and shall contain an SD card. OAS may use up to 5 percent of the device SD card.
11. OAS shall be enabled as an Optional Feature on compatible devices by a user with integrator-level scope or permissions. Organization-level users shall not be permitted to enable the feature.
12. Object Appearance Search metadata shall be stored locally on the device and shall not be considered a substitute for video recording.
13. A recording rule shall be configured when OAS results are expected to link to saved video. OAS results may exist without corresponding recorded footage where recording rules, analytic triggers, or include/exclude areas did not cause the associated video to be recorded.

2.9 Access control

1. Access control shall be cloud managed within the same platform used for video, audio, sensors, peripherals, events, and monitoring.
2. Supported controllers shall include AXIS A1210, A1610, and A1601 models meeting current platform firmware requirements.
3. Reader interfaces shall support Wiegand and OSDP v2 as supported by the controller/reader design.
4. Credentials shall support compatible cards/fobs and PIN entry. Mobile credentials shall support Bluetooth on iOS and supported mobile credential methods on compatible devices.
5. The system shall support up to 10,000 identities per organization under the current published platform specification.
6. Authentication methods shall include card-only, card plus PIN, and Request-to-Exit (REX), as applicable.
7. Administrators shall configure identities, credentials, schedules, access rules, barrier groups, identity groups, and authentication profiles.
8. Authorized users shall be able to remotely lock, unlock, grant temporary access to, and view the physical state of supported barriers.
9. Real-time access events and alarms shall include access granted, access denied, barrier forced open, barrier held open too long, and supported barrier status changes.

10. Access events shall be correlatable with video and usable in event search and notification workflows.
11. Automated lockdown capabilities shall be supported where configured and applicable.

2.10 IP audio

1. Supported IP audio devices shall be managed from the unified platform.
2. Two-way audio shall be supported on compatible devices; audio compression shall use AAC where applicable.
3. Live talkdown shall permit authorized users or monitoring operators to transmit announcements to supported speakers.
4. Audio recording shall be optional and device/configuration dependent.
5. Live and recorded audio shall be capable of being disabled to conform to applicable legal or policy requirements.
6. Supported audio events shall be available for event and notification workflows.

2.11 Peripherals and I/O

1. The platform shall support compatible network-connected I/O, relay, strobe, and auxiliary devices.
2. Authorized users shall be able to control supported peripheral states, including on, off, pulse, or toggle actions as applicable.
3. External I/O and peripheral events shall be usable as event triggers.
4. Supported event responses shall include output activation, video recording, notifications, and audio actions where configured.

2.12 Sensors

1. The platform shall support native sensors, including supported AXIS D63-series devices, and Modbus RTU sensors through a compatible gateway such as the AXIS A9210.
2. Sensor measurements shall be based on the capabilities of the connected sensor and may include environmental, operational, utility, power, air-quality, temperature, humidity, and other supported measurements.
3. Users shall be able to view live sensor values and historical sensor data.
4. Sensor data shall be viewable as gauges and/or historical graphs as supported by the user interface.

5. Sensor events and notifications shall support configurable minimum and maximum threshold conditions.
6. Sensor events shall integrate with the platform's broader event, notification, and investigation workflows.

2.13 Events, notifications, and alarm groups

1. Event sources shall include supported video analytics, audio detection, tampering, access control, peripherals/I/O, sensors, and device-health conditions.
2. Event sources shall be selectable from individual devices, device groups, and devices at one or more sites as supported.
3. Notifications shall support configurable weekly schedules.
4. Notification recipients shall include platform users, organization email addresses, webhooks, and supported central monitoring stations.
5. Delivery methods shall include email, mobile push notification, and webhooks as applicable to recipient type.
6. Alarm Groups/device groups shall support armed, disarmed, and schedule-based states.
7. Authorized end users and supported central station operators shall be able to arm and disarm Alarm Groups within their respective applications/permissions.
8. Event logs shall provide records of supported alarms and events for investigation and audit.

2.14 Health monitoring, device management, and firmware

1. The platform shall provide centralized cloud-based device management, including configuration management, automated firmware management, automated analytics/application management where supported, health monitoring, and cybersecurity hardening.
2. Native health monitoring shall provide operational status information for connected devices and storage resources.
3. Advanced Health Monitoring shall support proactive events for applicable conditions including CPU overutilization, network packet loss, RAM overutilization, and storage-full conditions when the corresponding Optional Features are enabled.
4. Image Health Analytics shall support proactive detection of applicable image-quality conditions including image blur, obstruction or blocked view, camera movement or shift, and poor lighting on compatible devices.

