Chương V. YÊU CẦU VỀ KỸ THUẬT

1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu:

- Chủ đầu tư: Ban Quản lý Khu kinh tế tỉnh An Giang

- Gói thầu số 04: Thuê dịch vụ công nghệ thông tin Hệ thống camera AI kiểm soát ra vào tại các khu công nghiệp trên địa bàn tỉnh An Giang

- Dự án/Dự toán mua sắm: Thuê dịch vụ công nghệ thông tin Hệ thống camera AI kiểm soát ra vào tại các khu công nghiệp trên địa bàn tỉnh An Giang

- Nguồn vốn: Ngân sách tỉnh (vốn sự nghiệp) 2025 - 2030 và các nguồn kinh phí hợp pháp khác

- Thời hạn thực hiện: 63 tháng, trong đó:

+ Thời gian thuê: 60 tháng (05 năm)

+ Tiến độ, thời gian xây dựng, phát triển, hình thành dịch vụ: 90 ngày (03 tháng) kể từ ngày hợp đồng có hiệu lực.

- Địa điểm: Khu công nghiệp Bình Hòa (xã Bình Hòa), Khu công nghiệp Bình Long (xã Châu Phú), tỉnh An Giang

2. Mục tiêu công việc:

a. Thuê vật tư, thiết bị hệ thống camera AI + khảo sát, lắp đặt, cài đặt:

TT	Hạng mục/Vật tư	Đơn vị tính	Số lượng
A	**Chi phí xây dựng, phát triển hình thành dịch vụ**		
I	**Camera**		
1	Camera nhận diện khuôn mặt	Chiếc	18
II	**Phần mềm quản lý**		
1	Hệ thống phần mềm VMS quản lý Camera Bình Hòa và Bình Long	License	1
2	Module phần mềm nhận diện khuôn mặt	License	18
III	**Hạ tầng**		
1	Tủ kỹ thuật ngoài trời (thiết kế chống nóng)	Chiếc	7
2	Thiết bị cắt lọc sét lan truyền đường nguồn 1 pha	Chiếc	7
3	Switch PoE công nghiệp	Chiếc	7

TT	Hạng mục/Vật tư	Đơn vị tính	Số lượng
4	Thiết bị chuyển mạch (đặt tại KCN)	Chiếc	2
5	Máy chủ Analytics Bình Hòa và Bình Long	Chiếc	1
6	Attomat	Chiếc	7
7	Dây cáp mạng ngoài trời	M	760
8	Triển khai cáp quang F8 4 FO	Mét	4850
9	Hàn ODF 4FO	Cái	14
10	ODF 4 FO (bao gồm pitail)	Cái	14
11	Đế, Bulong và kẹp cáp	Bộ	63
12	Dây đai inox 20x7mm	Mét	450
13	Khóa đai inox	Cái	405
14	Convert AC 1 sợi quang (Bộ 2 đầu)	Cái	12
15	Ổ điện	Chiếc	18
16	Dây cáp điện CVV ngoài trời 2x2.5mm	M	760
17	Mặt bích lắp camera	Chiếc	18
18	Giá treo camera (lắp vị trí cổng số 4, do không có cổng nên lắp trên cột điện);	Cái	1
19	Vật tư phụ kiện lắp đặt (băng dính, lạt nhựa, đinh vít, đai treo tủ, ruột gà, ống nhựa...)	Gói	18
IV	**Triển khai**		
1	Chi phí lắp đặt camera	Chiếc	18
2	Chi phí cài đặt, căn chỉnh, hiệu chỉnh camera kết nối phần mềm	Chiếc	18
3	Lắp đặt tủ kỹ thuật và các thiết bị trong tủ	Gói	7
4	Thi công hệ thống chống sét đường nguồn ở Camera	Gói	7

b) Đào tạo, tập huấn:

STT	Tên Hạng mục	Đơn vị	Số lượng
1	Lớp đào tạo cán bộ quản trị	Lớp	01

2	Lớp đào tạo, tập huấn người sử dụng	Lớp	01

c) Thuê đường truyền:

STT	Tên Hạng mục	Đơn vị	Số lượng
1	Đường truyền chuyên dụng dùng riêng L2VPN tốc độ 150Mbps (Khu CN Bình Hòa)	Line	01
2	Đường truyền chuyên dụng dùng riêng L2VPN tốc độ 80Mbps (Khu CN Bình Long)	Line	01

d) Thuê dịch vụ quản lý máy chủ

STT	Tên Hạng mục	Đơn vị	Số lượng
1	Thuê dịch vụ quản lý máy chủ (địa điểm, tiền điện, nhân sự bảo trì, vận hành…)	Máy chủ	01

3. Yêu cầu kỹ thuật của gói thầu:

3.1. Yêu cầu về chất lượng dịch vụ công nghệ thông tin

*** Yêu cầu chung:**

- Cung cấp trang thiết bị mới 100% và hướng dẫn thực hiện đúng quy trình quản lý, sử dụng.

- Cung cấp phần mềm quản lý đáp ứng các tính năng, yêu cầu phục vụ hệ thống Camera nhận diện khuôn mặt ra/vào khu công nghiệp và hướng dẫn thực hiện đúng quy trình quản lý, sử dụng.

- Phải triển khai, vận hành thử nghiệm hoàn thiện các thiết bị, phần mềm và dịch vụ tại các Khu công nghiệp. Chịu trách nhiệm bảo hành, bảo trì tại nơi sử dụng hệ thống thiết bị, hệ thống cập nhật các bản vá lỗi.

- Sửa chữa thay thế thiết bị, hiệu chỉnh, cập nhật phần mềm tối đa 05 (năm) ngày *(kể từ ngày nhận được thông tin thiết bị đã bị hư hỏng, phần mềm phát sinh sự cố)*. Bảo đảm hệ thống hoạt động ổn định trong suốt quá trình sử dụng dịch vụ.

- Các thiết bị và nội dung phải đảm bảo được bảo mật theo quy định.

*** Chất lượng dịch vụ công nghệ thông tin:**

STT	Tiêu chí chất lượng	Yêu cầu chất lượng cụ thể	Yêu cầu đầu ra	
			Giai đoạn chuẩn bị cung cấp dịch vụ	Giai đoạn thuê dịch vụ
(1)	*(2)*	*(3)*	*(4)*	*(5)*
1	**Nhóm tiêu chí về chức năng nghiệp vụ**			
1.1	Tính đầy đủ của chức năng nghiệp vụ.	100% các chức năng hệ thống đáp ứng yêu cầu nghiệp vụ	100% các chức năng hệ thống đáp ứng yêu cầu nghiệp vụ	100% các chức năng hệ thống đáp ứng yêu cầu nghiệp vụ
1.2	Tính chính xác của các chức năng nghiệp vụ.	Các chức năng nghiệp vụ của hệ thống phải đảm bảo tính chính xác tuyệt đối	Các chức năng nghiệp vụ của hệ thống phải đảm bảo tính chính xác tuyệt đối	Các chức năng nghiệp vụ của hệ thống phải đảm bảo tính chính xác tuyệt đối
1.3	Tính phù hợp của chức năng với nghiệp vụ.	100% các chức năng phù hợp với nghiệp vụ thực tế.	100% các chức năng phù hợp với nghiệp vụ thực tế.	100% các chức năng phù hợp với nghiệp vụ thực tế.
2	**Nhóm tiêu chí về hiệu năng vận hành**			
2.1	Hiệu năng đáp ứng của DVCNTT	Hệ thống cho phép xem lại hoặc xem trực tiếp 64 khung hình cùng lúc Đáp ứng 1000 người xem đồng thời khi stream video lên youtube, facebook… Ghi hình liên tục 24/24	Hệ thống cho phép xem lại hoặc xem trực tiếp 64 khung hình cùng lúc Đáp ứng 1000 người xem đồng thời khi stream video lên youtube, facebook… Ghi hình liên tục 24/24	Hệ thống cho phép xem lại hoặc xem trực tiếp 64 khung hình cùng lúc Đáp ứng 1000 người xem đồng thời khi stream video lên youtube, facebook… Ghi hình liên tục 24/24
2.2	Khả năng mở rộng	- Hệ thống cho phép mở rộng không giới hạn số lượng camera	- Hệ thống cho phép mở rộng không giới hạn số lượng camera	- Hệ thống cho phép mở rộng không giới hạn số lượng camera

STT	Tiêu chí chất lượng	Yêu cầu chất lượng cụ thể	Yêu cầu đầu ra	
			Giai đoạn chuẩn bị cung cấp dịch vụ	**Giai đoạn thuê dịch vụ**
(1)	*(2)*	*(3)*	*(4)*	*(5)*
	của DV CNTT	- Mở rộng thời gian lưu trữ dữ liệu hình ảnh từ camera không giới hạn	- Mở rộng thời gian lưu trữ dữ liệu hình ảnh từ camera không giới hạn	- Mở rộng thời gian lưu trữ dữ liệu hình ảnh từ camera không giới hạn
3	**Nhóm tiêu chí về an toàn, bảo mật thông tin**			
3.1.	Bảo mật thông tin	- Hệ thống quản lý có chức năng phân quyền truy cập - Phải có tường lửa mềm để ngăn chặn truy cập trái phép - Đường truyền kết nối camera phải là đường truyền cáp quang dùng riêng	Không xảy ra các sự cố bảo mật thông tin như đã yêu cầu (cột số 3).	Không xảy ra các sự cố bảo mật thông tin như đã yêu cầu (cột số 3).
3.2	Khả năng truy xuất nguồn gốc	Hệ thống phải có cơ chế tự động ghi nhận tất cả các sự kiện tác động vào hệ thông.	Hệ thống phải có cơ chế tự động ghi nhận tất cả các sự kiện tác động vào hệ thông.	Hệ thống phải có cơ chế tự động ghi nhận tất cả các sự kiện tác động vào hệ thông.
3.3	Cam kết về bảo mật thông tin	- Tất cả các thiết bị trong hệ thống phải được cài đặt mật khẩu truy cập nếu chưa được đặt. Nếu đã đặt mật khẩu thì phải đổi mật khẩu mặt định - Các dữ liệu về mật khẩu người dùng phải được mã hóa	- Tất cả các thiết bị trong hệ thống phải được cài đặt mật khẩu truy cập nếu chưa được đặt. Nếu đã đặt mật khẩu thì phải đổi mật khẩu mặt định - Các dữ liệu về mật khẩu người dùng phải được mã hóa	- Tất cả các thiết bị trong hệ thống phải được cài đặt mật khẩu truy cập nếu chưa được đặt. Nếu đã đặt mật khẩu thì phải đổi mật khẩu mặt định - Các dữ liệu về mật khẩu người dùng phải được mã hóa
4	**Nhóm tiêu chí phi chức năng khác**			

STT	Tiêu chí chất lượng	Yêu cầu chất lượng cụ thể	Yêu cầu đầu ra	
			Giai đoạn chuẩn bị cung cấp dịch vụ	Giai đoạn thuê dịch vụ
(1)	*(2)*	*(3)*	*(4)*	*(5)*
4.1	Tuân thủ các yêu cầu chung về kỹ thuật			
4.1.1	Tuân thủ các tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước	Tuân thủ các tiêu chuẩn kỹ thuật hiện hành về ứng dụng CNTT trong cơ quan nhà nước.	Tuân thủ các tiêu chuẩn kỹ thuật hiện hành về ứng dụng CNTT trong cơ quan nhà nước.	Tuân thủ các tiêu chuẩn kỹ thuật hiện hành về ứng dụng CNTT trong cơ quan nhà nước.
4.1.2	Nền tảng công nghệ	- Công nghệ nén hình ảnh tối thiểu H264 - Sử dụng giải pháp quản lý tập trung	- Công nghệ nén hình ảnh tối thiểu H264 - Sử dụng giải pháp quản lý tập trung	- Công nghệ nén hình ảnh tối thiểu H264 - Sử dụng giải pháp quản lý tập trung
4.2	Khả năng sử dụng			
4.2.1	Khả năng tái sử dụng	Các dữ liệu ghi hình camera có thể được trích xuất 1 cách dễ dàng nhanh chóng phục vụ công tác quản bá du lịch hoặc xử lý lỗi an ninh trật tự…	Các dữ liệu ghi hình camera có thể được trích xuất 1 cách dễ dàng nhanh chóng phục vụ công tác quản bá du lịch hoặc xử lý lỗi an ninh trật tự…	Các dữ liệu ghi hình camera có thể được trích xuất 1 cách dễ dang nhanh chóng phục vụ công tác quản bá du lịch hoặc xử lý lỗi an ninh trật tự…
4.2.2	Khả năng ngăn chặn lỗi cơ bản từ người dùng.	- Có cơ chế khóa mật khẩu khi người dùng nhập sai quá 3 lần - Đối với các loại dữ liệu bắt buộc nhập phải có tính năng lựa chọn từ nội dung sẵn có để tránh việc nhập sai từ người dùng	- Có cơ chế khóa mật khẩu khi người dùng nhập sai quá 3 lần - Đối với các loại dữ liệu bắt buộc nhập phải có tính năng lựa chọn từ nội dung sẵn có để tránh việc nhập sai từ người dùng	- Có cơ chế khóa mật khẩu khi người dùng nhập sai quá 3 lần - Đối với các loại dữ liệu bắt buộc nhập phải có tính năng lựa chọn từ nội dung sẵn có để tránh việc nhập sai từ người dùng

