General Requirements

- The specified unit shall, in its complete, be created and designed by and manufactured for the sole use of the manufacturer.
- The specified unit shall be of manufacturer’s official product line, designed for commercial and/or industrial 24/7/365 use.
- The specified unit shall be based upon standard components and proven technology using open and published protocols and adopt to industry established standards.

Electronic Security

Video Surveillance

The video surveillance system shall provide high definition (HD) live and recorded images of defined areas of the development utilising fixed or Pan Tilt and Zoom (PTZ) dome cameras. These cameras shall be installed internally and externally to provide the required level of detail and coverage based on six purpose categories; Monitor, Detect, Observe, Recognise, Identify and Inspect. An explanation of each of these purpose categories is as follows;

- Monitor To enable viewing of the number, direction and speed of movement of people across a wide area, providing their presence is known to the operator, the target shall represent not less than 5% of screen height (1080p) or more than 12.5 pixels per metre
- Detect To enable the operator to reliably and easily determine whether or not any target (e.g. a person or vehicle) is present, the target shall represent not less than 10% of screen height (1080p) or more than 25 pixels per metre
- Observe To enable characteristic details of an individual, such as distinctive clothing to be seen, whilst allowing a view of activity surrounding an

incident, the target shall represent not less than 10% of screen height (1080p) or more than 62.5 pixels per metre * (4 horizontal pixels per face)

- Recognise To enable the operator to determine, with a high degree of certainty, whether or not an individual shown is the same as someone they have seen before, the target shall represent not less than 20% of screen height (1080p) or more than 125 pixels per metre * (20 horizontal pixels per face)
- Identify To enable identification of an individual beyond reasonable doubt, the target shall represent not less than 40% of screen height (1080p) or more than 250 pixels per metre * (40 horizontal pixels per face) * Equivalent pixels per metre at target distance.

The video surveillance system shall be provided to monitor the following areas at the noted observation category standard;

- Reception entrances - identification
- General reception area and circulation areas - identification
- Reception meeting rooms - identification
- Reception pedestrian speed gates - identification
- Ground floor lift lobby - recognition
- All vehicle entrances and exits – identification
- Car parking area – recognition
- External Pedestrian routes – recognition
- Fence line and general area - recognition
- All external pedestrian gates - identification
- External building envelope – recognition

Video Management System (VMS) – Axis Camera Station / ACS

A. General Requirements

1. The video management software shall be based upon standard tools and proven technology using open and published protocols.

B. The manufacturer shall provide free upgrades to new software releases within the same major version for the lifetime of the version.

C. The video management software shall be backed by free support within warranty period.

1. The video management software shall, for each channel:

a. Support Baseline, Main and High Profile H.264 decoding in up to 120 fps.

b. Support dynamic media profile selection for live view with all supported profiles.

2. The video management software shall support the use of wide angle / 360° camera.

3. The video management software shall support two-way, full duplex audio encoded with the video stream with supported network cameras (one-way for third-party cameras).

b. The video management software shall accept notifications and alarms from an unlimited number of auxiliary devices connected to the network.

c. The video management software shall provide the following user functionality.

1. Live view functionality:

a. Single camera live view, split views, sequence views, site maps & web pages

2. Recording functionality:

a. Continuous, scheduled, manual and event driven recording

b. Locking of prioritized recordings

c. Individually and configurable resolution and frame rate for each video source.

d. Smart search for recordings based on camera, date and timeline visualization

e. Retrieval of failover recordings from cameras or encoders.

3. Playback functionality:

a. Playback at least eight simultaneous full frame rate Full HDTV 1080p video streams.

b. Export (manual or scheduled) multiple selected video and audio sequences

c. Digital signature on exported recordings.

4. Search functionality

a. Provide an ability to search for video based upon the following criteria's:

1. Time & Date

2. By camera

3. Motion detection within a customizable area of the video

5. Event functionality

a. The video management software shall be equipped with an event functionality, supporting events trigged in a camera, encoder or other network connected device

D. The video management software shall have a licence free privacy masking / video redaction facility built into the software. This shall be a built in offering with no need for third party integration to support in the compliance of DPA2018 / GDPR 'Subject Access Requests'.

E. The recording of the surveillance system will be for 31 days at 12fps at H.264 compression. It is the responsibility of the successful contractor to provide the necessary levels of storage to meet these requirements. As part of the tender return, contractors must include storage calculations taking into considerations the recording standards and scene complexities.

F. The surveillance system will be monitored and controlled from the main reception desk where a client workstation will be positioned consisting of a 2No 19" LCD monitors, PC Client workstation, CCTV KB and Mouse. There will also need to be a client workstation located at each nurse call station

Video Surveillance Camera

Internal & External fixed dome cameras should come with a Varifocal lens and come from the same product family. As a minimum the cameras provided must provide Identification up to 12m, Recognition up to 25M and Detection up to 100+M. Location of cameras is as per tender drawings.

A. General Requirements

1. Resolution - All cameras must operate at 1080p / Full HD resolution unless otherwise stated

2. Frame Rate - Camera must have the capability of operating at 25fps if required. (Recording requirements may differ depending on site requirements)

3. Fixed dome cameras must have a varifocal lens

4. Day and Night - Automatically removable infrared-cut filter

5. Video Compression - H.264 Baseline, Main and High Profile (MPEG-4 Part 10/AVC) Motion JPEG

6. Intelligent Compression - The captured scene shall be analyzed and compression shall be applied differently for areas based on structure and motion. These methods shall follow forensic aspects and shall prevent relevant details from being destroyed.

   a. The algorithms shall be dynamic and the need for configuration shall be limited to enable/disable and the adjustment of the intensity of the applied additional compression.

   b. All non-dynamic methods, like area of interest compression, noise reduction algorithms with a basis impact on the whole image etc. are not allowed.

7. Analytics - Video motion detection, Active tampering alarm Support and Application Platform enabling installation of additional analytics

   a. The camera shall provide a platform allowing the upload of third-party applications directly into the camera.

   b. Camera must have the capability to install a CPNI approved analytic directly on the camera without the need for additional hardware such as servers etc

8. Power – Power over Ethernet IEEE 802.3af/802.3at

9. Connectors - RJ45 10BASE-T/100BASE-TX PoE

<u>Internal Fixed Dome (AXIS P3245–LV Network Camera)</u>

This network camera offers excellent image quality in HDTV 1080p. This streamlined, IK10-rated camera features advanced WDR imaging technology and power efficient built-in IR LED technology deliver sharp video even in challenging light or complete darkness. It includes advanced low-light technology for video with more life-like colors and sharp video of moving objects. And, the varifocal lens with remote zoom and focus capabilities eliminates the need for hands-on fine tuning. With two-way audio you can hear what’s happening in the scene and benefit from audio analytics. Plus, it offers reduced bandwidth and storage needs technology with support for H.264/ H.265 and enhanced security features.