5. Image Health Analytics shall require compatible hardware and software, including supported ARTPEC-8 or ARTPEC-9 devices running AXIS OS 12 or newer, and shall be enabled on applicable devices in accordance with current YourSixOS requirements.
6. Health conditions shall be communicated as security events. Where personnel are expected to receive alerts, applicable notification rules shall be configured for the desired recipients and health events.
7. The platform shall provide fully automated firmware management for supported devices. Firmware management shall be included as part of the YourSixOS software stack and shall not require administrators to manually locate, download, and install firmware on each endpoint.
8. Automated firmware management shall use verified cloud delivery to keep compatible devices current with supported firmware and cybersecurity updates while minimizing operational disruption.
9. Firmware updates and cybersecurity patches shall be included with the applicable Base Device Subscription.

2.15 Professional monitoring and central station integration

1. The platform shall provide first-class support for professional central station monitoring and shall support alarm investigation without requiring a traditional onsite alarm panel for supported workflows.
2. The platform shall support a native central station application, YourSixOS Inspect, providing authorized operators access to applicable alarm-investigation resources including live video, recorded video playback, peripheral control, sensor visualization, speaker callouts, and other supported evidence and response functions.
3. Inspect shall be launchable from a pre-signed callback URL included with applicable central station event notifications.
4. Central station event notifications shall be delivered using HTTPS POST webhooks with the event serialized as JSON. Applicable central station webhook payloads shall include a central station account identifier and a callback URL to the associated Inspect investigation.
5. The platform shall provide a dedicated Central Station API (CSI API) for approved central station integrations. The CSI API shall provide authorized integrations access to applicable resources including sites, devices, events, video streams, and other supported resources required for alarm investigation and response.
6. Central station software shall be capable of integrating by launching the native YourSixOS Inspect application and/or, for approved integrations, providing its own investigation workflow using the Central Station API.

7. Central station integration access shall be limited to central stations approved by YourSix. YourSix shall authorize applicable integrator and central station relationships, after which an authorized integrator shall be able to grant the central station access to specific customer sites.
8. Where supported by the integration and authorized site access, central station operators shall be capable of performing supported response actions available to the central station application, including applicable Alarm Group state management, peripheral control, barrier control, video investigation, and audio/speaker actions.

2.16 API, webhook, and third-party integration

1. YourSixOS shall support third-party event-driven integration using HTTPS webhooks. Organization webhooks shall be available as notification recipients for compatible security events.
2. The platform shall provide a dedicated Central Station API for authorized central station integration partners. The Central Station API shall not be represented as an unrestricted general-purpose public API for customer or do-it-yourself integrations.
3. Access to the Central Station API and central station integration suite shall be limited to approved strategic integration partners in accordance with YourSix authorization requirements.
4. Central station webhooks and API integrations shall use secure HTTPS communications.
5. Third-party integration scope, supported resources, authentication requirements, and available API operations shall be validated against current YourSixOS technical and API documentation at the time of system design and integration.

2.17 System scalability and account management

1. The platform shall support unlimited customer accounts, unlimited sites per account, and unlimited users with individual permissions, subject to fair-use policies and platform terms.
2. Administrators shall be able to add, update, suspend, and manage accounts and users according to assigned permissions.
3. Permissions shall support organization, site, device, device-group, and platform-function granularity as supported by the current platform.
4. The system shall support multi-site and geographically dispersed deployments without requiring a central onsite server.

2.18 Subscriptions

1. Each managed endpoint device shall require the applicable YourSixOS Base Device Subscription unless otherwise defined by the current subscription policy.
2. The Base Device Subscription shall provide platform access and core features such as device management, software updates, cybersecurity patches, health monitoring, SSO/MFA, mobile access, and supported analytics, excluding optional cloud video storage.
3. Cloud video storage shall be an optional subscription applied per recorded stream and selected retention period.
4. Certain solutions, including sensors and other specialized functions, may require additional subscriptions based on device type and functionality.
5. Subscription quantities shall account for multisensor devices, audio devices, barriers, sensor gateways/sensors, radar, and other endpoint types according to current YourSix subscription rules.