STT	Tiêu chí chất lượng	Yêu cầu chất lượng cụ thể	Yêu cầu đầu ra	
			Giai đoạn chuẩn bị cung cấp dịch vụ	Giai đoạn thuê dịch vụ
(1)	*(2)*	*(3)*	*(4)*	*(5)*
4.2.3	Khả năng truy cập, sử dụng hệ thống đa dạng	- Cho phép người dùng xem hình ảnh camera trực tiếp từ: - Máy tính - Điện thoại. - Máy tính bảng - Trình duyệt - Hoặc ứng dụng riêng	- Cho phép người dùng xem hình ảnh camera trực tiếp từ: - Máy tính - Điện thoại. - Máy tính bảng - Trình duyệt - Hoặc ứng dụng riêng	- Cho phép người dùng xem hình ảnh camera trực tiếp từ: - Máy tính - Điện thoại. - Máy tính bảng - Trình duyệt - Hoặc ứng dụng riêng
4.2.4	Tính dễ học, dễ sử dụng	- Hệ thống hỗ trợ ngôn ngữ tiếng Viêt hoặc tiếng Anh - Giao diện đơn giản - Có chức năng trợ giúp người dùng khi người dùng cần hướng dẫn sử dụng tính năng phần mềm	- Hệ thống hỗ trợ ngôn ngữ tiếng Viêt hoặc tiếng Anh - Giao diện đơn giản - Có chức năng trợ giúp người dùng khi người dùng cần hướng dẫn sử dụng tính năng phần mềm	- Hệ thống hỗ trợ ngôn ngữ tiếng Viêt hoặc tiếng Anh - Giao diện đơn giản - Có chức năng trợ giúp người dùng khi người dùng cần hướng dẫn sử dụng tính năng phần mềm
4.3	Tính tin cậy			
4.3.1	Tính liên tục, sẵn sàng	- Hệ thống phải sẵn sàng phục vụ 99.9% - Khi có sự cố xảy ra phải có lực lượng kỹ thuật xử lý trong vòng 4 giờ	- Hệ thống phải sẵn sàng phục vụ 99.9% - Khi có sự cố xảy ra phải có lực lượng kỹ thuật xử lý trong vòng 4 giờ	- Hệ thống phải sẵn sàng phục vụ 99.9% - Khi có sự cố xảy ra phải có lực lượng kỹ thuật xử lý trong vòng 4 giờ
4.3.2	Khả năng phục hồi sau sự cố	Khi mất điện và có điện trở lại hệ thống tự hoạt động trở lại và ghi hình không cần bất kỳ tác động từ con người	Khi mất điện và có điện trở lại hệ thống tự hoạt động trở lại và ghi hình không cần bất kỳ tác động từ con người	Khi mất điện và có điện trở lại hệ thống tự hoạt động trở lại và ghi hình không cần bất kỳ tác động từ con người

STT	Tiêu chí chất lượng	Yêu cầu chất lượng cụ thể	Yêu cầu đầu ra	
			Giai đoạn chuẩn bị cung cấp dịch vụ	Giai đoạn thuê dịch vụ
(1)	*(2)*	*(3)*	*(4)*	*(5)*
4.4	Khả năng bảo trì			
4.4.1	Khả năng phân tích sự cố	Hệ thống được quy hoạch phân lớp Có sơ đồ mổ tả thông tin kết nối hệ thống	Hệ thống được quy hoạch phân lớp Có sơ đồ mổ tả thông tin kết nối hệ thống	Hệ thống được quy hoạch phân lớp Có sơ đồ mổ tả thông tin kết nối hệ thống
4.4.2	Khả năng thay thế linh hoạt	Cho phép thay thế thiết bị phần cứng khi xảy ra sự cố trên 1 thiết bị mà không ảnh hưởng tới các thiết bị còn lại	Cho phép thay thế thiết bị phần cứng khi xảy ra sự cố trên 1 thiết bị mà không ảnh hưởng tới các thiết bị còn lại	Cho phép thay thế thiết bị phần cứng khi xảy ra sự cố trên 1 thiết bị mà không ảnh hưởng tới các thiết bị còn lại
4.5	Khả năng điều chỉnh			
4.5.1	Khả năng tùy biến toàn bộ hoặc một số thành phần dịch vụ	Hệ thống cho phép tùy biến, thay đổi cấu hình cơ bản trên phần mềm	Hệ thống cho phép tùy biến, thay đổi cấu hình cơ bản trên phần mềm	Hệ thống cho phép tùy biến, thay đổi cấu hình cơ bản trên phần mềm
4.6	Khả năng tích hợp, kết nối			
4.6.1	Phương án kết nối, chia sẻ dữ liệu	Hệ thống cho phép chia sẽ dữ liệu dưới sự quản lý từ phía quản trị hệ thống.	Hệ thống cho phép chia sẽ dữ liệu dưới sự quản lý từ phía quản trị hệ thống.	Hệ thống cho phép chia sẽ dữ liệu dưới sự quản lý từ phía quản trị hệ thống.
4.6.2	Khả năng tích hợp, kết nối với các hệ thống giám sát, các hệ thống của bên thứ ba để phục vụ nhu cầu	Cho phép hệ thống khác kết nối thông qua các API (Application Programming Interface)	Cho phép hệ thống khác kết nối thông qua các API (Application Programming Interface)	Cho phép hệ thống khác kết nối thông qua các API (Application Programming Interface)

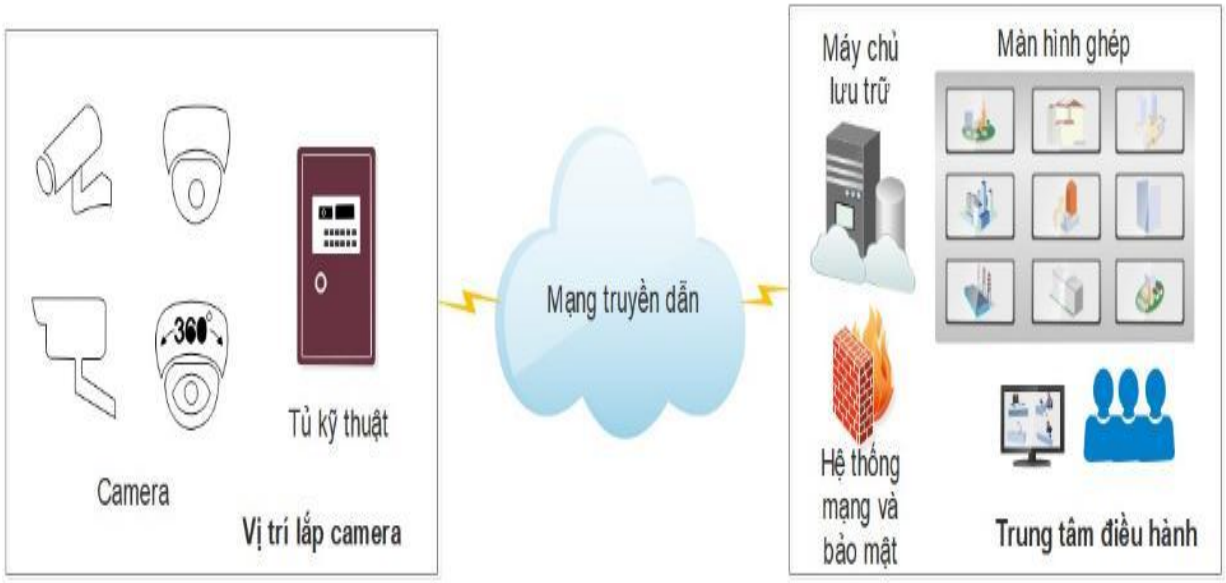
STT	Tiêu chí chất lượng	Yêu cầu chất lượng cụ thể	Yêu cầu đầu ra	
			Giai đoạn chuẩn bị cung cấp dịch vụ	Giai đoạn thuê dịch vụ
(1)	*(2)*	*(3)*	*(4)*	*(5)*
	quản lý, theo dõi, giám sát của bên thuê dịch vụ			
4.7	Mức độ sử dụng, khai thác của DVCNTT trong kỳ đánh giá	Khai thai tối đa năng lực thiết bị	Khai thai tối đa năng lực thiết bị	Khai thai tối đa năng lực thiết bị
5	**Nhóm tiêu chí về sự hài lòng của người sử dụng**			
5.1	Tính kịp thời	Cung cấp dịch vụ đảm bảo đúng thời gian, tiến độ theo hợp đồng	Cung cấp dịch vụ đảm bảo đúng thời gian, tiến độ theo hợp đồng	Cung cấp dịch vụ đảm bảo đúng thời gian, tiến độ theo hợp đồng
5.2	Phản hồi của người sử dụng	Góp ý trực tiếp thông qua hệ thống tổng đài	Góp ý trực tiếp thông qua hệ thống tổng đài	Góp ý trực tiếp thông qua hệ thống tổng đài
5.3	Khả năng hỗ trợ người dùng	Xư lý sự cố mất dịch vụ, mất kết nối camera trong vòng 4h Trường hợp phải thay thế thiết bị do hỏng hóc từ nhà cung cấp thì thời giant hay thế tối thiểu 24 giờ	Xư lý sự cố mất dịch vụ, mất kết nối camera trong vòng 4h Trường hợp phải thay thế thiết bị do hỏng hóc từ nhà cung cấp thì thời giant hay thế tối thiểu 24 giờ	Xư lý sự cố mất dịch vụ, mất kết nối camera trong vòng 4h Trường hợp phải thay thế thiết bị do hỏng hóc từ nhà cung cấp thì thời giant hay thế tối thiểu 24 giờ
5.4	Thái độ phục vụ	Thân thiên, niểm nở	Thân thiên, niểm nở	Thân thiên, niểm nở

STT	Tiêu chí chất lượng	Yêu cầu chất lượng cụ thể	Yêu cầu đầu ra	
			Giai đoạn chuẩn bị cung cấp dịch vụ	Giai đoạn thuê dịch vụ
(1)	*(2)*	*(3)*	*(4)*	*(5)*
6	**Nhóm tiêu chí về quản lý dịch vụ**			
6.1	Tuân thủ các quy trình	Nhà cung cấp tuân thủ các quy trình cung cấp thiết bị công nghệ thông tin	Nhà cung cấp tuân thủ các quy trình cung cấp thiết bị công nghệ thông tin	Nhà cung cấp tuân thủ các quy trình cung cấp thiết bị công nghệ thông tin
6.2	Môi trường làm việc	Bộ phận kỹ thuật triển khai và bảo trì dịch vụ phải được trang bị bảo hộ lao động và được đào tạo cấp chứng chỉ an toàn lao động.	Bộ phận kỹ thuật triển khai và bảo trì dịch vụ phải được trang bị bảo hộ lao động và được đào tạo cấp chứng chỉ an toàn lao động.	Bộ phận kỹ thuật triển khai và bảo trì dịch vụ phải được trang bị bảo hộ lao động và được đào tạo cấp chứng chỉ an toàn lao động.
6.3	Báo cáo dịch vụ	Hệ thống cho phép xuất báo cáo chất lượng dịch vụ trực tuyến	Hệ thống cho phép xuất báo cáo chất lượng dịch vụ trực tuyến	Hệ thống cho phép xuất báo cáo chất lượng dịch vụ trực tuyến
6.4	Quản lý tính sẵn sàng và tính liên tục của dịch vụ	Hệ thống phải có hồ sơ lưu trữ về tình hình hoạt động của thiết bị để phục vụ bảo trì bảo dưỡng đảm bảo tính liên tục của dịch vụ Đối với đường truyền kết nối phải có tính năng phát hiện mất kết nối thông báo cho người quản trị	Hệ thống phải có hồ sơ lưu trữ về tình hình hoạt động của thiết bị để phục vụ bảo trì bảo dưỡng đảm bảo tính liên tục của dịch vụ Đối với đường truyền kết nối phải có tính năng phát hiện mất kết nối thông báo cho người quản trị	Hệ thống phải có hồ sơ lưu trữ về tình hình hoạt động của thiết bị để phục vụ bảo trì bảo dưỡng đảm bảo tính liên tục của dịch vụ Đối với đường truyền kết nối phải có tính năng phát hiện mất kết nối thông báo cho người quản trị
6.6	Quản lý thay đổi	Phải có hồ sơ lưu thông tin thay đổi, tác động hệ thống	Có hồ sơ lưu thông tin thay đổi, tác động hệ thống	Có hồ sơ lưu thông tin thay đổi, tác động hệ thống

STT	Tiêu chí chất lượng	Yêu cầu chất lượng cụ thể	Yêu cầu đầu ra	
			Giai đoạn chuẩn bị cung cấp dịch vụ	Giai đoạn thuê dịch vụ
(1)	*(2)*	*(3)*	*(4)*	*(5)*
6.7	Quản lý và triển khai phiên bản	Có hồ sơ lưu trữ, quản lý thông tin các phiên bản nâng cấp sữa chữa hệ thống	Có hồ sơ lưu trữ, quản lý thông tin các phiên bản nâng cấp sữa chữa hệ thống	Có hồ sơ lưu trữ, quản lý thông tin các phiên bản nâng cấp sữa chữa hệ thống

3.2. Mô hình tổng thể

3.2.1. Mô hình kiến trúc vật lý hệ thống giám sát



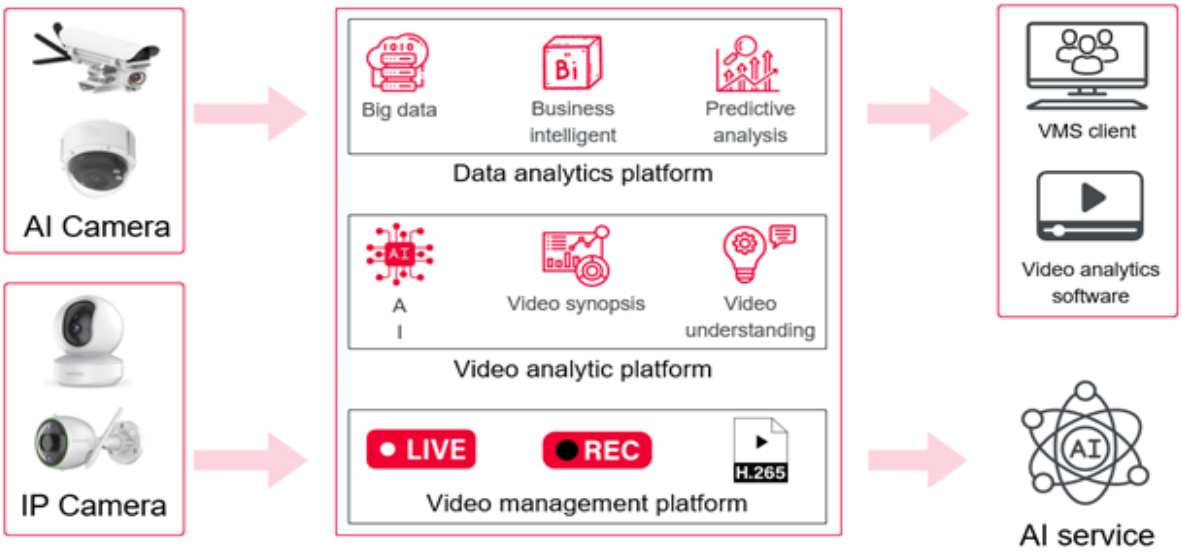
- Thiết bị lắp đặt tại các điểm trọng yếu: bao gồm các Camera chuyên dụng; bộ chuyển đổi tín hiệu quang điện, thiết bị điện, điện tử và cơ khí …

- Trung tâm điều hành: Thực thi toàn bộ quy trình xử lý và thực hiện quản lý, lưu trữ dữ liệu của hệ thống. Trung tâm xử lý được trang bị hệ thống điều khiển, lưu trữ, xử lý dữ liệu Video, màn hình hiển thị hình ảnh cỡ lớn và các thiết bị tin học bao gồm máy chủ, máy trạm, máy in, hệ thống quản trị cơ sở dữ liệu và các phần mềm ứng dụng...