- HDTV 1080p video quality
- Advanced low-light technology, advanced WDR imaging technology and power efficient built-in IR LED technology
- Built-in reduced bandwidth and storage technology with support for H.264 and H.265
- Signed firmware and secure boot
- Two-way audio and I/O connectivity

Image sensor

1/2.8” progressive scan RGB CMOS

Lens

Varifocal, 3.4–8.9 mm, F1.8
Horizontal field of view: 100°-36°
Vertical field of view: 53°-20°
Remote zoom and focus, P-Iris control, IR corrected

Day and night

Automatically removable infrared-cut filter

Minimum illumination

With advanced WDR imaging and low-light technology 2.0:
Color: 0.1 lux at 50 IRE, F1.8
B/W: 0.02 lux at 50 IRE, F1.8; 0 lux with IR illumination on

Shutter time

1/66500 s to 2 s

Camera angle adjustment

Pan ±180°, tilt ±75°, rotation ±175°

Video compression

H.264 (MPEG-4 Part 10/AVC) Baseline, Main and High Profiles
H.265 (MPEG-H Part 2/HEVC) Main Profile
Motion JPEG

Resolution

1920x1080 to 160x90

Frame rate

With WDR: 25/30 fps with power line frequency 50/60 Hz
Without WDR: 50/60 fps with power line frequency 50/60 Hz

Video streaming

Multiple, individually configurable streams in H.264, H.265, and Motion JPEG
Reduced bandwidth and storage needs technology for H.264 and H.265
Controllable frame rate and bandwidth
VBR/ABR/MBR H.264/H.265

Multi-view streaming

Up to 2 individually cropped out view areas in full frame rate

Image settings

Compression, color saturation, brightness, sharpness, contrast, local contrast, white balance, day/night threshold, tone mapping, exposure control (including automatic gain control), exposure zones, defogging, advanced WDR imaging: up to 120 dB depending on scene, barrel distortion correction, fine tuning of low-light behavior, dynamic text and image overlay, privacy masks, mirroring, rotation: 0°, 90°, 180°, 270°, including corridor format

Pan/Tilt/Zoom

Digital PTZ, preset positions

Audio streaming

Full duplex

Audio compression

48bit LPCM, AAC-LC 8/16/32/44.1/48 kHz, G.711 PCM 8 kHz, G.726 ADPCM 8 kHz, Opus 8/16/48 kHz
Configurable bit rate

Audio input/output

External microphone input, line input, digital input with ring power, line output, automatic gain control
Two-way audio connectivity via optional audio and I/O interfaces with portcast technology

Security

Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X (EAP-TLS) network access control, digest authentication, user access log, centralized certificate management, brute force delay protection, signed firmware, secure boot,

Supported protocols

IPv4, IPv6 USGv6, HTTP, HTTPS, SSL/TLS, QoS Layer

3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP®, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SRTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH, SIP, LLDP, MQTT

Application Programming Interface

Open API for software integration
ONVIF® Profile G, ONVIF® Profile S, and ONVIF® Profile T, specification at onvif.org
Support for Session Initiation Protocol (SIP) for integration with Voice over IP (VoIP) systems, peer to peer or integrated with SIP/PBX

Analytics

Included
video motion detection, active tampering alarm
Audio detection
Supported
live privacy shield, perimeter defender, motion guard, fence guard, and loitering guard, occupancy estimator, people counter, tailgating detector, direction detector, random selector
Support for installation of third-party applications.

Event conditions

Analytics, external input, supervision of input, edge storage events, virtual inputs through API

Event actions

Record video: SD card and network share
Upload of images or video clips: FTP, SFTP, HTTP, HTTPS, network share, and email
Pre- and post-alarm video or image buffering for recording or upload
Notification: email, HTTP, HTTPS, TCP, and SNMP trap
Overlay text, external output activation, play audio clip, make call

Data streaming

Event data

Built-in installation aids

Pixel counter, remote focus, remote zoom
IR with adjustable IR illumination intensity

Casing

IP52-rated, IK10 impact-resistant casing with hard-coated dome and dehumidifying membrane
Encapsulated electronics and captive screws

Color: white NCS S 1002-B
For repainting instructions and impact on warranty, contact your distributor partner.

Sustainability
PVC free

Memory
1024 MB RAM, 512 MB Flash

Power
Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 1 Class 3
Typical 6.4 W, max 10.7 W

Connectors
RJ45 10BASE-T/100BASE-TX PoE
I/O: 4–pin 2.5 mm (0.098 in) terminal block for 1 supervised digital input and 1 digital output (12 V DC output, max. load 25 mA)
Audio: 4-pin 2.5 mm (0.098 in) terminal block for audio in and out
Audio and I/O connectivity via audio and I/O interfaces with portcast technology

IR illumination
IR with power-efficient, long-life 850 nm IR LEDs
Range of reach 40 m (130 ft) or more depending on the scene

Storage
Support for microSD/microSDHC/microSDXC card and encryption
Recording to network-attached storage (NAS)

External Fixed Dome (AXIS P3245-LVE Network Camera)

This network camera offers excellent image quality in HDTV 1080p. This outdoor-ready, IK10-rated camera features advanced WDR imaging technology and power efficient built-in IR LED technology to deliver sharp video even in challenging light or complete darkness. It includes advanced low-light technology for video with more life-like colors and sharp images of moving objects. And, the varifocal lens with remote zoom and focus capabilities eliminates the need for hands-on fine tuning. With two-way audio you can hear what’s happening in the scene and benefit from audio analytics. Plus, it offers the reduced bandwidth and storage needs technology with support for H.264/ H.265 and enhanced security features.

- HDTV 1080p video quality
- Advanced low-light technology, advanced WDR imaging technology and power efficient built-in IR LED technology
- reduced bandwidth and storage needs technology supporting H.264 and H.265
- Signed firmware and secure boot
- Two-way audio and I/O connectivity

Image sensor

1/2.8” progressive scan RGB CMOS

Lens

Varifocal, 3.4–8.9 mm, F1.8
Horizontal field of view: 100°-36°
Vertical field of view: 53°-20°
Remote zoom and focus, P-Iris control, IR corrected

Day and night

Automatically removable infrared-cut filter

Minimum illumination

With advanced WDR imaging and low-light technology 2.0:
Color: 0.1 lux at 50 IRE, F1.8
B/W: 0.02 lux at 50 IRE, F1.8; 0 lux with IR illumination on

Shutter time

1/66500 s to 2 s

Camera angle adjustment

Pan ±180°, tilt ±75°, rotation ±175°

Video compression

H.264 (MPEG-4 Part 10/AVC) Baseline, Main and High Profiles
H.265 (MPEG-H Part 2/HEVC) Main Profile
Motion JPEG

Resolution

1920x1080 to 160x90

Frame rate

With WDR: 25/30 fps with power line frequency 50/60 Hz
Without WDR: 50/60 fps with power line frequency 50/60 Hz

Video streaming

Multiple, individually configurable streams in H.264, H.265, and Motion JPEG
Reduced bandwidth and storage needs technology for H.264 and H.265
Controllable frame rate and bandwidth
VBR/ABR/MBR H.264/H.265

Multi-view streaming

Up to 2 individually cropped out view areas in full frame rate

Image settings

Compression, color saturation, brightness, sharpness, contrast, local contrast, white balance, day/night threshold, tone mapping, exposure control (including automatic gain control), exposure zones, defogging, advanced WDR imaging: up to 120 dB depending on scene, barrel distortion correction, fine tuning of low-light behavior, dynamic text and image overlay, privacy masks, mirroring, rotation: 0°, 90°, 180°, 270°, including corridor format

Pan/Tilt/Zoom

Digital PTZ, preset positions

Audio streaming

Full duplex

Audio compression

48bit LPCM, AAC-LC 8/16/32/44.1/48 kHz, G.711 PCM 8 kHz, G.726 ADPCM 8 kHz, Opus 8/16/48 kHz
Configurable bit rate

Audio input/output

External microphone input, line input, digital input with ring power, line output, automatic gain control
Two-way audio connectivity via optional audio and I/O interfaces with portcast technology

Security

Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X (EAP-TLS) network access control, digest authentication, user access log, centralized certificate management, brute force delay protection, signed firmware, secure boot,

Supported protocols

IPv4, IPv6 USGv6, HTTP, HTTPS, SSL/TLS, QoS Layer

3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP®, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SRTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH, SIP, LLDP, MQTT

Application Programming Interface

Open API for software integration
ONVIF® Profile G, ONVIF® Profile S, and ONVIF® Profile T, specification at onvif.org
Support for Session Initiation Protocol (SIP) for integration with Voice over IP (VoIP) systems, peer to peer or integrated with SIP/PBX

Analytics

Included
video motion detection, active tampering alarm
Audio detection
Supported
live privacy shield, perimeter defender, motion guard, fence guard, and loitering guard, occupancy estimator, people counter, tailgating detector, direction detector, random selector
Support for installation of third-party applications.