2.19 Data residency and regional availability

A. Cloud infrastructure

1. The platform shall be operated using Amazon Web Services (AWS) cloud infrastructure.
2. Backend applications shall be operated regionally from the United States and may use content delivery networks (CDNs) to accelerate global application access.
3. In each AWS region in which YourSixOS maintains a presence, platform operations shall span a minimum of three AWS Availability Zones (AZs).

B. Cloud recording data residency

1. Cloud recording storage shall support regional storage within the United States and Canada in accordance with the YourSixOS regional architecture.
2. The YourSixOS application region shall include AWS us-east-1 under the current documented architecture.
3. United States cloud recording storage shall use supported AWS regions including us-east-1 and us-west-2.
4. Canadian cloud recording storage shall use the AWS ca-central-1 region.
5. The system design shall use the appropriate cloud recording storage region based on the organization's configured YourSixOS presence and applicable project data-residency requirements.

6. Cloud recording storage residency requirements shall not be interpreted to mean that all YourSixOS backend applications or application data are hosted in the same country as cloud recordings.
7. Project-specific data-residency and regional requirements shall be confirmed against current YourSixOS documentation during system design and commissioning.
8. Where a specific cloud recording storage region is required, the project DNS architecture shall use a DNS resolver located within the intended YourSixOS storage region. The regional endpoint used for cloud recording upload is determined based on the location from which the applicable DNS query originates.

2.20 Network architecture and dataflows

A. Device network requirements

1. YourSixOS-managed endpoint devices shall not require inbound port forwarding or inbound Network Address Translation (NAT) configuration for normal platform operation.
2. Device communications with YourSixOS cloud services shall use outbound traffic. Primary YourSixOS device-to-cloud communications shall use HTTPS over TCP port 443.
3. Devices shall support the network connectivity required for WebRTC streaming, including STUN over UDP port 3478 and outbound UDP ports 30000–40000 where required.
4. Axis device enrollment shall support connectivity to the AXIS O3C Dispatcher over TCP port 443 in accordance with current YourSixOS network documentation.
5. Devices shall maintain accurate system time using NTP over UDP port 123. Where an NTP server is announced by DHCP, the DHCP-announced NTP server shall take precedence.
6. The project network shall provide appropriate IP addressing and DNS configuration. Where devices and viewing clients are separated across VLANs or subnets, required WebRTC UDP traffic shall be permitted between applicable networks to support streaming.

B. Application and integration network requirements

1. Web and mobile application connectivity shall use trusted YourSixOS application paths within the yoursix.com domain. The software provider shall not be required to maintain a fixed permanent list of individual application endpoints.

2. Outbound YourSixOS webhooks shall use secure HTTPS communications. Firewall and allow-list requirements for webhook delivery shall be configured in accordance with the current YourSixOS Network Dataflows documentation.
3. Current firewall, FQDN, protocol, and port requirements shall be validated against the then-current YourSixOS Network Dataflows documentation during system design, commissioning, and material network changes.
4. For system planning, the project network should provide a minimum of 0.5 Mbps of dedicated upload bandwidth per camera where cloud storage and/or cloud viewing is required, subject to project-specific camera configuration, recording mode, scene activity, resolution, codec, and viewing requirements.
5. The platform shall support bandwidth-management approaches including edge recording, motion- or analytic-triggered recording, Axis Zipstream on compatible devices, and peer-to-peer live streaming where available.
6. Published bandwidth-consumption examples shall be treated as planning guidance rather than guaranteed per-camera utilization because actual bandwidth varies based on scene activity, device configuration, recording behavior, and network conditions.

PART 3

Execution

3.1 Installation

1. Contractor shall follow current YourSix and endpoint-manufacturer installation, network, firmware, and commissioning documentation.
2. All endpoint devices shall be installed, powered, networked, and configured in accordance with manufacturer requirements and the approved system design.
3. Supported firmware shall meet the minimum versions specified by YourSix at time of commissioning.
4. Default device passwords shall not remain in service. Device onboarding and credentials shall follow the platform's secure device-dispatch and credential-management process.
5. Network configuration shall provide required DNS and outbound connectivity to YourSixOS. Inbound port forwarding shall not be configured solely for YourSixOS operation.
6. Where WebRTC peer-to-peer streaming is required, firewall policy shall permit the applicable outbound UDP traffic.
7. Cloud, edge, and NAS recording shall be verified against the approved recording schedule and retention design.
8. Access control barriers, readers, REX devices, locks, schedules, identities, credentials, and alarms shall be tested where included.
9. Audio, sensors, peripherals, alarm groups, notifications, and central-station workflows shall be tested where included.
10. Installation shall comply with applicable electrical, low-voltage, life-safety, privacy, and building-code requirements.