- Mạng truyền dẫn: Thực hiện việc kết nối thiết bị được lắp đặt trên tuyến đường với Trung tâm xử lý cũng như giữa các thiết bị được lắp đặt trên tuyến với nhau và giữa các trung tâm với nhau. Mạng truyền dẫn xây dựng trên hệ thống cáp quang độc lập truyền dẫn giữa các thiết bị với trung tâm xử lý và các trạm giám sát. Vì vậy, tốc độ lên đến Gbps.

Với các thiết bị được trang bị trên tuyến thì cần tối thiểu kênh truyền dẫn:

+ 10 Mbps cho 1 camera đã nén tín hiệu chuẩn H.264



3.2.2. Kiến trúc tổng thể Trung tâm giám sát, điều hành

Hệ thống máy chủ sẽ được đặt tại Trung tâm công nghệ thông tin và truyền thông (Sở Thông tin và Truyền thông) điều hành hoạt động của toàn bộ hệ thống, Ban Quản lý Khu kinh tế tỉnh An Giang sẽ quản lý tổng thể và được cấp tài khoản giám sát tư xa. Tại các Khu Công nghiệp sẽ được trang bị các camera, máy tính để khai thác hệ thống. Tại đây hình ảnh từ tất cả các Camera tại các điểm lắp đặt được truyền tải về thông qua hệ thống mạng chuyên dụng bảo mật cao. Phòng Giám sát được trang bị các màn hình kích thước lớn phục vụ xử lý cùng lúc dữ liệu hành ảnh của nhiều camera và nhiều tác vụ khác của hệ thống. Các thiết bị được lắp đặt tại đây bao gồm: Các thiết bị hiển thị hình ảnh, các màn hình lớn, thiết bị điều kiển Camera AI, thiết bị lưu trữ dự phòng….

Hệ thống Camera AI tại cửa ra vào khu công nghiệp sẽ kết nối nhiều camera từ nhiều điểm với khoảng cách kết nối xa vì vậy cần có một đường truyền chuyên dụng dùng riêng L2VPN cho Hệ thống, đường truyền chuyên dụng phải phù hợp với cấu trúc, công nghệ mạng hiện có và xu hướng phát triển công nghệ mới trên thế giới, đáp ứng được các yêu cầu về dịch vụ trong công tác quản lý, điều hành và có khả năng nâng cấp mở rộng trong tương lai.

- Hệ thống truyền dẫn có thể triển khai linh động.

• Camera AI: camera quang học cố định có chức năng phân tích hình ảnh phát hiện đối tượng người/xe.

- Máy chủ quản lý, ghi hình: ghi hình và quản lý tập trung tất cả các camera trong hệ thống. Phân phối luồng hình ảnh tới các máy khai thác, cho phép xem trực tiếp, xem lại.

- Máy tính khai thác: máy tính để bàn cấu hình cao kèm màn hình để thực hiện các tác vụ tra cứu, trích xuất hình ảnh của cán bộ vận hành.

- Màn hình tivi: nhận các tín hiệu hình ảnh từ máy tính khai thác và tạo kịch bản hiển thị các cảnh báo từ hệ thống máy chủ nhận diện người lạ mặt xâm nhập hoặc cảnh báo Blacklist danh sách đối tượng nguy hiểm đang có âm mưu xâm nhập khu công nghiệp.

*** Nguyên lý hoạt động:**

- Tất cả các camera truyền luồng hình ảnh tới máy chủ quản lý ghi hình thông qua chuẩn RTSP. Máy chủ quản lý ghi hình thu thập tập các luồng tín hiệu video và lưu vào bộ nhớ lưu trữ video chuyên dụng. Video được lưu dưới dạng file với cấu trúc MP4 chuẩn nén H264 có thể trích xuất và xem trên các ứng dụng video thông dụng.

- Camera AI tự động phân tích hình ảnh liên tục để phát hiện đối tượng và các đặc trưng của đối tượng như màu sắc, khuôn mặt và gửi tới máy chủ để quản lý lưu trữ phục vụ tra cứu.

- Trên các máy tính khai thác cài đặt phần mềm hiển thị hình ảnh có khả năng kết nối với Máy chủ ghi hình để nhận luồng video và giải mã ra hình ảnh.

- Bộ điều khiển kết hợp nhiều lưới video để đưa lên màn hình lớn để đồng thời quan sát được tất cả camera trong hệ thống.

- Trên các máy vận hành cài đặt phần mềm quản lý hình ảnh kết nối với Máy chủ ghi hình cho phép người dùng xem trực tiếp, xem lại và tra cứu sự kiện, tra cứu đối tượng theo nhiều tiêu chí như thời gian, địa điểm, loại đối tượng.

3.2.3. Giải pháp định danh và xác thực điện tử sử dụng CCCD gắn chip

a. Quy trình xác thực ID Check kết nối RAR-C06

Mô hình cung cấp dịch vụ của Trung tâm RAR đối với dịch vụ xác thực thẻ CCCD gắn chip của Bộ Công An

b. Khi triển khai hệ thống ID Check kết nối với RAR-06:

- ✓ **OCR:** Bóc tách thông tin trong giấy tờ tùy thân với tỉ lệ chính xác lên đạt hơn 98%.
- ✓ **NFC:** Đọc thông tin trong Chip của CCCD gắn chip bằng NFC với tỉ lệ chính xác 100%.
- ✓ **Fraud detection:** Xác định tính chính xác của các thông tin trên Giấy tờ tùy thân (FAR<=1.5%).
- ✓ **Liveness detection:** Xác minh người thực hiện là thực thể sống, độ chính xác đạt FAR ≤ 1%.
- ✓ **Face Matching:** Đối sánh khuôn mặt, độ chính xác đạt FAR ≤ 0.5%, TAR ≥ 99%.

c. Các tính năng chính của IDCheck

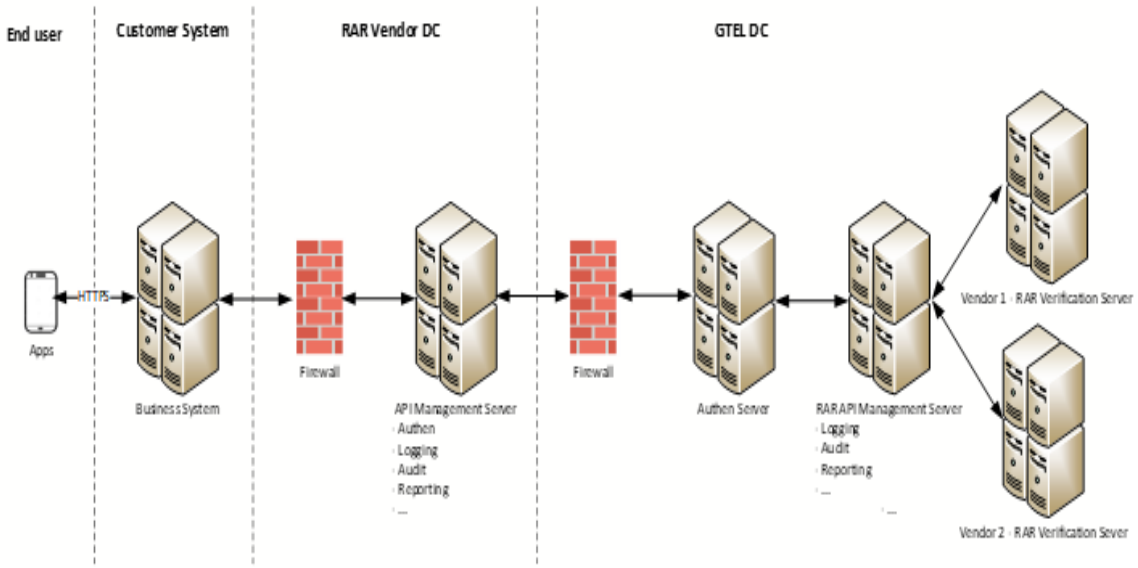
- **Xác thực chân dung**

Phát hiện các khuôn mặt không đảm bảo chất lượng: quá mờ, quá tối/sáng, bị che khuất, nhắm mắt..

Phát hiện và ngăn chặn các trường hợp không phải người thật, gian lận bằng các hình thức: Đeo mặt nạ, deepfake, mặt 3D, chụp qua thiết bị,..

- **Xác minh ảnh chụp CCCD**

Phát hiện ảnh CCCD gắn chip không đảm bảo chất lượng: quá mờ, quá tối/sáng, giấy tờ bị bẩn, bị che viền, chụp không đầy đủ, có vật lạ bên trong..



Phát hiện và ngăn chặn các trường hợp ảnh CCCD gắn chip không phải bản gốc, không còn giá trị sử dụng: bị cắt góc, đục lỗ, dán đè ảnh, photo, in màu, bị chỉnh sửa, chụp qua màn hình thiết bị, giấy tờ bị hết hạn.

- **Truy xuất thông tin khuôn mặt (Face search, 1:N):** Xây dựng cơ sở dữ liệu đặc trưng của khuôn mặt giúp kiểm tra và xác thực chéo dữ liệu, tối đa hóa khả năng phát hiện giả mạo và đảm bảo sự an toàn cho người dùng
- **Đối sánh khuôn mặt (Face matching, 1:1):** Kiểm tra khuôn mặt trong Chip và ảnh chụp khuôn mặt KH tại thời điểm đăng ký dịch vụ có cùng một người hay không, đảm bảo CCCD sử dụng đăng ký dịch vụ là của đúng KH đang tương tác.
- **Bóc tách thông tin CCCD gắn chip (OCR):** Nhận dạng và bóc tách các trường thông tin từ ảnh chụp mặt trước và mặt sau của Căn cước công dân gắn chip.
- **Quét mã QR trên CCCD gắn chip:** Mã QR: Số căn cước công dân gắn chip, số chứng minh nhân dân cũ (nếu có), họ và tên, ngày tháng năm sinh, giới tính, địa chỉ thường trú.
- **Quét chuỗi MRZ mặt sau CCCD gắn chip:** Định dạng chuỗi MRZ tuân theo tiêu chuẩn quốc tế ICAO 9303 (Machine Readable Travel Documents)
- **Trích xuất thông tin trong Chip của CCCD gắn chip:** Đọc thông tin trong thẻ chíp của CCCD gắn chip bằng công nghệ từ trường gần NFC. Đọc đầy đủ và chính xác 18 trường thông tin trong Chip, giúp giảm thiểu rủi ro giả mạo giấy tờ so với việc xác thực giấy tờ bằng công nghệ OCR.
- **Xác thực dữ liệu:** Xác thực tính toàn vẹn và tính xác thực của dữ liệu được xác minh theo tiêu chuẩn ICAO. Dữ liệu được xác thực bằng cách băm nội dung và so sánh kết quả với giá trị băm tương ứng trong SOD.
- **Xác thực chip:** Xác minh Chip không bị sao chép, là bản gốc và thiết lập các khóa mã hóa mới (khóa mã hóa, khóa xác thực thông báo) cho giao tiếp được mã hóa giữa Hệ thống kiểm tra và Chip.
- **Xác thực ký số với RAR-C06:** Xác thực chữ ký số với RAR-C06 đảm bảo chip được phát hành bởi Bộ Công an. Đây là mức bảo mật cấp cao nhất để xác thực toàn bộ thông tin khách hàng, đảm bảo tính pháp lý cho nghiệp vụ xác thực.
- **Tái sử dụng kết quả xác thực:** Xây dựng cơ sở dữ liệu kết quả xác thực chữ ký số với Bộ Công an, cho phép tái sử dụng lại kết quả cho

lần xác thực tiếp theo với cùng thẻ CCCD gắn chip. Giúp tối ưu hóa tốc độ xử lý, đảm bảo độ chính xác và tiết kiệm chi phí khi gửi yêu cầu xác thực.