Event conditions

Analytics, external input, supervision of input, edge storage events, virtual inputs through API

Event actions

Record video: SD card and network share
Upload of images or video clips: FTP, SFTP, HTTP, HTTPS, network share, and email
Pre- and post-alarm video or image buffering for recording or upload
Notification: email, HTTP, HTTPS, TCP, and SNMP trap
Overlay text, external output activation, play audio clip, make call

Data streaming

Event data

Built-in installation aids

Pixel counter, remote focus, remote zoom
IR with adjustable IR illumination intensity

Casing

IP66- and NEMA 4X-rated, IK10 impact-resistant casing with hard-coated dome and dehumidifying membrane
Encapsulated electronics and captive screws

Color: white NCS S 1002-B
For repainting instructions and impact on warranty, contact your distributor partner.

Mounting

Mounting bracket with holes for junction box (double-gang, single-gang, and 4” octagon) and for wall or ceiling mount
¼”-20 UNC tripod screw thread

Sustainability

PVC free

Memory

1024 MB RAM, 512 MB Flash

Power

Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 1 Class 3
Typical 6.4 W, max 11.3 W

Connectors

RJ45 10BASE-T/100BASE-TX PoE
I/O: 4–pin 2.5 mm (0.098 in) terminal block for 1 supervised digital input and 1 digital output (12 V DC output, max. load 25 mA)
Audio: 4-pin 2.5 mm (0.098 in) terminal block for audio in and out
Audio and I/O connectivity via audio and I/O interfaces with portcast technology

IR illumination

IR with power-efficient, long-life 850 nm IR LEDs
Range of reach 40 m (130 ft) or more depending on the scene

External Bullet Camera (AXIS P1445-LE Network Camera)

This network camera is a cost-effective, all-around camera providing excellent image quality at full frame rate in 2 megapixel resolution and in 16:9 format. Fully-featured with advanced low-light technology, power efficient built-in IR LED technology and advanced WDR imaging technology, forensic details are captured even in challenging light conditions including low light and strong backlight. Outdoor-ready with a wide temperature range, this sturdy and impact resistant camera has shock detection and is ready for extreme temperatures. This network camera offers easy installation with remote zoom and focus for fine tuning of the picture. With reduced bandwidth and storage needs technology, I/O and audio support, this product got you covered.

- HDTV 1080p at up to 60 fps
- Ease of installation
- Power efficient built-in IR LED technology
- Advanced WDR imaging
- Advanced low-light technology
- I/O and audio support
- Reduced bandwidth and storage needs technology

Image sensor

1/2.8” progressive scan RGB CMOS

Lens

2.8–8.5 mm, F1.2
Horizontal field of view 110˚–38˚
Vertical field of view 62˚–21˚
Varifocal, Remote focus and zoom, P-Iris control, IR corrected

Day and night

Automatically removable infrared-cut filter

Minimum illumination

HDTV 1080p 25/30 fps with advanced WDR imaging and low-light technology:
Color: 0.07 lux, at 50 IRE F1.2; B/W: 0.01 lux, at 50 IRE F1.2
HDTV 1080p 50/60 fps with low-light technology:
Color: 0.14 lux, at 50 IRE F1.2; B/W: 0.03 lux, at 50 IRE F1.2
0 lux with IR illumination on

Shutter time

1/66500 s to 2 s

Video compression

H.264 (MPEG-4 Part 10/AVC) Baseline, Main and High Profiles
Motion JPEG

Resolution

1920x1080 to 160x90

Frame rate

HDTV 1080p (1920x1080) with WDR: Up to 25/30 fps

(50/60 Hz) in all resolutions
HDTV 1080p (1920x1080) without WDR: Up to 50/60 fps (50/60 Hz) in all resolutions

Video streaming

Multiple, individually configurable streams in H.264 and Motion JPEG
Controllable frame rate and bandwidth
VBR/ABR/MBR H.264

Multi-view streaming

Up to 8 individually cropped out view areas

Image settings

Saturation, contrast, brightness, sharpness, advanced WDR imaging: Up to 120 dB depending on scene, white balance, day/night threshold, exposure mode, exposure zones, compression, orientation: auto, 0°, 90°, 180°, 270° including corridor format, mirroring of images, dynamic text and image overlay, privacy masks

Pan/Tilt/Zoom

Digital PTZ

Audio streaming

Audio in, simplex

Audio compression

24bit LPCM, AAC-LC 8/16/32/48 kHz, G.711 PCM 8 kHz, G.726 ADPCM 8 kHz, Opus 8/16/48 kHz
Configurable bit rate

Audio input/output

External microphone input or line input

Security

Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X (EAP-TLS) network access control, digest authentication, user access log, centralized certificate management, brute force delay protection, signed firmware

Supported protocols

IPv4, IPv6 USGv6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP®, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SRTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH, LLDP

Application Programming Interface

Open API for software integration
ONVIF® Profile G, ONVIF® Profile S and ONVIF® Profile T, specification at onvif.org

Analytics

Included
video motion detection
Supported
digital autotracking, perimeter defender, cross line detection
Support for installation of third-party applications.

Event triggers

Analytics
Detectors: live stream accessed, video motion detection, audio detection, day/night mode, shock detection, tampering
Hardware: network, temperature
Input Signal: digital input port, manual trigger, virtual inputs
Storage: disruption, recording
System: system ready
Time: recurrence, use schedule

Event actions

Record video: SD card and network share
Upload of images or video clips: FTP, SFTP, HTTP, HTTPS, network share and email
Pre- and post-alarm video or image buffering for recording or upload
Notification: email, HTTP, HTTPS, TCP and SNMP trap
PTZ: PTZ preset, start/stop guard tour
Overlay text, external output activation, day/night mode

Data streaming

Event data

Built-in installation aids

Pixel counter, remote zoom (3x optical), remote focus, auto rotation

Casing

IP66/IP67-, NEMA 4X-, and IK10-rated casing
Polycarbonate blend and aluminium
Color: white NCS S 1002-B

Power

Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3

Typical: 5.6 W, max 12.95 W

Connectors

Shielded RJ45 10BASE-T/100BASE-TX PoE
3.5 mm mic/line in
I/O: 4-pin terminal block for 1 alarm input and 1 output

IR illumination

IR with power-efficient, long-life 850 nm IR LEDs
Range of reach 40 m (131 ft) or more depending on the scene

External PTZ (AXIS Q6125-LE PTZ Network Camera)

This PTZ Network Camera offers discreet and unobtrusive surveillance. Its clever dome design effectively conceals the direction of the lens, and its integrated, automatically adaptable IR LED illumination enables surveillance in total darkness (up to 200 m (656 ft) or more depending on the scene). The camera provides full scene fidelity and sharp images both above and below the horizon thanks to innovative dome rotation technology. The advanced dome cleaning function removes water drips from the dome, for clear images in rainy weather.