3.2 Commissioning and acceptance testing

1. Verify user authentication, MFA/SSO where specified, role/scope permissions, and site/device access.
2. Verify all supported live actions.
3. Verify each configured recording destination, playback, search, and export workflow.

4. Verify event generation and notification delivery for representative video, access, sensor, peripheral, health, and tamper events included in scope.
5. Verify access-control grant/deny behavior, schedules, alarm conditions, and remote barrier controls.
6. Verify sensor live values, historical data, and configured threshold events.
7. Verify professional monitoring/central station workflows where included.
8. Document any project-specific exceptions, unsupported functions, or device-dependent limitations before acceptance.

3.3 Training

1. Software provider and/or qualified integrator shall provide operations and administration training appropriate to the project scope.
2. Where included, training shall also cover access control, audio/talkdown, sensors, peripherals, Alarm Groups, and professional monitoring workflows.
3. Training materials may include YourSix Academy, documentation, recorded training, and project-specific instruction.
4. The software provider shall provide access to an online training and education platform for integrators, administrators, and end users. Training resources shall include self-paced courses covering applicable platform operation, administration, configuration, and solution capabilities.
5. End-user and administrator training resources shall address applicable workflows including platform navigation, Matrix live viewing, Forensics, system configuration, user administration, scopes and permissions, and other supported YourSixOS functions.
6. Integrator training resources shall include applicable platform configuration, deployment, administration, solution-component, and central station/Inspect training.
7. The software provider shall offer formal certification learning paths for integrator personnel responsible for selling, deploying, configuring, administering, and supporting YourSixOS. Certification shall not be considered a project closeout requirement unless specifically required by the Contract Documents.
8. Online YourSix Academy resources shall supplement project-specific system training and remain available for ongoing education, refresher training, and onboarding of additional personnel.

9. Current course availability, certification paths, prerequisites, and enrollment requirements shall be verified through the YourSix Academy at the time training is delivered.

3.4 Closeout

1. Provide final device, site, recording, access-control, sensor, and subscription schedules as applicable.
2. Provide current administrator documentation and support/escalation information.
3. Confirm customer administrative ownership and authorized support access.
4. Confirm final retention settings, notification recipients, alarm-group schedules, and monitoring routing where applicable.

APPENDIX

Reference basis

R Sources

This 2026 revision was prepared from the March 1, 2024 YourSixOS Master A&E specification, the YourSixOS Software Data Sheet dated August 12, 2026, current YourSix public product/resource documentation, and current platform information supplied for this update. Because supported devices, firmware, integrations, subscriptions, and software capabilities evolve, project specifications should be validated against current YourSix documentation at time of design and commissioning.

1. YourSixOS Software Data Sheet, August 12, 2026.
2. YourSix Platform Overview.
3. YourSix Access Control solution details.
4. YourSix Sensors solution details.
5. YourSixOS Canadian Data Residency announcement.
6. YourSixOS Master A&E Specification, March 1, 2024.
7. YourSix Changelog / Versions Archive.
8. YourSix Service Status Page.
9. YourSixOS Video Export Validator.
10. YourSixOS Technical Reference: Central Stations.
11. YourSixOS Central Station API (CSI API) Documentation.
12. YourSixOS Technical Reference: Third-Party Integration and Authorization Model.
13. YourSixOS Documentation: Data Residency.
14. YourSixOS Documentation: Network Dataflows.
15. YourSix Resource: Direct Peer-to-Peer Streaming.
16. YourSix Resource: Object Appearance Search.
17. YourSix Resource: YourSixOS Mobile App.
18. YourSix Resource: Low-Latency Cloud Physical Security.
19. YourSix Resource: Video Surveillance Bandwidth Requirements.
20. YourSix Resource: Proactive Health Monitoring.
21. YourSixOS Technical Reference: Device Management.

- 22. YourSix Resource: YourSixOS Subscriptions & Cloud Storage.
- 23. YourSix Resource: YourSix Academy for Integrators.
- 24. YourSix Resource: YourSixOS Training for End Users & Administrators.
- 25. YourSix Academy: Current Course Catalog and Certification Learning Paths.