3.2.4. Giải pháp camera giám sát:

Yêu cầu cơ bản

Hệ thống bao gồm các camera quang học có tích hợp công nghệ phân tích hình ảnh thông minh dùng trí tuệ nhân tạo AI tự động phát hiện chuyển động, phát hiện đối tượng người/xe/ bao gồm các thông tin chi tiết như màu sắc đối tượng, khuôn mặt, khuôn mặt có đeo khẩu trang.

Camera AI nhận diện khuôn mặt

Camera AI có thể hiểu là giải pháp tích hợp, cung cấp hệ thống camera an ninh thông minh sử dụng trí tuệ nhân tạo tự động nhận dạng, phát hiện sự kiện, hành vi một cách chính xác… giúp đáp ứng các nhu cầu về kiểm soát an ninh, phân tích dữ liệu và cung cấp thông tin cho các đơn vị, tổ chức.

Hệ thống camera AI trở nên ngày càng thông minh cho phép xây dựng cơ sở dữ liệu về các mối đe dọa tiềm ẩn và phản ứng nhanh chóng với các sự việc đó. Điều này giúp hệ thống "Tự học" và cảnh báo về sự kiện đáng nghi. Chính vì thế, các cảnh báo sẽ ngày càng chính xác và đáng tin cậy hơn.

Các đặc điểm ở người Camera AI có thể phát hiện được là: khuôn mặt, giới tính, màu sắc quần áo, độ tuổi, trang phục/khẩu trang

Giải pháp Camera AI còn gọi là giải pháp xử lý tại biên vì các tác vụ xử lý phân tích hình ảnh thực hiện ngay trên camera không phải truyền hình ảnh về trung tâm xử lý. Vì vậy mang lại lợi thế về khả năng triển khai nhanh chóng, gọn nhẹ tiết kiệm chi phí.

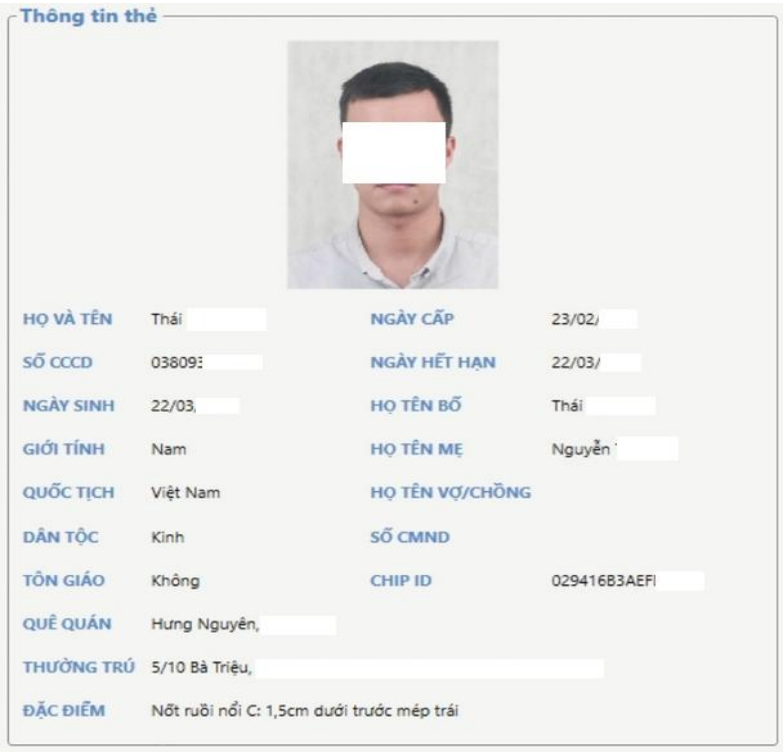
Giải pháp nhận diện khuôn mặt Công nhân ra vào Khu công nghiệp:

Với những tính năng đa dạng và lợi ích trên đề xuất triển khai sử dụng Camera AI tại cổng ra vào khu công nghiệp để giám sát các đối tượng người ra vào. Cụ thể như sau:

Bước 1: Công nhân thực hiện xác thực thẻ CCCD bằng đầu đọc CCCD thông qua ID Check. Cụ thể thao tác thực hiện:

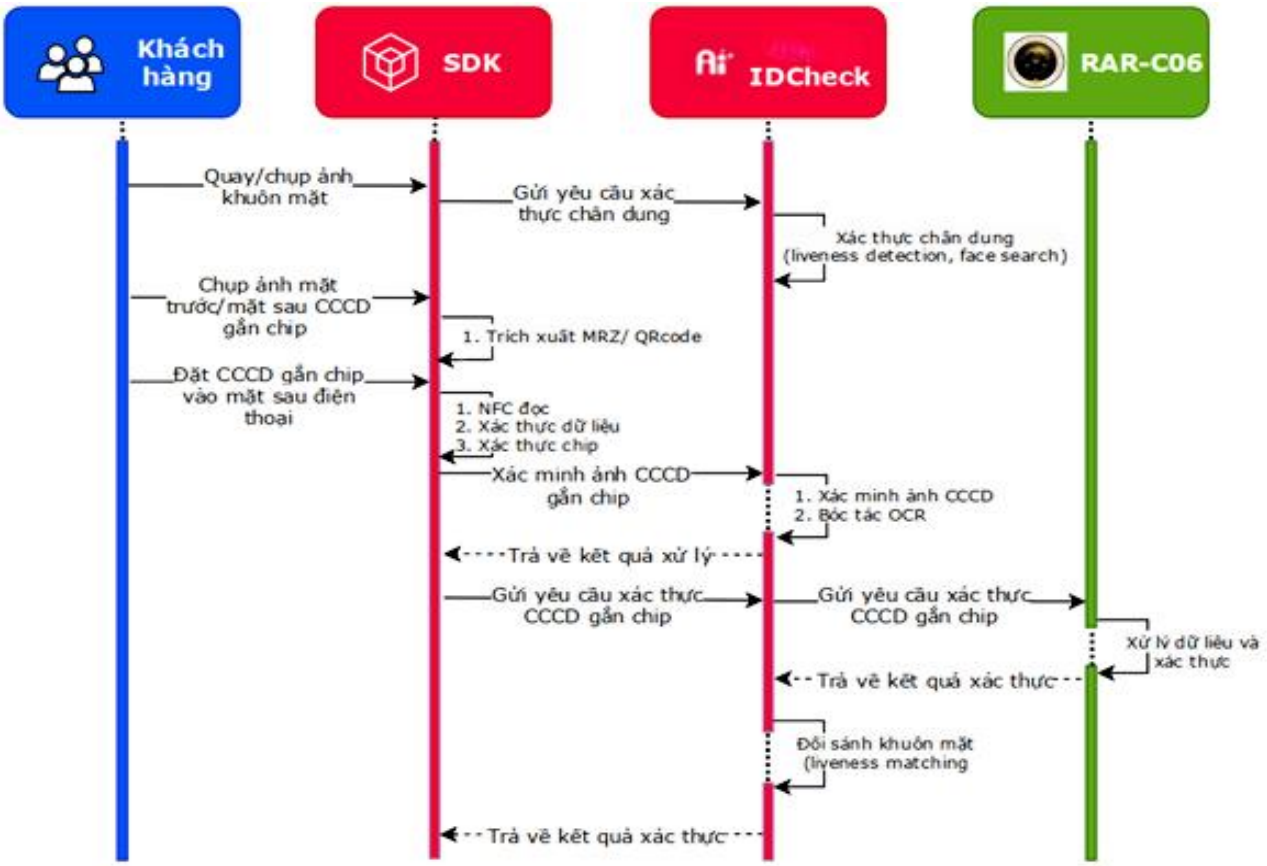
Công nhân: Chụp ảnh mặt trước/mặt sau CCCD đưa vào thiết bị đọc CCCD

Thiết bị đọc CCCD (SDK): gửi yêu cầu xác thực đến RAR-C06



Thông tin thẻ

HỌ VÀ TÊN	Thái	NGÀY CẤP	23/02/
SỐ CCCD	038093	NGÀY HẾT HẠN	22/03/
NGÀY SINH	22/03,	HỌ TÊN BỐ	Thái
GIỚI TÍNH	Nam	HỌ TÊN MẸ	Nguyễn
QUỐC TỊCH	Việt Nam	HỌ TÊN VỢ/CHỒNG	
DÂN TỘC	Kinh	SỐ CMND	
TÔN GIÁO	Không	CHIP ID	029416B3AEFI
QUÊ QUÁN	Hưng Nguyên,		
THƯỜNG TRÚ	5/10 Bà Triệu,		
ĐẶC ĐIỂM	Nốt ruồi nổi C: 1,5cm dưới trước mép trái		



Mô hình kết nối xác thực CCCD dến RAR-06

Bước 2: Lập CSDL khuôn mặt Công nhân trong KCN để định danh nhận diện thông tin. Bao gồm: họ tên, ngày tháng năm sinh, số CCCD, Cty đang làm việc, chức vụ trong doanh nghiệp…

Bước 3: CAM AI hoạt động nhận diện Công nhân ra vào. Quy định Công nhân ra vào khu công nghiệp phải dừng xe tắt máy dẫn bộ vào cổng hoặc chạy xe với tốc độ dưới 5 Km/h. Khi ra vào công nhân phải cởi khẩu trang, chỉ đội mũ bảo hiểm đi vào. Nếu Công nhân đội mũ bảo hiểm, đeo khẩu trang và đeo kính chống bụi thì Camera AI không thể nhận diện được đối tượng chính xác.

Hình ảnh sẽ tập trung chuyển về trung tâm giám sát bảo vệ của Khu Công nghiệp để NV Bảo vệ có thể quan sát phát hiện những đối tượng nghi vấn.

Nếu có người lạ hệ thống sẽ tự động cảnh báo cho NV bảo vệ trực tại vị trí giám sát. NV Bảo vệ sẽ yêu cầu người lạ phải khai báo kiểm tra CCCD và khai báo thông tin cá nhân, mục đích ra vào KCN để làm gì để quản lý. Sau khi định danh xong có thể vào khu công nghiệp để làm việc. Khi người lạ đi ra hệ thống sẽ cảnh báo thời gian vào ra của người lạ ghi nhận thông tin dữ liệu phục vụ cho việc điều tra giám sát sau này (nếu có).

Bước 4: Đẩy dữ liệu về hệ thống Quản lý tập trung tại:

+ Hệ thống máy chủ đặt tại Trung tâm CNTT và truyền thông

+ Trung tâm điều hành thông mình (IOC) tỉnh An Giang

+ Hệ thống Giám sát An ninh PC06 Công an tỉnh

3.3. Camera giám sát

Camera AI: Các camera quang học có tích hợp công nghệ phân tích hình ảnh thông minh dùng trí tuệ nhân tạo AI tự động phát hiện chuyển động, phát hiện đối tượng người/xe/ bao gồm các thông tin chi tiết như màu sắc đối tượng, khuôn mặt, khuôn mặt có đeo khẩu trang.

3.3.1. Yêu cầu thông số kỹ thuật

- Khoảng cách chiếu xa của đèn IR: ≥ 40m

- Đầu vào nguồn điện: IEEE 802.3af Class3 PoE

- Kích thước cảm biến: 1/1.8" Progressive CMOS

- Độ phân giải lớn nhất xuất ra màn hình: ≥ 3840 × 2160

- Tốc độ khung hình tối đa: ≥ 30 fps @3840×2160

- Độ dài tiêu cự: 4.4 ~ 10 (mm)

- Loại cửa điều sáng: P-iris

- Tự động bật đèn hồng ngoại ban đêm: Hỗ trợ

- Bộ mã hóa video: H241/H242

- Kiểu kết nối mạng, Ethernet RJ45: 100/1000 Mbps

- Tiêu chuẩn về độ kín khít, chống nước: ≥ IP66

- Tiêu chuẩn về mức Độ chống va đập cơ học của vỏ thiết bị: IK10

- Khoảng nhiệt độ môi trường mà thiết bị có thể hoạt động bình thường: -50oC - 50oC

- Khoảng độ ẩm môi trường mà thiết bị có thể hoạt động bình thường: 0 – 95%

- Số luồng video streaming đồng thời: ≥ 2

- Ứng dụng phân tích video Hỗ trợ : Smart VCA

- Các giao thức mạng hỗ trợ: ONVIF, DHCP, DNS, HTTP, HTTPS, IPv4, IPv6,RTSP/RTP/RTCP, NTP, TCP

- Khả năng bảo mật: HTTPS, password protection, signed firmware

- Nhận diện khuôn mặt nhân viên, khách hàng:

- Nhận diện khuôn mặt (xử lý trực tiếp trên camera):
- Độ chính xác nhận diện khuôn mặt: ≥ 99%
- Số lượng người hỗ trợ quản lý: ≥ 1.000
- Số lượng người xử lý đồng thời: ≥ 5
- Thời gian xử lý nhận diện: ≤ 200ms
- Kiểm soát ra vào:
- Hiển thị thông tin nhận diện người vào ra: Tên, Hình ảnh, Độ chính xác
- Hỗ trợ Hiển thị đồng thời nhiều vị trí giám sát vào ra: có
- Báo cáo chấm công theo cá nhân, phòng ban: Có
- Quản lý lịch sử vào ra:
- Thông tin lịch sử: Nhân viên, Khách, Người lạ
- Thời gian lưu trữ lịch sử: ≥ 90 ngày
- Hỗ trợ tìm kiếm: Tên, Thời gian, Vị trí
- Thông tin lưu trữ lịch sử: Thời gian, ảnh, video
- Đọc biển Số phương tiện
- Khoảng nhận diện biển số:≤ 10m (zoom 1x) và ≥ 50m (zoom 10x)
- Độ chính xác nhận diện: ≥ 98.5 %
- Quản lý lịch sử vào ra:
- Thông tin lịch sử: Phương tiện đã đăng ký, chưa đăng ký
- Thời gian lưu trữ lịch sử: ≥ 90 ngày
- Hỗ trợ tìm kiếm: Tên, Thời gian, Vị trí
- Thông tin lưu trữ lịch sử: Thời gian, ảnh, video

3.3.2. Yêu cầu an toàn thông tin mạng cơ bản

Thiết bị Camera giám sát phải có đầy đủ các tính năng đảm bảo đạt yêu cầu an toàn thông tin mạng cơ bản theo Quyết định số 724/QĐ-BTTTT ngày 07/5/2024 của Bộ Thông tin và Truyền thông về việc ban hành Bộ tiêu chí về yêu cầu an toàn thông tin mạng cơ bản cho camera giám sát, cụ thể:

1. Yêu cầu về tài liệu

Có tài liệu hướng dẫn sử dụng sản phẩm cho người sử dụng.