- HDTV 1080p and 30x zoom
- Power efficient built-in IR LED technology
- Innovative dome rotation technology with advanced dome cleaning function
- Advanced WDR imaging, low-light technology and reduced bandwidth and storage needs technology

Image sensor

1/2.8” Progressive scan CMOS

Lens

4.3-129 mm, F1.6-4.7
Horizontal field of view: 63.5˚–2.3˚
Vertical field of view: 38.4˚–1.3˚
Autofocus, auto-iris

Day and night

Automatically removable infrared-cut filter

Minimum illumination

Color: 0.1 lux at 30 IRE, F1.6
B/W: 0.008 lux at 30 IRE, F1.6, 0 lux with IR illumination on

Color: 0.15 lux at 50 IRE, F1.6
B/W: 0.01 lux at 50 IRE, F1.6, 0 lux with IR illumination on

Shutter time

1/10000 s to 1 s

Pan/Tilt/Zoom

Pan: 360° endless, 0.05°–700°/s
Tilt: +20 to -90°, 0.05°–500°/s
Zoom: 30x optical, 12x digital, total 360x zoom
Nadir flip, 256 preset positions, tour recording, guard tour, control queue, on-screen directional indicator, set new pan 0°, adjustable zoom speed, speed dry

Video compression

H.264 (MPEG-4 Part 10/AVC), Main and High Profiles
H.265 (MPEG-H Part 2)
Motion JPEG

Resolution

1920x1080p (HDTV 1080p) to 640x360

Frame rate

Up to 25/30 fps or 50/60 fps (50/60 Hz) in all resolutions

Video streaming

Multiple, individually configurable streams in H.264, H.265 and Motion JPEG
and H.265
Controllable frame rate and bandwidth
VBR/MBR H.264/H.265

Image settings

Compression, color, brightness, sharpness, white balance, exposure control, exposure zones, noise reduction, rotation, electronic image stabilization (EIS), manual shutter time, text and image overlay, image freeze on PTZ, scene profiles, focus recall
Defogging, backlight compensation
Contrast, highlight compensation, advanced WDR imaging technology: 120 dB, 32 individual 3D privacy masks

Security

Password protection, IP address filtering, HTTPS encryption, IEEE 802.1x (EAP-TLS) network access control, digest authentication, User access log, Centralized Certificate Management, Brute force delay protection, signed firmware

Supported protocols

IPv4, IPv6 USGv6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPnP, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SRTP, SFTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH, NTCIP, MQTT

Application Programming Interface

Open API for software integration
ONVIF® Profile G and ONVIF® Profile S, specifications at onvif.org

Analytics

Included
video motion detection, fence guard, motion guard, loitering guard, Autotracking, Active Gatekeeper
Supported
Support for installation of third-party applications.

Event triggers

Detectors: live stream accessed, shock detection, day/night mode
Hardware: network, temperature, fan
Input Signal: manual trigger, virtual inputs
PTZ: autotracking, error, moving, preset reached, ready
Storage: disruption, recording
System: system ready
Time: recurrence, use schedule

Event conditions

Analytics, external input, virtual inputs through API
Audio: audio detection
Device status: above operating temperature, above or below operating temperature, below operating temperature, fan failure, IP address removed, network lost, new IP address, shock detected, storage failure, system ready, within operating temperature
Edge storage: recording ongoing, storage disruption
I/O: digital input, manual trigger, virtual input
PTZ: PTZ malfunctioning, PTZ movement, PTZ preset position reached, PTZ ready
Scheduled and recurring: scheduled event
Video: live stream open

Event actions

Record video: SD card and network share

Pre- and post-alarm video or image buffering for recording or upload
Upload of images or video clips: FTP, SFTP, HTTP, HTTPS, network share, and email
Notification: email, HTTP, HTTPS, TCP, and SNMP trap
PTZ: PTZ preset, guard tour
Overlay text, day/night mode
IR illumination

Data streaming

Event data

Built-in installation aids

Focus assistant, pixel counter, remote back focus

Casing

IK08, IK10 housing and mounting, IP66- and NEMA 4X-rated
Repaintable metal casing (aluminum), hard coated Polycarbonate (PC) clear dome with Sharpdome technology

Memory

1 GB RAM, 512 MB Flash

Power

High PoE midspan 1-port: 100–240 V AC, max 74 W
Camera consumption: typical 14 W (no IR), max 51 W
PoE+ midspan 1-port: 100–240 V AC, max 37 W
IEEE 802.3at Type 2 Class 4
Camera consumption: typical 14 W, max 25 W

Connectors

RJ45 10BASE-T/100BASE-TX
RJ45 Push-pull Connector (IP66)

IR illumination

Power efficient built-in IR LED (850 nm) with automatic adapting angle of illumination and intensity.
With 30 W midspan: Range of reach 150 m (492 ft) or more depending on the scene
With 60 W midspan: Range of reach 200 m (656 ft) or more depending on the scene

Operating conditions

With 30 W midspan: -30 °C to 50 °C (-22 °F to 122 °F)
With 60 W midspan: -50 °C to 50 °C (-58 °F to 122 °F)
Maximum temperature according to NEMA TS 2 (2.2.7): 74 °C (165 °F)

Arctic Temperature Control: Start-up as low as -40 °C (-40 °F)
Humidity 10–100% RH (condensing)

Storage conditions
-40 °C to 70 °C (-40 °F to 158 °F)
Humidity 5-95% RH (non-condensing)

Data protection

The Contractor shall recognise that the use of the CCTV system is for the purpose of surveillance and is therefore encompassed by the requirements of the Data Protection Act 2018 / DPA2018 / General Data Protection Regulation.

The Video surveillance system that is installed must comply with all necessary local legislation when it comes to Data Protection and Privacy by Design. The three main articles for consideration for compliance to GDPR are Article 15, EU GDPR “Right of access by the data subject”, Article 30, EU GDPR “Records of processing activities” and Article 35 “Data Protection Impact Assessment”.

Article 15, EU GDPR “Right of access by the data subject”
To support with the legal requirement of Article 15, EU GDPR “Right of access by the data subject” The Video Management System must provide a privileged based export facility that is logged accordingly, to comply with Article 30 “Records of processing activities”. To protect the integrity and security of the exported video footage, exported footage will be provided as a password protected .zip file to support the recommendation given by the ICO.

Article 30, EU GDPR “Records of processing activities”
To support with the legal requirement of Article 30, EU GDPR “Records of processing activities” The Video Management System must provide a reporting log, giving transparency of how the system has been used. Access to ACS is privileged based with specific functions enabled and disabled based on approval levels. Live video streaming, start and stop is logged so live operation can be identified. Should a ‘Subject access

request’ occur, associated video exporting information is fully logged. Exported video footage is time and date stamped. The ability to export is privileged based and can only be carried out by an authorised operator. Information associated with who has exported the video can be logged in the comments box which has been included for the operator to provide necessary reporting information such as ‘Justification for exporting video’, ‘Whom the intended recipient is and why’ and finally to protect the integrity of the exported video, exported footage will be provided as a unique password protected .zip file

Product functionality

- The unit shall operate on an open source; Linux-based platform, and including a built-in web server.
- The unit shall support the use of HTTPS and SSL/TLS, providing the ability to upload signed certificates to encrypt and secure authentication and communication of both administration data and video streams.
- The unit shall provide centralized certificate management, with both pre-installed CA certificates and the ability to upload additional CA certificates. The certificates shall be signed by an organization providing digital trust services.
- The unit shall support IEEE 802.1X authentication.
- The unit shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications.
- The implemented API shall be standardized and supported by all network video products offered by the manufacturer.
- The unit shall comply with relevant ONVIF profile as defined by the ONVIF Organization.