2. Quản lý xác thực

2.1. Phòng chống tấn công vét cạn

a) Có chức năng quản trị hệ thống cho phép thay đổi thời gian khóa, số lần đăng nhập sai và khoảng thời gian đăng nhập sai liên tục; Thiết lập mặc định khóa không cho đăng nhập trong vòng 5 phút, sau khi đăng nhập thất bại 5 lần liên tục trong khoảng thời gian 30 giây hoặc ngắn hơn.

b) Chỉ thông tin cho người sử dụng nội dung đăng nhập thành công/thất bại mà không có nội dung khác làm cơ sở thực hiện tấn công vét cạn.

2.2. Quản lý mật khẩu an toàn

a) Có chức năng yêu cầu người dùng bắt buộc thay đổi mật khẩu mặc định hoặc mật khẩu khởi tạo khi sử dụng thiết bị lần đầu tiên.

b) Có chức năng kiểm soát mật khẩu an toàn. Mật khẩu được tạo ra phải có yêu cầu về độ phức tạp đối với mật khẩu (mật khẩu phải có độ dài tối thiểu 8 ký tự, có chữ hoa, chữ thường, chữ số, ký tự đặc biệt).

c) Sử dụng hàm băm SHA-256 hoặc cao hơn.

2.3. Khởi tạo mật khẩu mặc định an toàn

Mật khẩu khởi tạo mặc định trên thiết bị camera và các dịch vụ liên kết (nếu có) phải đáp ứng các yêu cầu sau:

a) Có độ dài tối thiểu 8 ký tự, có chữ hoa, chữ thường, chữ số, ký tự đặc biệt.

b) Cơ chế khởi tạo mật khẩu sử dụng phương pháp sinh mã có giá trị ngẫu nhiên.

c) Cơ chế khởi tạo mật khẩu không dùng các thông tin công khai (ví dụ: địa chỉ MAC; chuỗi định danh Wifi SSID; tên sản phẩm; loại sản phẩm;...).

d) Là khác nhau đối với mỗi thiết bị camera khác nhau.

2.4. Quản lý xác thực

a) Có chức năng xác thực cho phép xác thực nhiều loại đối tượng khác nhau như người dùng hoặc thiết bị với thiết bị với loại giá trị xác thực khác nhau.

b) Mật khẩu lưu trữ trên camera phải được mã hóa.

3. Quản lý lỗ hổng bảo mật

3.1. Yêu cầu đối với hệ thống quản lý lỗ hổng của thiết bị

Nhà sản xuất có hệ thống trực tuyến cho phép tiếp nhận và công bố thông tin về lỗ hổng của thiết bị tới người sử dụng.

3.2. Yêu cầu đối với thông tin công bố lỗ hổng bảo mật của thiết bị

a) Có mô tả về lỗ hổng, phân loại và xác định mức độ nghiêm trọng;

b) Có mô tả về các phiên bản bị ảnh hưởng.

c) Có hướng dẫn cập nhật, xử lý lỗ hổng.

4. Quản lý và thực hiện cập nhật

4.1. Yêu cầu đối với hệ thống quản lý cập nhật

Nhà sản xuất có hệ thống trực tuyến cho phép:

a) Công bố thông tin về các phiên bản cập nhật.

b) Quản lý và thực hiện cập nhật đối với các thiết bị camera có chức năng kết nối Internet.

4.2. Yêu cầu đối với thông tin của phiên bản cập nhật

Thông tin phiên bản cập nhật bao gồm tối thiểu các thông tin:

a) Phiên bản phần mềm hệ thống.

b) Mã kiểm tra an toàn đối với phần mềm hệ thống.

c) Có mô tả về thông tin phần mềm hệ thống được cập nhật.

4.3. Yêu cầu đối với chức năng cập nhật phiên bản qua Internet

a) Chức năng cập nhật phải được thực hiện qua kênh kết nối mạng an toàn có phương pháp mã hóa an toàn đáp ứng yêu cầu tại Mục 6.1 tài liệu này.

b) Có chức năng xác thực trước khi thực hiện cập nhật.

c) Có chức năng thông báo khi có phiên bản cập nhật mới khi người dùng đăng nhập, quản trị thiết bị.

d) Có chức năng thiết lập cho phép thiết bị tự động cập nhật bản vá từ nhà sản xuất.

đ) Có chức năng kiểm tra tính nguyên vẹn của bản cập nhật có sử dụng chữ ký số của nhà sản xuất.

5. Quản lý phiên an toàn

5.1. Quản lý phiên đăng nhập

Thiết bị camera, ứng dụng giao tiếp với người sử dụng có chức năng lựa chọn timeout cho phép tự động đăng xuất ứng dụng sau một khoảng thời gian.

5.2. Tạo khóa phiên an toàn

Tạo khóa phiên cho người sử dụng khi đăng nhập thành công đáp ứng các yêu cầu sau:

a) Khóa phiên không có khả năng bị tấn công vét cạn.

b) Khóa phiên không được sinh cố định, có yếu tố ngẫu nhiên.

c) Khóa phiên không có khả năng bị khôi phục:

d) Có chức năng yêu cầu hủy phiên đăng nhập hoặc hủy phiên đăng nhập cũ khi người dùng đăng nhập lại.

6. Quản lý kênh giao tiếp

6.1. Yêu cầu đối với các giao tiếp kết nối an toàn

a) Sử dụng các phương pháp mã hóa dựa trên các tiêu chuẩn Việt Nam hiện hành hoặc tiêu chuẩn quốc tế tương đương.

b) Phương pháp mã hóa sử dụng phiên bản không tồn tại lỗ hổng, điểm yếu an toàn thông tin mạng được công bố bởi các cơ quan, tổ chức trong nước hoặc nước ngoài.

6.2. Truy cập cấu hình thiết bị an toàn

a) Sử dụng kênh bảo mật an toàn trước khi thực hiện truy cập, cấu hình thiết bị.

b) Kiểm soát truy cập cấu hình thiết bị:

i. Cấp quyền truy cập tối thiểu (chỉ phục vụ việc cấu hình và quản trị thiết bị) với đối tượng xác thực thành công.

ii. Không cấp quyền truy cập đối với đối tượng xác thực thất bại. iii. Không cấp quyền truy cập đối với đối tượng chưa xác thực.

c) Từ chối đối tượng xác thực (người và máy) truy cập khi camera ở trạng thái hoạt động ban đầu đối với:

i. Đối tượng xác thực thành công nhưng không có đủ quyền truy cập.

ii. Đối tượng xác thực thất bại.

iii. Đối tượng chưa xác thực.

Ngoại lệ: Tất cả yêu cầu trên không áp dụng đối với các dịch vụ hệ thống, phục vụ hoạt động của thiết bị camera như: ARP; DHCP; DNS; ICMP; NTP;...

7. Quản lý giao diện

7.1. Bảo mật thông tin xác thực

Ở trạng thái hoạt động ban đầu, khi người sử dụng chưa được xác thực, giao diện mạng của thiết bị chỉ cung cấp các thông tin công khai liên quan đến vận hành và sử dụng thiết bị.

7.2. Quản lý giao diện logic và mạng

a) Các giao diện logic và mạng được kích hoạt khi thiết bị ở trạng thái hoạt động ban đầu phải có mô tả mục đích sử dụng, để giải thích tại sao giao diện được kích hoạt.

b) Có chức năng cho phép kích hoạt hoặc vô hiệu hóa giao diện theo mô tả.

7.3. Quản lý giao diện gỡ lỗi

Giao diện gỡ lỗi phải được mặc định vô hiệu hóa.

7.4. Quản lý giao diện vật lý

a) Có chức năng vô hiệu hóa các cổng kết nối vật lý khi không sử dụng.

b) Tất cả giao diện vật lý mà không sử dụng phải được vô hiệu hóa truy cập ở chế độ cài đặt gốc.

8. Bảo đảm an toàn thông tin dữ liệu người sử dụng

8.1. Bảo vệ dữ liệu cá nhân

Thiết bị camera và các dịch vụ liên kết có tối thiểu tính năng cho phép thiết lập, cấu hình địa điểm tại Việt Nam đối với việc xử lý, lưu trữ và khai thác dữ liệu (như: trên thẻ nhớ/thiết bị ngoại vi, dịch vụ điện toán đám mây đặt tại Việt Nam,...) nhằm đảm bảo tuân thủ quy định của pháp luật Việt Nam về bảo vệ dữ liệu cá nhân.

8.2. Cảm biến thu thập dữ liệu

Tài liệu hướng dẫn sử dụng (hoặc tài liệu tương đương được công bố công khai) phải liệt kê danh mục các cảm biến được sử dụng bởi thiết bị camera và mô tả chức năng, nguyên lý hoạt động của từng cảm biến được thiết bị camera sử dụng.

8.3. Thông báo liên quan đến bảo vệ dữ liệu cá nhân

Trong quá trình khởi tạo, thiết lập, cấu hình thiết bị, phải có giao diện thông báo cho người sử dụng về địa điểm (quốc gia) lưu trữ và xử lý dữ liệu được thu thập bởi thiết bị camera và các dịch vụ liên kết.

8.4. Xóa dữ liệu trên thiết bị camera

a) Có chức năng cho phép người sử dụng xóa dữ liệu được thu thập và lưu trữ trên thiết bị camera.

b) Có chức năng thông báo cho người sử dụng xóa dữ liệu thành công/thất bại trên thiết bị khi thực hiện chức năng xóa.

c) Có chức năng xác nhận người dùng đồng ý xóa dữ liệu trước khi thực hiện xóa.

8.5. Xóa dữ liệu trên dịch vụ liên kết

a) Có chức năng cho phép người sử dụng xóa dữ liệu lưu trữ trên các dịch vụ liên kết.

b) Có chức năng thông báo cho người sử dụng xóa dữ liệu thành công/thất bại trên các dịch vụ liên kết khi thực hiện chức năng xóa.

c) Có chức năng cho phép người sử dụng thiết lập thời gian xóa dữ liệu tự động dữ liệu trên dịch vụ liên kết. Thời gian xóa được người sử dụng thiết lập trên camera hoặc theo thời gian mặc định của nhà sản xuất.

d) Có chức năng xác nhận người sử dụng đồng ý xóa dữ liệu trước khi thực hiện xóa.

9. An toàn ứng dụng

Thiết bị camera phải có các tính năng sau:

a) Kiểm tra tính hợp lệ của dữ liệu đầu vào do người sử dụng nhập hoặc qua giao diện lập trình.

b) Ngăn chặn quá trình xử lý dữ liệu đầu vào vi phạm điều kiện lọc đã định nghĩa trước theo nhà sản xuất.

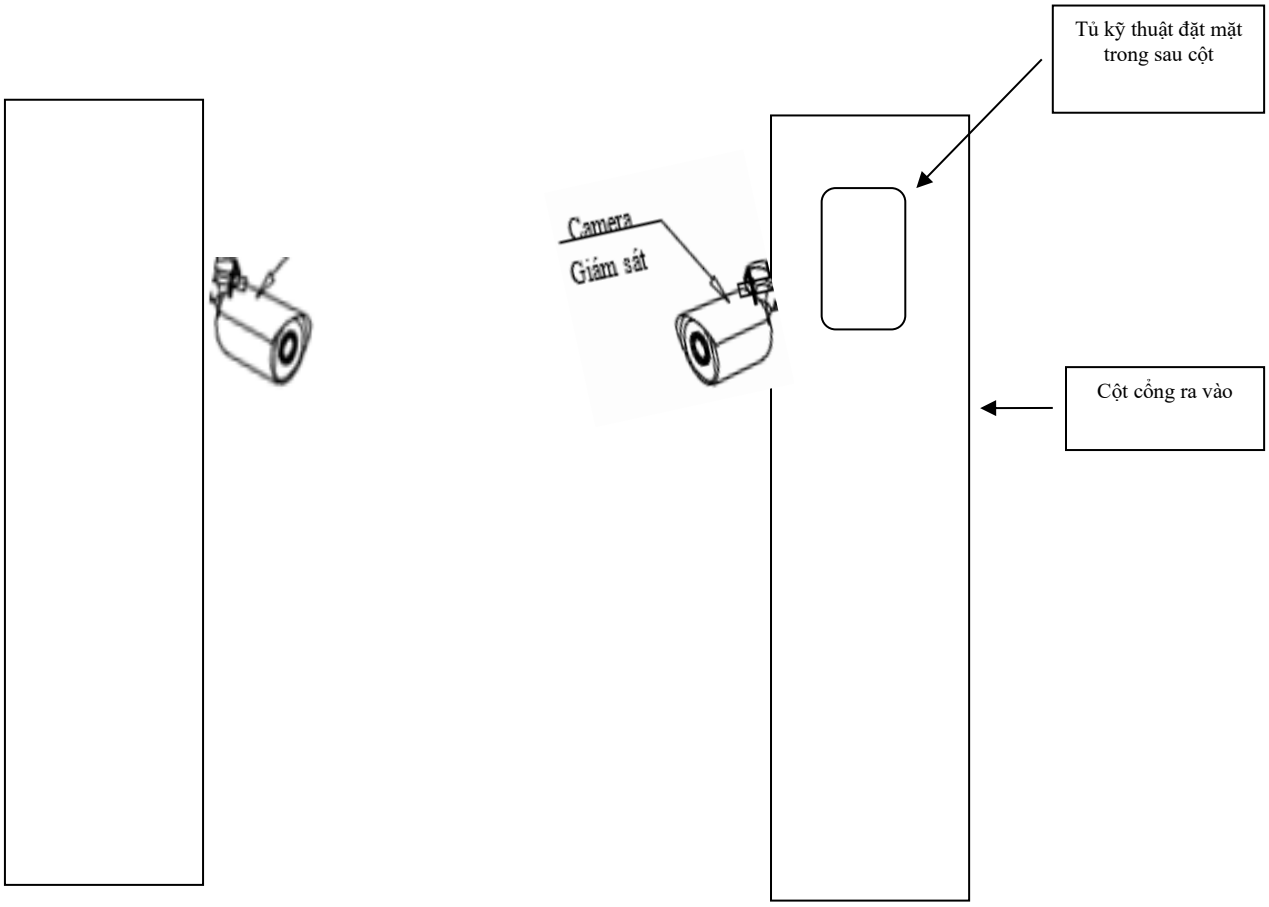
c) Kiểm tra tính hợp lệ của dữ liệu để ngăn chặn các dạng tấn công vào giao diện của thiết bị. Các dạng tấn công bao gồm nhưng không giới hạn những dạng sau: SQL Injection; OS Command Injection; XPath Injection; Remote File Inclusion (RFI); Local File Inclusion (LFI); Cross-Site Scripting (XSS); Cross- Site Request Forgery (CSRF).