Installation

- The Contractor or security sub-contractor shall be a licensed security Contractor with a minimum of five (5) years’ experience installing and servicing systems of similar scope and complexity and evidence that is completed at least three (3) projects of similar design and is currently engaged in the installation and maintenance of systems herein described.

- The Contractors or subcontractors' main resources within the project shall carry proper professional certification issued by the manufacturer and verified by a third party organization to confirm sufficient product and technology knowledge.
- The Contractor shall carefully follow instructions in documentation provided by the manufacturer to ensure all steps have been taken to provide a reliable, easy-to-operate system.
- All installation, configuration, setup, program and related work shall be performed by electronic technicians thoroughly trained by the manufacturer in the installation and service of the equipment provided.
- All equipment shall be tested and configured in accordance with instructions provided by the manufacturer prior to installation.
- All firmware found in products shall be the latest and most up-to-date provided by the manufacturer, or of a version as specified by the provider of the Video Management Application (VMA) or Network Video Recorder (NVR).
- All equipment requiring users to log on using a password shall be configured with user/site-specific password/passwords. No system/product default passwords shall be allowed.

Physical Access Control System (Quanika Software & Axis A1601)

A physical access control system (PACS) shall be installed to control access to the premises and to control access to restricted parts of the premises. PACS also provides a platform for the introduction of intelligent I/0 for monitoring and alarm.

Open standards compliance

ONVIF Profiles 'A' and 'C' compliance requirement

The growth in interoperability between access control and other devices is key to the end user 'fit for future' philosophy. Access controllers and field devices must be able to function on different software platforms; i.e. the controllers shall not be restricted to one manufacturer software. This is essential to afford end users with choice, both in immediate selection and to ensure the PACS remains fit for purpose over time, as demands and needs change. Access controllers shall demonstrate conformance with ONVIF Profiles A & C. Controllers that do not conform to this open standard shall not be considered for this project.

OSDP compliance

The controllers should be compatible with OSDP (Open Supervised Device Protocol) door readers. The PACS solution shall also be capable of both 125KHz and 13.56MHz Wiegand door reader technology, within a transition path from lower to higher frequency, the timing of which is dictated by the end user.

IP / Networked Controllers

The system shall be an IP based configuration with controllers connected via a dedicated network switch. Only IP controllers which are designed specifically for connection to company or security networks are acceptable.

All IP Network controllers with full intelligence, distributed processing controllers. The applicable system database, operating parameters shall be downloaded from the host server to all IP controller, stored on controller memory.
All requests from card readers, local linkage parameters, scheduled functions from the on-board processor with no assistance requirement from the host software server.

IP Network controllers support multiple card technologies:

- 125Khz proximity, 13.56Mhz smart card technologies (iClass, Mifare, etc.)
- Wiegand & OSDP
- Magnetic strip
- Keypads
- Biometric devices
- Bar code & QR code
- wireless lock sets
- Data interface to the card readers shall support standard Wiegand Data1 / Data0, as well as Clock/Data protocols.

PoE controller power / lock output

The controllers shall use PoE as the basis for operating power, together with lock output power, managed directly from the controller and configuration menu. Where additional power is required, the bid shall include power enclosures designed as suitable for user lock demand and power/battery back up in the event of a power outage and tested to perform with the nominated PACS controller.

Controller - operational overview

- The Controllers should be configurable in a 'by the door' design; i.e. capable of location close to doors, thereby reducing the cabling to readers and door furniture (sensors, locks, buttons, etc.). each controller shall have a housing fit for that purpose, with tamper sensing for cover and base removal. Controllers must offer a scalable growth path to enable the user to decide, on their timescale, if expansion of the system is required. which is scalable and can be able to be adapted to a variety of applications. Each controller shall have, as standard, its own administration software for single controller installation. Set-up, alarms, events and a full reporting solution for all events and actions are to be included in the admin software.
- Controllers should be able to operate without need for a permanently connected server or pc, where necessary and preferred. This is useful where a single controller or smaller installation can function without incurring additional costs of servers / pc's. UI software and configuration programmes useful for the set up and commissioning / re-programming of controllers and enhanced management of rules across several controllers are of course accepted for that purpose.
- Multiple controllers may be connected in a standalone network, to be administered by any pc, without the need for that pc or server to be connected during normal operational mode (out of configuration). Access to the controller(s) is achieved via a web enabled device and the device's IP address.

Interoperable solutions

A key value of IoST devices is their ability to form solutions with other devices or software. The chosen access controller should, in its core options, offer open connectivity to hardware and software partners, through published and verified API's and SDK's. Further, the supplier guarantees that it offers API's and SDK's for its controllers, to 3rd party developers, so that future system demands which cannot yet be envisaged, can be made available.

Interoperability options include solutions useful to users, including but not limited to;

Wireless Locking

The growth in wireless locking must be accommodated in modern PACS solutions. Therefore, it is required that the controller shall be able to offer at least two wireless locking manufacturer options, the programming of which must be native to the controller UI / configuration menu (not as a separate ‘linked’ function).

Mobile (Soft) Credentials

The adoption of soft credentials is critical to the development of cloud or hosted pacs solutions and to the increasing recognition of user focus and multi-technology credential roll out to smart devices, such as BYOD. To protect the capability of the system to be fit for future purpose, the controller shall have on board capacity to manage mobile credentials such as those offered by HID Global. Processes native to the controller allow mobile credential as a user profile selection, with the capability to liaise directly with HID’s mobile portal and issue credentials directly to users

Visitor Management

Visitor / contractor management using QR codes in combination with cameras

LPR

License plate recognition in combination with user access rights, without the need for additional server enacted programme functions

QR Codes

QR/Barcode reading via direct integration with surveillance cameras

Facial Recognition Software

Face recognition using a software provider application in a connected camera, to manage the face recognition and interoperate with the door controller to receive a converted signal, appropriate and process that information and compare the data to programmed user (face) access rights for open / do not open, door release decisions

Door monitoring contacts

Door monitoring contacts shall be installed to each opening leaf of each door to be monitored to monitor the door status where this is not achievable through an access control lock or where an access control lock shall not be installed.

Electric locks

All electronically controlled locks to be installed shall meet current building regulations. The type of lock shall take into account the nature, construction and use of the door, the volume of traffic and the level of security required.

The Contractor shall confirm in their tender response which locks they propose for each door.
All locks that are fitted shall be of the type that allows monitoring of the lock by the system or a door contact must monitor each door leaf.

Any one and a half and double leaf doors shall have both leaves fitted with a locking device or the Contractor shall obtain agreement from the Client that the half leaf is to be normally secured shut using alternative mechanical locks.

All locking devices shall have a holding force of at least:
12 kN
All locking devices shall adhere to the requirements of PAS 24:2012 requirements and will be tested as part of the full doorset.

Fail safe/fail secure

All access control doors shall fail safe in the event of a fire alarm.

Emergency break glass units (BGU)

Green emergency break glass units shall be installed adjacent to each access controlled door to allow the door to be released in the case of an emergency.
The BGUs:
Shall either have "EMERGENCY DOOR RELEASE" etched in white or a pictogram of a man exiting. The

style shall match that of the red fire BGUs.
Shall match the red fire BGUs in moulding
Shall utilise resettable plastic elements.

Software Access Control Key Features

- Scalability - The Access Control software shall support:
- Server based software supports Windows 7+ version
- Supports SQL Server 2014 + version
- Encrypted database
- from single site to multiple buildings or sites from one central server
- from two-reader up to 128 readers
- supports IP network control 2x reader with full intelligence
- 100,000 offline transactions support per Controller
- supports IP network input output relay boards with full intelligence
- Unlimited Card formats up to max 80bit card
- Unlimited Cardholders
- Events management
- Turnstile support
- Carpark barrier support
- Support Unlimited Inputs/Outputs
- Unlimited Support Rules and Routines
- Soft & Hard Timed Antipassback
- Unlimited Access Groups
- Communication Service module
- Sensor / Outputs management
- Sensor / Outputs management
- Time and Attendance
- Mustering / Roll call function
- Custom report generation
- Alarm Management System
- Manual Control to control doors, sensors and outputs
- Multilingual Support
- Include Interactive Graphical Floor plans
- Support single or dual screen workstation
- Supports unlimited workstation
- Realtime stat & statics gauges
- Realtime On-site Cardholder

- Auto Import/Export data
- Unlimited Operator profile, Access, Permissions
- Database Integration Software
- Mobile apps with Identification and Verification capabilities
- All Alarms show events on Graphical map
- Alarm events reported, listed in the alarm log with order of priority, date/time
- Alarm log provide reporting alarm events, acknowledgement and/or action of operator.
- Integration CCTV software with bi direction communications
- Integration direct to Intruder alarm panel
- Integration direct to Fire alarm panel
- Integration to IP Network intercom hardware
- Integration to IP Network Audio system
- Integration to Key management system
- Integration direct to Hotel front of house system

Unlimited Access Levels

- Unlimited access levels defining what doors/portals the cardholder is authorized to enter. an Unlimited assigned schedule to designate to access levels and cardholder, doors.
- Cardholder record assignment of multiple access levels to the same cardholder.

Rules Management of event or input to be linked to an event or output and trigger the following

- Door Momentary
- Door Unlock
- Door Lock
- Door Group Momentary
- Door Group Unlock
- Door Group Lock
- Door Lockdown
- Door Lockdown Clear
- Output Momentary
- Output On
- Execute Program
- Execute SQL
- Send E Mail

- Interactive graphical plans with Icons, to indicate or click on to: Lock, Unlock, Momentary Unlock, Lockdown, Clear Lockdown, acknowledge alarms status of
  - Doors
  - Inputs (sensors).
  - Outputs.
  - Outputs Groups.
  - CCTV

- Interactive graphics plans window have ability to provide floating function of window

Unlimited Schedules

- unlimited number of schedules for triggers or events.
- Capable of creating two types of schedules
  - Recurring events
  - One Time events

Unlimited Anti-Passback

- Hard anti-passback
- Soft anti-passback
- Timed anti-passback
- Area Entering
- Area Exiting
- Hard Anti-passback

Operator Access and Permissions

- Unlimited number of system operators.
- Operators profile setup, what can see, do, acknowledge, program, proffered language.
- Operator defined by unique operator name and password.
- Operators setup with expiration date

Report Generator

- full featured Report Generation Utility to display or print database information Reports.
- The Report Utility, with report wizard to create site specific reports tailored for their site. The Wizard shall allow for selecting of a database table or View, Fields within the table or View, Sort Conditions and Sort Order
- The Report Utility should contain the following

functionality:

- Contain over 150 canned reports
- Parameter select functions
- Search between two date/time stamps
- Search on event time
- Export to text file (TXT)
- Export to Web Page (HTM)
- Export to Comma Delimited file (CSV)
- Export to SQL File (SQL)
- Email to Recipient
- Refresh Timer

Network Video Door Station

The video door stations will be located at all unmanned entrances and exits and will connected back to the control room. The network video door station will ask as both a means of visual communication between the visitor and also an access control reader. To manage visitors and deliveries, the video door station will also recognise QR codes as a form of controlling access to site.

AXIS A8207-VE Mk II Network Video Door Station

This network video door station combines a fully featured 6 MP security camera with high-quality, two-way audio communication and remote entry control. It also has an integrated RFID multi-frequency reader with support for most standard credential types including HID® iClass®, allowing you to integrate with other access control systems. By providing both surveillance and access for visitors and employees, this network video door station increases the efficiency while keeping down the number of devices at the door. Interaction is intuitive and accessible, with an induction loop for hearing aids. Analytics, such as motion or sound detection, are supported.

- 6MP wide-angle camera
- Multiple hardware interfaces: audio input/output, relays, HDMI output, RS485
- Easy integration with SIP, API and ONVIF
- Signed firmware with Secure Boot
- Support for HID® iClass®

Image sensor

1/2.9” progressive scan RGB CMOS

Lens

1.56 mm, F2.8
Horizontal field of view: 180°
Vertical field of view: 120°
Fixed focus, IR corrected, fixed iris

Minimum illumination

LED lit: 0.0 lux
LED unlit (with WDR): 0.7 lux
LED unlit (without WDR): 0.55 lux

Shutter time

1/143000 s to 2 s with 50 Hz
1/143000 s to 2 s with 60 Hz

Video compression

H.264 (MPEG-4 Part 10/AVC) Main and High Profiles
Motion JPEG

Resolution

3072x2048 to 160x90

Frame rate

Up to 30/25 fps (60/50 Hz) in all resolutions

Video streaming

Multiple, individually configurable streams in H.264 and Motion JPEG
Controllable frame rate and bandwidth
VBR/MBR H.264

Image settings

Saturation, contrast, brightness, sharpness, forensic WDR: Up to 120 dB depending on scene, white balance, exposure mode, exposure zones, compression, text and image overlay, privacy masks

Pan/Tilt/Zoom

Digital PTZ

Audio streaming

Two-way, full duplex
Echo cancellation and noise reduction

Audio compression

384bit LPCM, AAC-LC 8/16 kHz, G.711 PCM 8 kHz,
G.726 ADPCM 8 kHz, Opus 8/16 kHz

Configurable bit rate

Audio input/output

Line input, line output, dual built-in microphone (can be disabled)
T-coil
Built-in speaker
73 dB (at 50 cm / 19.7 in)

Amplifier description

Built-in 2 W Class D amplifier

Entry authentication

Card, tag, PIN, door code

Alarm status indication

User feedback for access granted, access denied, keypad, armed, disarmed

Supported protocols

RS485 (OSDP), Wiegand, VAPIX reader interface

Reader technology

Generic 13.56 MHz (MIFARE Classic®, MIFARE Plus® (Level 1), MIFARE DESFire® EV1 and EV2, HID® iCLASS®, HID® iCLASS® Elite).
Proximity 125 kHz (HID® Prox, EM-42xx, ISOProx II).

Hearing loop

T-coil
4 W Class D amplifier

User feedback

Illuminated symbols, indicator stripe, illuminated buttons, audible feedback

Detection type

Tamper switch, accelerometer (shock detection), video tampering

Security

Password protection, IP address filtering, signed firmware, HTTPS encryption, IEEE 802.1X network access control, digest authentication, user access log, centralized certificate management, secure boot

Supported protocols

IPv4/v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP®, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SRTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH, SIP, SIPS, LLDP, STUN, TURN

Application Programming Interface

Open API for software integration
ONVIF® Profile S and ONVIF® Profile G, specification at onvif.org

VoIP

Support for Session Initiation Protocol (SIP) for integration with Voice over IP (VoIP) systems, peer to peer or integrated with SIP/PBX
Tested with various SIP software such as Cisco, Bria and Grandstream
Tested with various PBX softwares such as Cisco, Avaya and Asterisk
Phone book, parallel call forking, sequential call forking, call extension dialing

Analytics

Included
video motion detection, active tampering alarm, audio detection
Supported
motion guard, fence guard, and loitering guard
Support for installation of third-party applications.