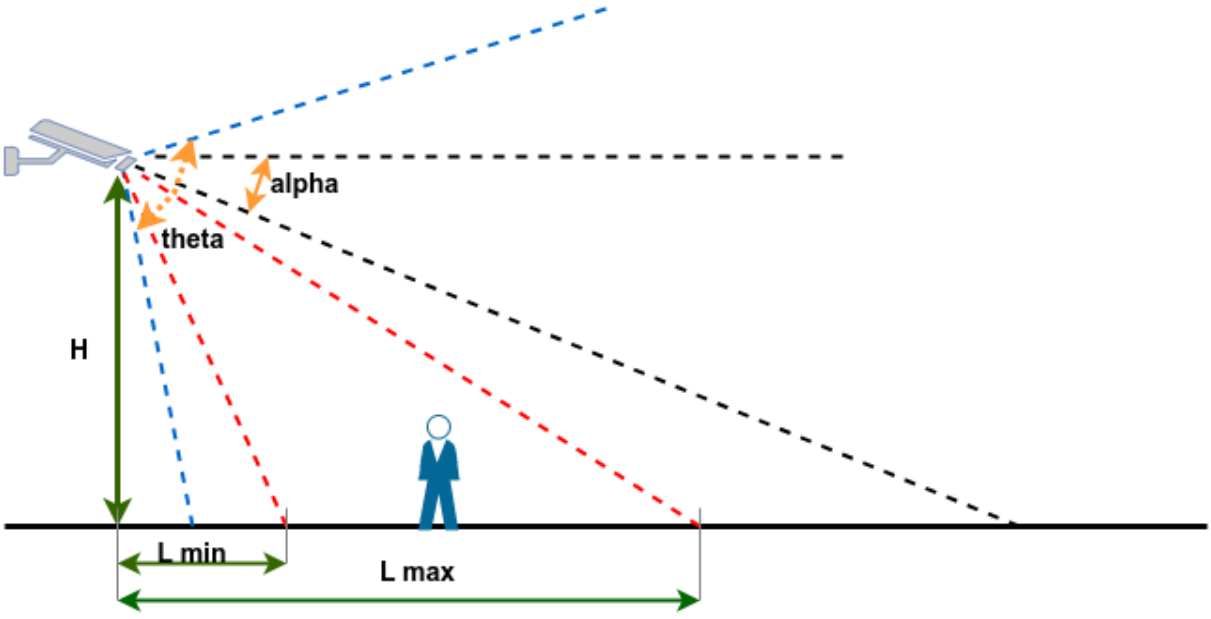
10. Khả năng tự khôi phục lại hệ thống bình thường sau sự cố

Trong trường hợp thiết bị phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), thiết bị đảm bảo hoạt động bình thường trong lần khởi động kế tiếp.

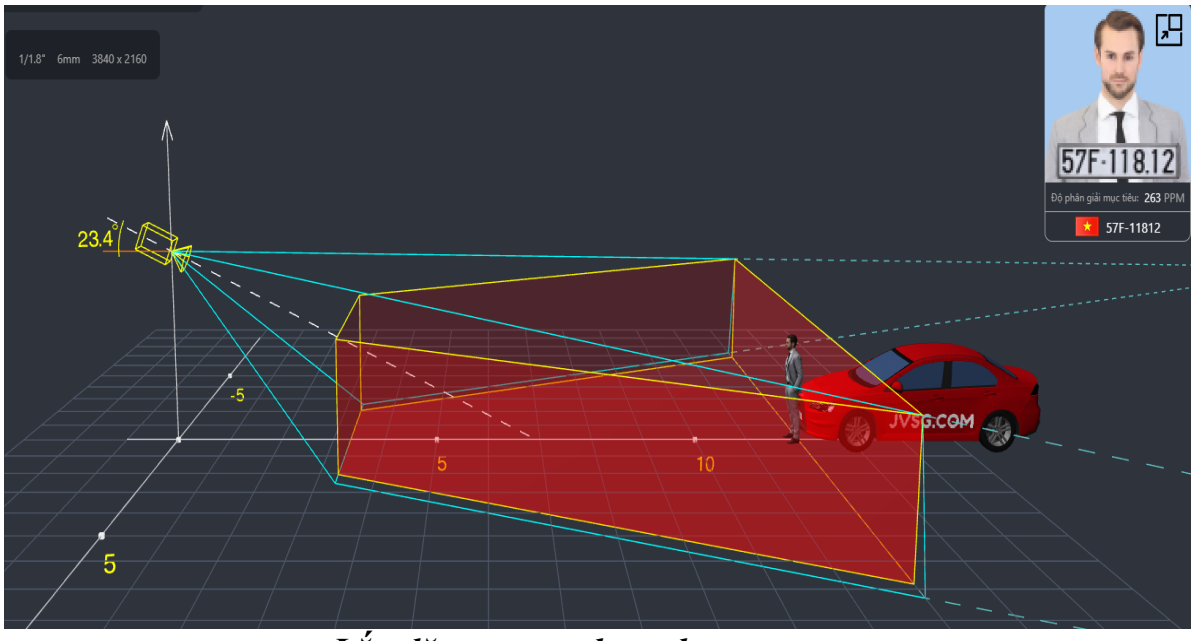
11. Phương án lắp đặt camera, tủ kỹ thuật

Các Camera sẽ được lắp trên các cột của cổng ra vào để đảm bảo nhận diện khuôn mặt, các tủ kỹ thuật ngoài trười cũng sẽ được lắp lên các trụ đó. Yêu cầu các thiết bị Camera, tủ kỹ thuật phải trang thị thiết kế chống sét, đảm bảo an toàn khi vận hành. Chiều cao Camera từ 3,5m trở xuống, ở những cổng lớn cần giám sát Tài xế lái xe Container thì lắp vị trị cao tầm 3m-4m





Thiết kế phương án lắp đặt Camera



Lắp đặt camera theo phương ngang

Các vị trí lắp đặt Camera cụ thể như sau:

a) Về các vị trí Camera AI tại khu công nghiệp Bình Hòa (huyện Châu Thành), tổng cộng 3 cổng gồm: Cổng 1 hướng ra Quốc lộ 91 về TP Châu Đốc, Cổng 2 phía tỉnh lộ 941 hướng về huyện Tri Tôn, Cổng 3 đối diện Dự án Cầu tàu. Ngoài ra, còn có cổng phụ thông qua Nhà ở xã hội KCN Bình Hoà)

STT	VỊ TRÍ	Cổng 2 làn vào ra riêng biệt	Số lượng Camera hướng vào	Số lượng Camera hướng ra	Tổng cộng
1	**Vị trí 1: Cổng chính đường số 3** (ngay ngã tư Quốc lộ 91 rẽ vào Khu Công nghiệp): Cổng nằm trên trục đường chính. Có xe container, xe tải lớn ra vào thường xuyên, xe oto con, xe máy công nhân ra vào số lượng lớn. Cổng có 2 làn xe, mỗi làn 10m	x	2	2	4

STT	VỊ TRÍ	Cổng 2 làn vào ra riêng biệt	Số lượng Camera hướng vào	Số lượng Camera hướng ra	Tổng cộng
	(tổng cộng 2 bên 20m). Có nhà điều hành bảo vệ ở giữa. Dự kiến lắp 2 CAM AI nhận diện ở 2 bên cổng, tổng là 4 CAM cho 2 chiều ra và vào 				
2	**Vị trí 2: Cổng phụ đường số 2** (hướng tỉnh lộ 941 đi về xã Cần Đăng). Có xe tải ra vào thường xuyên, xe oto con, xe máy công nhân ra vào số lượng lớn. Cổng rộng khoảng 9m mỗi bên, 2 bên khoảng 18m. Dự kiến lắp 2 CAM 2 chiều vào ra để nhận diện. 	x	2	2	4
3	**Vị trí 3: Cổng phụ đường số 1** (gần các khu nhà trọ ra hướng Quốc lộ 91): Gần các khu nhà trọ của Công nhân, Cổng này đa số Công nhân vào thường xuyên bằng xe máy. Xe oto con và xe tải không đi cổng này.		1	1	2

STT	VỊ TRÍ	Cổng 2 làn vào ra riêng biệt	Số lượng Camera hướng vào	Số lượng Camera hướng ra	Tổng cộng
	Chiều dài cổng khoảng 7m. Hướng cổng ra quốc lộ 91. Dự kiến lắp 2 CAM ở 2 chiều vào ra. 				
4	**Vị trí 4: Cổng phụ thông qua khu Nhà ở Xã hội KCN Bình Hoà:** Cổng tiếp thông qua khu nhà Xã hội phục vụ cho người lao động, chuyên gia của KCN, các dịch vụ liên quan nên là "Cổng thường mở" cần có giám sát. Dự kiến lắp 2 CAM ở 2 chiều vào ra. 		1	1	2
	Tổng cộng		**6**	**6**	**12**

b) Về các vị trí Camera AI tại KCN Bình Long: Quy mô diện tích khu lớn, có 1 cổng ra Quốc lộ 91. Chi tiết các vị trí cụ thể:

STT	VỊ TRÍ	Cổng 2 làn vào ra riêng biệt	Số lượng Camera hướng vào	Số lượng Camera hướng ra	Tổng cộng
1	**Cổng chính đường số 2** (ngay ngã ba Quốc lộ 91 rẽ vào Khu Công nghiệp) Cổng nằm trên trục đường chính. Có xe container, xe tải lớn ra vào thường xuyên, xe oto con, xe máy công nhân ra vào số lượng lớn. Chiều dài cổng 2 bên là 12m, mỗi bên 6m. Vị trí không có cột thuận tiện để lắp đặt CAM trên cột. Dự kiến sẽ lắp đặt cột mới cao từ 3m-5m để lắp đặt CAM AI ở 2 chiều vào ra. 	x	2	2	4
2	**Cổng số 1**: Cổng nằm trên trục đường chính hướng ra Quốc lộ 91. Cổng này nằm ở hướng Cty Bình Long. Chiều dài cổng khoảng 4m, đề xuất lắp 2 Camera AI 2 chiều vào ra 		1	1	2
	Tổng cộng		**3**	**3**	**6**

3.3.4. Trung tâm điều hành

- Máy chủ quản lý, ghi hình (đặt tại Trung tâm CNTT-TT An Giang): ghi hình và quản lý tập trung tất cả các camera trong hệ thống. Phân phối luồng hình ảnh tới các máy khai thác, cho phép xem trực tiếp, xem lại.

- Máy tính khai thác: máy tính để bàn cấu hình cao kèm màn hình để thực hiện các tác vụ tra cứu, trích xuất hình ảnh của cán bộ vận hành.

- Màn hình Tivi: nhận các tín hiệu hình ảnh từ máy tính khai thác và tạo kịch bản hiển thị các cảnh báo từ hệ thống máy chủ nhận diện người lạ mặt xâm nhập hoặc cảnh báo Blacklist danh sách đối tượng nguy hiểm đang có âm mưu xâm nhập khu công nghiệp.

3.3.5. Giải pháp giám sát

Camera luồng hình ảnh tới máy chủ quản lý ghi hình thông qua chuẩn RTSP.Máy chủ quản lý ghi hình thu thập tập các luồng tín hiệu video và lưu vào bộ nhớ lưu trữ video chuyên dụng. Video được lưu dưới dạng file với cấu trúc MP4 chuẩn nén H264 có thể trích xuất và xem trên các ứng dụng video thông dụng.

Camera AI tự động phân tích hình ảnh liên tục để phát hiện đối tượng và các đặc trưng của đối tượng như màu sắc, khuôn mặt và gửi tới máy chủ để quản lý lưu trữ phục vụ tra cứu.

Trên các máy tính hiển thị cài đặt phần mềm hiển thị hình ảnh có khả năng kết nối với Máy chủ ghi hình để nhận luồng video và giải mã ra hình ảnh. Phần mềm cùng lúc có thể xử được nhiều luồng video và sắp xếp hiển thị trên nhiều loại lưới video (video grid) kích thước khác nhau như 2x2, 3x3, 4x4

Bộ điều khiển kết hợp nhiều lưới video để đưa lên màn hình lớn để đồng thời quan sát được tất cả camera trong hệ thống.