Event triggers

Analytics, external input, edge storage events, virtual inputs through API
Call: DTMF, state, state changes
Detectors: audio detection, live stream accessed, shock detection, tampering, PIR, motion alarm
Hardware: Casing open, temperature, relays and outputs, network
Input Signal: digital input port, manual trigger, virtual inputs
Storage: disruption, recording
System: system ready
Time: recurrence, use schedule
PTZ: moving, preset reached

Event actions

Door control
HDMI
Make call: SIP, API
Terminate call: SIP, API
Record video and audio: SD card and network share

Upload of images or video clips: FTP, SFTP, HTTP, HTTPS, network share, and email
Pre- and post-alarm video or image buffering for recording or upload
Notification: email, HTTP, HTTPS and TCP
External output activation, play audio clip, overlay text, PTZ controls, status LED, WDR mode

Data streaming
Event data

Casing
IP66 and NEMA 4X-rated, IK08 impact- and scratch-resistant glass
Aluminum casing, polycarbonate (PC) hard-coated dome
Color: metallic dark grey

Sustainability
PVC free

PIR sensor
Passive infrared (PIR) motion sensor.

Memory
2048 MB RAM, 512 MB Flash

Power
Power in: Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 1 Class 3, or Power over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4, or 8-28 V DC min. 25 W
Power consumption: typical 8 W, max 22 W
Power out: Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 1 Class 3: 24 V/0.05 A or 12 V/0.1 A. Power over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4, or 8-28 V DC: 24 V/0.3 A or 12 V/0.7 A
Relay rating: 30 V, 1 A

Connectors
RJ45 10BASE-T/100BASE-TX, PoE
I/O: 6–pin terminal block for 4 alarm inputs/outputs
DC input, 2 relays, line out, line in, microHDMI, RS485/Wiegand

Storage
Support for microSD/microSDHC/microSDXC card
Support for recording to network-attached storage (NAS)

Operating conditions
-40 °C to 55 °C (-40 °F to 131 °F)

Humidity 10-100% RH (condensing)

Storage conditions
-40 °C to 65 °C (-40 °F to 149 °F)

Dimensions
H x W x D: 248 x 106 x 51 mm (9 3/4 x 4 3/16 x 2 in)

Weight
1.3 kg (2.9 lbs)

Mounting option
Wall mount, wall mount with conduit pipe, or recessed mount

Network Audio System Specification

Outline Description:
The Contractor shall be responsible for the supply, installation, commissioning and demonstration or a network audio system for the use of PA, background music and security enhancement.

The public address system shall be used for the broadcast of routine public address announcements, background music and other entertainment programmes to specified zones selected.

The Contractor shall engage a specialist Audio Systems Contractor and provide a complete system in accordance with associated specification and drawings. The entire system will be commissioned and demonstrated to the satisfaction of the engineer.

System Overview:

The system shall consist of, but not limited to the following principle devices and components, which collectively shall form the Audio installation:

- Audio Player / Audio Manager
- VoIP Handset or SIP Desktop PA Microphone
- Speakers (Internal & External)
- Audio bridge if existing analogue speakers and amplifiers need to be retained
- Edge based Network Amplifier to extend speaker offering if needed
- All speakers and devices to be PoE

The client has the desire to deploy a flexible network audio systems that is a complete high-quality audio systems that can be used in various situations all from the same system. The aim of the network audio system is to:

- Improve security across the premises with event-triggered announcements and direct callouts.
- Make live or scheduled announcements in different zones, at the right time and right place.
- Create ambiance with easy and flexible scheduling of great-sounding background music.
- Utilising the network infrastructure rather than separate infrastructure just for the audio system

Public Address – Broadcast to single or multiple zones:

A network audio system will be utilised to deliver different kinds of informative messages and updates across the site. The network audio system will allow the operators to give live announcements and/or scheduled announcements. The PA system can also issue live or triggered announcements during an emergency.

Security:

The network audio system is proposed to enhance the operational use for the video based security installation. Where a perimeter protection systems is deployed, there will be a cause and effect strategy developed around the use of video and audio. The camera will alerts a security guard to give a warning to the intruder using the audio system. Depending on the sophistication of the agreed security system, this facility can either be an automated audio alert activated by an analytic in the camera, or this can be a live audio alert given by an authorised individual. Live audio announcements can be delivered by a SIP Compatible MIC or a SIP enabled telephone or from a VMS

Wrong way detection

By integrating camera, software and network audio you can detect people moving in the wrong direction and notify immediately via an audio message or an alarm via the speaker. An easy and cost-effective solution for minimizing losses due to theft.

Real-time direction detection

Wrong-Way notification

Deter unwanted activity

Improve security on your premises with direct callouts, live or recorded. Axis outdoor loudspeaker provides clear, long-range speech for remote speaking in video surveillance applications enabling an operator to remotely address people and deter unwanted activity. The speaker can also play a pre-recorded audio file when it is manually or automatically triggered in response to an alarm event.

Background Music (For Business)

The chosen vendor must be able to offer a complete solution for background music in a business setting. The vendor must provides the network audio systems and provide the music content. This can either be done individually or through an approved partner offering.

The network audio systems will let the user manage their music, delivering it via network speakers to the user at the agreed volume and at the time and place of their choice. The network audio system will also be able to deliver live or pre-recorded voice announcements whenever appropriate from the same speakers.

Audio Management Software

The manufacturer must be able to provide Audio Management Software that lets you efficiently manage and control your audio system regardless of its size and complexity. Depending on the size and complexity of the system, the manufacturer must have different offerings depending on the requirements. Network speakers must come with a pre-installed audio player for basic systems. The pre-installed audio player must allow for schedule playlists with music and announcements.

A more sophisticated network Audio Manager will be required for larger systems. The network audio manager must be server based and provides easy, management of large IP audio installations. This offering will take control of the complete audio system from one single user interface which handles, for example, system setup of audio devices, zone management, audio content management, and audio scheduling. The network Audio Manager will help broadcast music, live or scheduled announcements, emergency messages, either individually in separate zones or centrally to all devices. The network Audio Manager realizes the benefits of network audio:

- One single user interface
- Local Central control
- Zone management
- Audio content management
- Advanced Scheduling

Speaker offering

This is an all-in-one speaker system connected with a single network cable. It delivers out-of-the-box-ready high-quality sound without any need for fine-tuning. Background music can be played via the preinstalled Audio Player application. You can create and schedule your own playlists from an onboard SD card or from audio streaming services. The speaker is also perfect for voice announcements (scheduled or live calls). The speakers can be zoned together thanks to built-in audio synchronization technology.

- Easy music streaming
- Voice announcements
- All-in-one speaker system
- Quick installation with just one network cable (PoE)
- Future-proof with openness and integration
  - Single Zone with Leader/Followers up to 50 per zone
  - Single source
  - 2 Priority Levels (Announcements and Music)

General Speaker Specification

Audio streaming

- One-way/two-way*, mono

Audio compression

- G.711 PCM 8 kHz, G.726 ADPCM 8 kHz, µ-law 16 kHz, WAV,
- MP3 in mono/stereo from 64 kbps to 320 kbps.
- Constant and variable bit rate.
- Sampling rate from 8 kHz up to 48 kHz.

Audio input/output

- Mic-in, line-in, line-out

Security

- Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X network access control, Digest authentication, User access log, Centralized Certificate Management

Supported protocols

- IPv4/v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH, NTCIP, SIP (Cisco, Avaya, Asterisk)

Music streaming

- Music playback through supported audio player.
- Offline streaming from SD card and audio-in, online streaming support.

- Audio-in connector can be used as a streaming source using Audio Bridge

Voice announcement

- Up to 50 pre-recorded voice announcements through supported audio player. Voice announcement through built-in SIP support for connection to any IP telephone /VoiP system and API support.

Application Programming Interface

- Open API for software integration.

VoIP

- Support for Session Initiation Protocol (SIP) for integration with Voice over IP (VoIP) systems. Peer to peer or integrated with SIP/PBX.
- Tested with: SIP client such as Cisco, Bria and Grandstream and PBX suppliers such as Cisco and Asterisk.

Audio synchronization

- Built-in audio synchronization for up to 50 speakers with unicast and hundreds of speakers with multicast. No additional speaker management software or hardware required.

Intelligent audio

- Auto Speaker Test (verification via built-in microphone)

Event triggers

- Call, Virtual inputs, External input

Event actions

- Play audio clip, send SNMP trap, status LED
- File upload via HTTP, network share and email
- Notification via email, HTTP, HTTPS and TCP
- External output activation

Built-in installation aids

- Test verification and identification

Approvals

- EMC

- EN 55032 Class A, EN 61000-3-2, EN 61000-3-3, EN 55035, EN 61000-6-1, EN 61000-6-2, FCC Part 15 Subpart B Class A, ICES-003 Class A, VCCI Class A, RCM AS/NZS CISPR 32 Class A,
- Safety
- IEC/EN/UL 62368-1
- Environment
- IEC/EN 60529 IP20, UL2043 Plenum rated, NEMA 250 Type 1, IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27

Warranty

- The main unit shall be backed by a minimum of three years manufacturer warranty. The manufacturer shall provide the option of extended warranty for the unit. The optional extended warranty shall be available for a total warranty period of maximum five years.

Installation and Commissioning

- The contractor or designated subcontractor shall submit credentials of completed manufacturer certification, verified by a third party organization, as proof of the knowledge.

Testing & Commissioning

- The system shall be tested and commissioned by the Audio system Specialist in line with equipment manufacturer’s specifications to the satisfaction of the engineer.

Demonstration and Training

- In addition to attendances and brief system training at a client handover seminar the contractor will allow two further training session of 2hrs duration to be given to personnel nominated by the client at time to be agreed with the client.

Sustainability

- The specified unit shall be manufactured in accordance with the environmental standards as defined in ISO 14001.
- The specified unit shall be compliant with the EU directives 2011/65/EU (RoHS) and 2012/19/EU (WEEE).

- The specified unit shall be compliant with the EU regulation 1907/2006 (REACH).
- The specified unit shall be PVC-free.
- The manufacturer shall have signed and support the UN Global Compact initiative as defined by United Nations https://www.unglobalcompact.org/
- The manufacturer and its sustainability strategy and policy, shall be based on the ten principles outlined by UN Global Compact, relating to; ”human rights, labor, environment and anti-corruption”.

General Specification Consideration

The below section relations to all technologies and disciplines specified within this tender document where relevant.

Sustainability

- The specified unit shall be manufactured in accordance with the environmental standards as defined in ISO 14001.
- The specified unit shall be compliant with the EU directives 2011/65/EU (RoHS) and 2012/19/EU (WEEE).
- The specified unit shall be compliant with the EU regulation 1907/2006 (REACH).
- The specified unit shall be PVC-free.
- The manufacturer shall have signed and support the UN Global Compact initiative as defined by United Nations https://www.unglobalcompact.org/
- The manufacturer and its sustainability strategy and policy, shall be based on the ten principles outlined by UN Global Compact, relating to; ”human rights, labor, environment and anti-corruption”.

Quality Assurance

- The manufacturer shall through documented physical testing ensure the products’ complete functionality for the complete specified operative environments in a worst-case scenario.
- The specified unit shall be manufactured in accordance with ISO9001.

Warranty

- All security system components provided by the manufacturer shall be fully warranted for a minimum of three (3) years.
- The manufacturer shall provide warranty and optional extended warranty for the unit for a total period of minimum five years. If enacted as part of a contract, the contractor will repair or replace parts per the warranty for the length of this warranty at no cost to the client.
- Manufacturers shall provide phone and online support 24/5.
- Manufacturers shall provide support and repair of product for a minimum of 5 years after the product has been removed from the market.
- The manufacturer shall provide an advanced replacement process, where products within warranty period shall be replaced by a replacement product before the faulty product is returned.

  This should either be done free of charge or as a selectable option. This service may also be extended beyond the standard warranty.

  In cases where a product is found to be defective within 30 days from the date of purchase, the manufacturer shall provide a new product.

Cybersecurity

- In order to support the lifetime cyber security process for this specification, only cameras from the original supplier with the firmware are allowed. Therefore, all necessary information about original manufacturer need to be provided. Transparency about the total supply chain from the device manufacturer to installer is essential for this process.
- No OEM or ODM products will be approved as part of the installation of the security system unless as detailed risk process is included to any critical vulnerabilities and may be identified in the future.
- The Contractor shall follow network security best practices, based on a standardized framework

(NIST, ISO, SANS) and the manufacturers cyber hardening recommendations.

- Manufacturers shall have a documented and communicated vulnerability policy detailing how it manages and responds to security vulnerabilities and how this is communicated to the market
- Connected devices must not communicate with any 3rd party server outside the network, except for explicitly approved connections. Core network services (DHCP, DNS, NTP, etc.) shall be expected to be provided within the network.
- Connected devices shall not include any hardcoded credentials ("backdoors"). Any process required to do a factory reset or recover for a lost password on a device must include a physical presence test, such as pressing a reset button.
- Connected devices shall support the use of HTTPS and SSL/TLS, providing the ability to upload signed certificates to encrypt and secure authentication and communication of both administration data and video streams.
- Devices must be HTTPS from start, have a password strength indicator, password prompts.
- Connected devices must support individual client certificates (802.1X) and server certificates (HTTPS).
- Connected devices shall provide support for restricting access to pre-defined IP addresses only, so-called IP address filtering.
- Connected devices shall support multiple user accounts with different privileges, secured by passwords with up to 64 characters which are stored as cryptographich digest (not in clear text), and be equipped with a strength indicator.
- Vendors and manufacturers must provide a security advisors policy / notification service. The communication channel, should be an opt in service that sit independent of any partner program that the vendor has in place.
- Manufacturers must be Cyber Essentials plus certified in compliance with UK Government guidelines.
- The manufacturer of the device(s) shall offer a

software tool for efficient handling in relation to cybersecurity of the products that are to be used, the following functionalities needs to be included in the tool:

- User and password management
  - Functionality for setting device password for multiple devices at the same time
  - Deploy HTTPS certificates
  - Deploy 802.1x certificates
  - Renew and manage certificates
  - Copy configuration between devices
  - Upgrade firmware
  - Upgrade camera(s) with available LTS firmware
- The device manufacturer shall offer LTS (Long Term Support) firmware, including only stability, performance and security patches. The LTS firmware shall be maintained up to 10 years from when the device was introduced to the market.
- LTS support should retain integrations with other third parties related to original firmware version.
- The device manufacturer must have defined and transparent vulnerability management process including vulnerability policy, contact information, firmware patching, security advisory (vulnerability disclosure) and notification.