Trên các máy vận hành cài đặt phần mềm quản lý hình ảnh kết nối với Máy chủ ghi hình cho phép người dùng xem trực tiếp, xem lại, điều khiển PTZ và tra cứu sự kiện, tra cứu đối tượng theo nhiều tiêu chí như thời gian, địa điểm, loại đối tượng.

3.4. Yêu cầu hệ thống lưu trữ và máy chủ phân tích dữ liệu cao

Máy chủ đáp ứng được khả năng tính toán, phân tích và xử lý dữ liệu với hiệu suất cao, linh hoạt trong việc mở rộng và nâng cấp cấu hình dễ dàng phù hợp cho mọi thay đổi theo nhu cầu sử dụng của đơn vị ở thời điểm hiện tại và trong tương lai. Cấu hình đề xuất như sau:

Khu công nghiệp Bình Hòa và Khu công nghiệp Bình Long

- Máy chủ công nghiệp 12x3.5"(F)+4x2.5(R)

- Silver 2x4310/128GB (4x32GB)

- SSD 480GB (2x240GB)
- HDD NLSAS 48TB (6X8TB)
- PERC H755
- RTX A5000 24GB
- iDRAC9 Ent
- DP 1GbE LOM + BC5720QP OCP/ 2x800W/ Bezel/ DVD Ext/ No OS

3.5. Tủ kỹ thuật goài trời (thiết kế chống nóng)

- Kích thước tủ (DxCxR): 400x400x300mm; dày 1,2mm
- Sơn tĩnh điện 1 lớp, màu phù hợp với cột kẽm
- Chịu nhiệt độ cao, chống nước, có khóa.

3.6. Thông số kỹ thuật của các thiết bị khác

3.6.1. Thiết bị cắt lọc sét lan truyền đường nguồn 1 pha

- Điện áp làm việc (Un): 220-240Vac
- Tần số làm việc (Hz): 50/60Hz
- Điện áp làm việc tối đa (Uc): 275V
- Cấp điện áp (Up): < 1.5kV
- Công nghệ chế tạo: MOV
- Cấu hình bảo vệ: N-E, L-N
- Bao gồm: 3 cọc tiếp địa + ốc xiết cáp tiếp địa và 6m cáp tiếp địa 1x10mm2

3.6.2. Swich PoE công nghiệp

- Số cổng: ≥ 8 cổng PoE+ & 2 cổng SFP/RJ45 kết hợp
- Nhiệt độ hoạt động: -40°C to +75°C
- Nguồn: 48-57 VDC
- Độ ẩm hỗ trợ: 5% to 95%

3.6.3. Thiết bị chuyển mạch (đặt tại KCN)

- Cổng mạng: 24 x 1G
- Cổng đường lên: 4 x 10G SFP +
- Tổng ports: 24 x Gigabit Ethernet + 4 x 10 Gigabit
- Cấp nguồn qua Ethernet (PoE): Chỉ thông tin
- Nguồn cấp Nội bộ

- Đặc trưng: Chuyển mạch lớp 2, hỗ trợ VLAN, Giao thức Spanning Tree (STP), bảo vệ mối đe dọa nâng cao, bảo mật bước đầu tiên IPv6, chất lượng dịch vụ (QoS), sFlow, định tuyến động

- Bộ đệm gói: 1,5 MB

- Quản lý mạng: Bảng điều khiển kinh doanh của Cisco và ứng dụng di động; giao diện người dùng, CLI và SNMP trên thiết bị

3.6.4. Attomat

Aptomat MCB 2P 25A 6KA

Số cực: 2P

Dòng điện định mức: 25A

Dòng cắt ngắn mạch: 6kA

Điện áp định mức: 230V

3.6.5. Dây cáp mạng ngoài trời

- Cáp mạng treo ngoài trời Cat.5e.

- Dây cáp mạng chuẩn quốc tế Cat.5e.

- Thiết kế với 4 cặp dây, chất liệu: đồng nguyên chất, kích thước: 24AWG (0.51mm).

- Dây cáp thép gia cường cho phép treo và móc, cho việc triển khai ngoài trời dễ dàng.

- Chạy được tốc độ thật 1G với khoảng cách 100m.

- Đáp ứng nhu cầu cho những ứng dụng Gigabit Ethernet, 10/100BASE-TX...

- Quy cách: 305m/thùng, vỏ bảo vệ PVC.

3.6.6. ODF 4 FO (bao gồm pitail)

Hộp ODF bằng nhựa 04FO SC-UPC

Đầy đủ phụ kiện: 04 Adapter SC-UPC+ 4 Dây hàn quang + 4 ỐNG co nhiệt - M2ODF-SCU4P

3.6.7. Đế, Bulong và kẹp cáp

Đế ốp D12: 4 mm ± 0.1mm, Mạ kẽm nhúng nóng tiêu chuẩn ASTM-A123, đồng đều bề mặt, nhẵn bóng không rạn nứt, không có cạnh mép sắc,

3.6.8. Convert AC 1 sợi quang (Bộ 2 đầu)

- Adapter 5V-2A.

- Bộ chuyển đổi quang điện 10/100M Single Fiber (1 Sợi quang).

- Chuẩn IEEE802.3 10Base-T, and IEEE802.3u 100Base-TX/FX standards.

- Truyền dẫn đồng thời 2 tín hiệu cáp quang.

- Hỗ trợ tính năng tự động nhận diện tốc độ.

- Khoảng cách truyền 25Km.

3.6.9. Mặt bích lắp camera

- Bích bắt cột cho Camera

- Kích thước mặt bích 210x150mm

- Sử dụng với cột vuông, tròn, lục giác…

- Sử dụng với các loại Camera hoặc hộp Camera

- Chất liệu: thép sơn tĩnh điện chống gỉ

- Bộ sản phẩm gồm có 1 bích và 3 đai bắt cột đường kính 20cm phù hợp bắt các loại cột cỡ lớn, đai inox A200 và khóa đai A20/bulong 14x150

3.6.10. Giá treo camera

Giá treo camera ngoài trời, chất liệu thép, mạ kẽm có khả năng chống ăn mòn, chống chịu thời tiết tốt.

Kích thước: 1 mét (1000mm). Chịu lực 15kg

Môi trường làm việc: -10°C đến +45°C (< 95%RH)

3.6.11. Các thiết bị khác như: Màn hình Tivi, máy tính điều hành, bàn ghế tủ, máy điều hòa nhiệt độ,... được tận dụng các thiết bị của Khu công nghiệp.

Các hạ tầng thiết bị hiện có, được tận dụng tại Ban quản lý khu kinh tế, Ban Quản lý Khu công nghiệp như sau:

STT	Đơn vị quản lý	VỊ TRÍ	Hiện trạng đang có	ĐVT	Số lượng	Năm đưa vào sử dụng	Trạng thái	Ghi chú
1	Khu công nghiệp Bình Hòa	Vị trí 1: Cổng chính đường số 3	Phòng bảo vệ	Phòng	1		Tốt	
2			Bàn làm việc Loại gỗ ép, KT: 70cm x 140cm	Cái	1	2012	Tốt	Chưa có máy tính để kết nối hiển

STT	Đơn vị quản lý	VỊ TRÍ	Hiện trạng đang có	ĐVT	Số lượng	Năm đưa vào sử dụng	Trạng thái	Ghi chú
3			Ghế xếp Hòa Phát. Loại xếp, inox G04-I	Cái	1	2016	Tốt	thị lên màn hình TV
4			TV Samsung 32inch - Analog	Cái	1	2017	Tốt	
5			Máy tính bàn; Core i3, RAM 8GB, SSD tối thiểu 128GB	Cái	1	2019	Tốt	Đề xuất bổ sung cấp về KCN Bình Hòa
6		Vị trí 2: Cổng phụ đường số 2	Phòng bảo vệ	Phòng	1		Tốt	Đề xuất xem trên smartphone của bảo vệ
7		Vị trí 3: Cổng phụ đường số 1	Phòng bảo vệ	Phòng	1		Tốt	
8		Vị trí 4: Cổng phụ thông qua khu Nhà ở Xã hội KCN Bình Hoà:	Phòng bảo vệ	Phòng	1		Tốt	
9	Khu công nghiệp Bình Long	Vị trí 1:Cổng chính đường số 2	Phòng bảo vệ	Phòng	1		Tốt	
10			Bàn làm việc Loại gỗ ép, KT: 70cm x 140cm	Cái	1	2010	Tốt	Chưa có máy tính để kết nối hiển

STT	Đơn vị quản lý	VỊ TRÍ	Hiện trạng đang có	ĐVT	Số lượng	Năm đưa vào sử dụng	Trạng thái	Ghi chú
11			Ghế xếp Hòa Phát. Loại xếp, inox G04-I	Cái	1	2012	Tốt	thị lên màn hình TV
12			TV Panasonic 49inch - SmartTV	Cái	1	2019	Tốt	
13			Máy tính bàn; Core i3, RAM 8GB, SSD tối thiểu 128GB	Cái	1	2019	Tốt	Đề xuất bổ sung cấp về KCN Bình Long
14		Vị trí 2: Cổng Cty Bình Long						Đề xuất xem trên smartphone của bảo vệ
15	Ban Quản lý KKT tỉnh							Không có màn hình giám sát, chỉ quản lý tổng thể và được cấp tài khoản giám sát từ xa

3.7. Yêu cầu hạ tầng kết nối mạng (đường truyền):

Sử dụng đường truyền L2VPN chuyên dụng của nhà cung cấp dịch vụ để phục vụ kết nối mạng. đảm bảo được vấn đề triển khai giải pháp kết nối, đảm bảo đáp ứng về mặt lưu lượng dữ liệu sử dụng.

Nội dung công việc triển khai hạ tầng kết nối để phục vụ Hệ thống camera an ninh giám sát tuyến biên giới và phòng chống tội phạm như sau:

- Sử dụng đường truyền L2VPN tại Trung tâm điều hành để hỗ trợ lực lượng chuyên trách cơ động xử lý ngoài cơ quan. Đồng thời cung cấp kết nối cho các lực lượng chức năng tại các đồn/điểm/chốt giám sát, xử lý. Có thể kết nối vào mạng truyền số liệu chuyên dụng cấp độ 2 của Đảng và Nhà nước

- Sử dụng đường truyền dùng riêng để thu gom tín hiệu từ các Camera về hệ thống quản lý và lưu trữ tập trung; đồng thời để kết nối trung tâm giám sát và các máy tính phục vụ giám sát, hiển thị hình ảnh về hệ thống quản lý tập trung.

- Đảm bảo kết nối ổn định, an toàn và bảo mật tuyệt đối.

Thuê đường truyền như sau:

STT	Tên Hạng mục	Đơn vị	Số lượng
1	Đường truyền chuyên dụng dùng riêng L2VPN tốc độ 150Mbps (Khu CN Bình Hòa)	Line	01
2	Đường truyền chuyên dụng dùng riêng L2VPN tốc độ 80Mbps (Khu CN Bình Long)	Line	01

3.8. Hệ thống VMS quản lý (Video Management System):

Yêu cầu chức năng hệ thống VMS quản lý

STT	Chỉ tiêu	Nội dung chi tiết	Giá trị
A	**Quản lý tài khoản người dùng**		
1	Thêm/sửa thông tin người dùng đăng ký	- Cho phép user đăng ký tài khoản bằng số điện thoại, hỗ trợ lưu trữ thông tin cơ bản của người dùng - Cho phép người dùng chỉnh sửa thông tin đăng ký	Có
2	Đăng nhập	Chức năng quản lý xác thực username/password khi người dùng thực hiện đăng nhập hệ thống	Có
3	Đăng xuất	Chức năng cho phép người dùng thực hiện đăng xuất hệ thống	Có

STT	Chỉ tiêu	Nội dung chi tiết	Giá trị
4	Thay đổi mật khẩu	Chức năng cho phép người dùng thực hiện thay đổi mật khẩu	Có
5	Quên mật khẩu	Chức năng cho phép người dùng thực hiện quên mật khẩu	Có
6	Hiển thị thông tin người dùng cơ bản	Các thông tin người dùng có thể cập nhật, thay đổi: - Tên account - Password - Email/Số điện thoại đăng ký	Có
B	**Xem trực tiếp**		
1	Hiển thị danh mục site	Hiển thị danh sách các địa điểm lắp đặt được gán quyền xem đối với user hiện hành	Có
2	Hiển thị hình ảnh camera	Hiển thị hình ảnh của các camera thuộc site đang lựa chọn, gồm các thông tin cơ bản sau + Tên camera + Trạng thái xem trực tiếp/xem lại + Hình ảnh từ camera + Thời gian camera	Có
3	Số lượng camera hiển thị	Số lượng camera hiển thị tối đa trên 1 trang	1-16 camera
4	Thiết lập layout hiển thị	- Cho phép thiết lập layout hiển thị danh sách các camera theo số hàng/cột từ 1-5 - Trường hợp có nhiều camera thì phải phân trang, số camera trên mỗi trang = số cột * số hàng	Có
5	Hỗ trợ lưu cấu hình layouts hiển thị	Hỗ trợ lưu cấu hình layouts hiển thị	Có
6	Hỗ trợ chia sẻ layouts hiển thị giữa các tài khoản	Hỗ trợ chia sẻ layouts hiển thị giữa các tài khoản	Có
7	Lựa chọn chế độ xem toàn màn hình	- Cho phép chọn chế độ xem toàn màn hình đối với layout hiển thị đã lựa chọn	Có

STT	Chỉ tiêu	Nội dung chi tiết	Giá trị
		- Cho phép chọn chế độ xem toàn màn hình đối với 1 camera	
8	Lựa chọn camera hiển thị	Lựa chọn camera hiển thị	Có
C	**Xem lại**		
1	Số lượng camera hiển thị	Số lượng camera hiển thị tối đa trên 1 trang	1-16 camera
2	Điều chỉnh tốc độ hiển thị	Điều chỉnh tốc độ hiển thị	0.5x, 1x, 2x, 4x, 8x
3	Timeline hiển thị và điều khiển dữ liệu	Timeline hiển thị và điều khiển dữ liệu	Có
4	Hỗ trợ hiên thị thumbnail khi lựa chọn vị trí trên timeline	Hỗ trợ hiên thị thumbnail khi lựa chọn vị trí trên timeline	Có
5	Hỗ trợ lựa chọn vị trí phát trên timeline	Hỗ trợ lựa chọn vị trí phát trên timeline	Có
6	Lựa chọn chế độ xem toàn màn hình	- Cho phép chọn chế độ xem toàn màn hình đối với layout hiển thị đã lựa chọn - Cho phép chọn chế độ xem toàn màn hình đối với 1 camera	Có
D	**Quản lý sự kiện thông minh**		
		Kiểm soát ra vào	
		Hiển thị thông tin nhận diện người vào ra	Tên, Hình ảnh, Độ chính xác
		Hỗ trợ hiển thị đồng thời nhiều vị trí giám sát vào ra	Có
		Báo cáo chấm công theo cá nhân, phòng ban	Có

STT	Chỉ tiêu	Nội dung chi tiết	Giá trị
		Quản lý lịch sử vào ra	
		Thông tin lịch sử	Nhân viên, Khách, Người lạ
		Thời gian lưu trữ lịch sử	≥ 90 ngày
		Hỗ trợ tìm kiếm	Tên, Thời gian, Vị trí
		Thông tin lưu trữ lịch sử	Thời gian, ảnh, video
E	**Hỗ trợ tích hợp**		
		Hỗ trợ tích hợp vào hệ thống khác qua API	Hỗ trợ
		Giao thức kết nối	RTSP, WebRTC, HTTPS

3.9. Yêu cầu về nguồn điện

- Đảm bảo nguồn điện cung cấp cho thiết bị kỹ thuật hoạt động ổn định không bị gián đoạn.

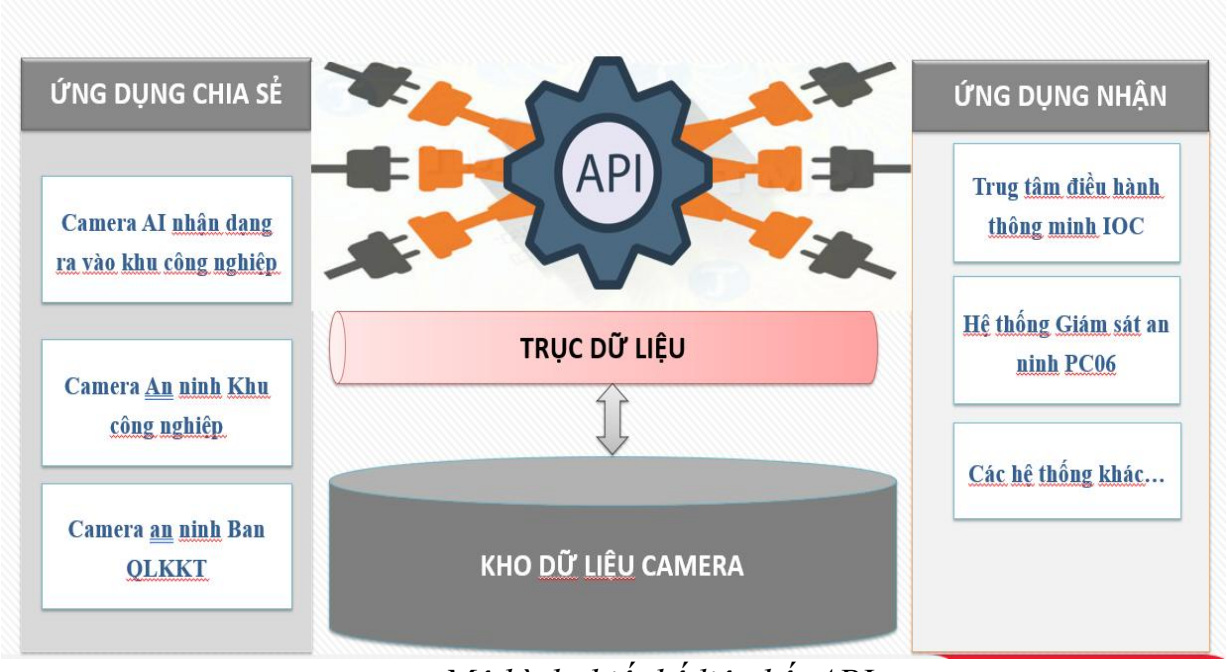
- Đảm bảo nguồn điện lưới (220VAC) để cung cấp ổn định cho hệ thống. Lựa chọn phương án cấp điện lưới 220V ưu tiên cao nhất (từ các trạm điện hạ thế của ngành điện lực).

- Ngoài cấp điện nguồn 220VAC còn có sử dụng nguồn điện áp thấp 12VDC/24VAC hoặc cấp nguồn qua giao diện mạng PoE cho các Camera.

- Nguồn điện và chi phí điện tại các khu công nghiệp do Ban quản lý khu kinh tế tỉnh không tính vào chi phí thuê.

3.10. Yêu cầu, điều kiện về khả năng kết nối, liên thông với ứng dụng, hệ thống thông tin khác

Đảm bảo thực hiện kết nối, liên thông ứng dụng với các hệ thống thông tin khác sử dụng API (viết tắt của Application Programming Interface – phương thức trung gian kết nối các ứng dụng và thư viện khác nhau). Sử dụng API trên hệ thống VMS giúp kết nối và chia sẽ thông tin qua các hệ thống khác.



Mô hình thiết kế liên kết API

Đảm bảo kết nối, liên thông thông qua Nền tảng tích hợp, chia sẻ dữ liệu tỉnh An Giang, tuân thủ Khung kiến trúc Chính phủ điện tử, Kiến trúc Chính quyền điện tử tỉnh An Giang, hiện hành và quy định tại Nghị định số 47/2020/NĐ-CP ngày 09/4/2020 về quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước, đảm bảo kết nối với Trung tâm giám sát điều hành thông minh (IOC) tỉnh.

Để kết nối với các hệ thống khác, yêu cầu phải cung cấp các giao thức kết nối (RTSP, WebRTC, HTTPS) để hỗ trợ tích hợp hiển thị liveview video trên các hệ thống khác.

Giao thức kết nối RTSP, WebRTC, HTTPS là ba giao thức kết nối phổ biến được sử dụng trong các ứng dụng phát trực tuyến, hội nghị truyền hình và bảo mật. Các giao thức kết nối cung cấp một cách tiêu chuẩn để các thiết bị và ứng dụng trao đổi dữ liệu và thông tin.

- ✓ RTSP (Real Time Streaming Protocol) là một giao thức kết nối được sử dụng để truyền phát video và âm thanh trực tiếp. RTSP cung cấp một cách tiêu chuẩn để các thiết bị và ứng dụng kiểm soát luồng truyền phát, chẳng hạn như bắt đầu, dừng và điều chỉnh tốc độ phát lại.

- ✓ WebRTC (Web Real-Time Communication) là một giao thức kết nối được sử dụng để truyền dữ liệu thời gian thực giữa các thiết bị. WebRTC cung cấp một cách tiêu chuẩn để các thiết bị và ứng dụng giao tiếp với nhau mà không cần phải sử dụng một máy chủ trung gian.
- ✓ HTTPS (Hypertext Transfer Protocol Secure) là một giao thức kết nối được sử dụng để truyền dữ liệu qua internet một cách an toàn. HTTPS sử dụng mã hóa để bảo vệ dữ liệu khỏi bị truy cập trái phép.

Về phương thức kết nối với CSDL dân cư quốc gia, thực hiện xác thực thẻ CCCD bằng đầu đọc CCCD thông qua ID Check như đã trình bày tại Mục: Giải pháp định danh và xác thực điện tử sử dụng CCCD gắn chip, tuân thủ yêu cầu tại văn bản số 3147/QLHC-TTDLDC ngày 17/4/2024 của Cục Cảnh sát Quản lý hành chính về trật tự xã về việc trao đổi triển khai Hệ thống Camera AI kiểm soát KCN.

Nhà thầu thực hiện phải chịu trách nhiệm về chi phí kết nối (thiết bị, dịch vụ liên quan) và phương thức kết nối với CSDL dân cư quốc gia.

3.11. Danh mục quy chuẩn, tiêu chuẩn kỹ thuật áp dụng:

- Quyết định số 724/QĐ-BTTTT ngày 07/5/2024 của Bộ Thông tin và Truyền thông về việc ban hành Bộ tiêu chí về yêu cầu an toàn thông tin mạng cơ bản cho camera giám sát.

- Công văn số 3147/QLHC-TTDLDC ngày 17/4/2024 của Cục Cảnh sát Quản lý hành chính về trật tự xã về việc trao đổi triển khai Hệ thống Camera AI kiểm soát KCN.

- TCVN 6768-1:2000 về thiết bị hệ thống nghe nhìn, video và truyền hình - Quy định chung.

- TCVN 8071:2009 về công trình viễn thông - Quy tắc thực hành chống sét và tiếp đất.

- TCCS 01:2009-BCA về tiêu chuẩn kỹ thuật hệ thống giám sát, xử lý vi phạm trật tự, an toàn giao thông đường bộ.

- TCVN 9385:2012 về chống sét cho các công trình xây dựng - hướng dẫn thiết kế, kiểm tra và bảo trì hệ thống.

- QCVN 33:2019/BTTTT về quy chuẩn kỹ thuật quốc gia về lắp đặt mạng cáp ngoại vi viễn thông.

- QCVN 71:2013/BTTTT về quy chuẩn kỹ thuật quốc gia về tương thích điện tử (EMC) của mạng cáp phân phối tín hiệu truyền hình.

- Camera sử dụng công nghệ PoE (Power over Ethernet), chuẩn nén hình ảnh H.264/MJPEG, đạt tiêu chuẩn IP66.

- Các tiêu chuẩn về an ninh ISO/IEC 27001:2013.

- Tiêu chuẩn, quy chuẩn kỹ thuật đối với Trung tâm dữ liệu theo thông tư số 03/2013/TT-BTTTT ngày 22/11/2013 của Bộ Thông tin và Truyền thông.

- Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ, tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

- Thông tư số 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ trưởng Bộ Thông tin và Truyền thông về ban hành danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước.

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1	**Tiêu chuẩn về kết nối**			
1.1	Truyền siêu văn bản	HTTP v1.1	Hypertext Transfer Protocol version 1.1	Bắt buộc áp dụng
		HTTP v2.0	Hypertext Transfer Protocol version 2.0	Khuyến nghị áp dụng
1.2	Truyền tệp tin	FTP	File Transfer Protocol	Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn
		HTTP v1.1	Hypertext Transfer Protocol version 1.1	
		HTTP v2.0	Hypertext Transfer Protocol version 2.0	Khuyến nghị áp dụng
		WebDAV	Web-based Distributed Authoring and Versioning	Khuyến nghị áp dụng
1.3	Truyền, phát luồng âm thanh/ hình ảnh	RTSP	Real-time Streaming Protocol	Khuyến nghị áp dụng
		RTP	Real-time Transport Protocol	Khuyến nghị áp dụng
		RTCP	Real-time Control Protocol	Khuyến nghị áp dụng

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1.4	Truy cập và chia sẻ dữ liệu	OData v4	Open Data Protocol version 4.0	Khuyến nghị áp dụng
1.5	Truyền thư điện tử	SMTP/ MIME	Simple Mail Transfer Protocol/Multipurpose Internet Mail Extensions	Bắt buộc áp dụng
1.6	Cung cấp dịch vụ truy cập hộp thư điện tử	POP3	Post Office Protocol version 3	Bắt buộc áp dụng cả hai tiêu chuẩn đối với máy chủ
		IMAP 4rev1	Internet Message Access Protocol version 4 revision 1	
1.7	Truy cập thư mục	LDAP v3	Lightweight Directory Access Protocol version 3	Bắt buộc áp dụng
1.8	Dịch vụ tên miền	DNS	Domain Name System	Bắt buộc áp dụng
1.9	Giao vận mạng có kết nối	TCP	Transmission Control Protocol	Bắt buộc áp dụng
1.10	Giao vận mạng không kết nối	UDP	User Datagram Protocol	Bắt buộc áp dụng
1.11	Liên mạng LAN/WAN	IPv4	Internet Protocol version 4	Bắt buộc áp dụng
		IPv6	Internet Protocol version 6	Bắt buộc áp dụng đối với các thiết bị có kết nối Internet
1.12	Mạng cục bộ không dây	IEEE 802.11g	Institute of Electrical and Electronics Engineers Standard (IEEE) 802.11g	Bắt buộc áp dụng
		IEEE 802.11n	Institute of Electrical and Electronics Engineers Standard (IEEE) 802.11n	Khuyến nghị áp dụng
1.13	Truy cập Internet với thiết bị không dây	WAP v2.0	Wireless Application Protocol version 2.0	Bắt buộc áp dụng

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1.14	Dịch vụ Web dạng SOAP	SOAP v1.2	Simple Object Access Protocol version 1.2	Bắt buộc áp dụng một, hai hoặc cả ba tiêu chuẩn
		WSDL V2.0	Web Services Description Language version 2.0	
		UDDI v3	Universal Description, Discovery and Integration version 3	
1.15	Dịch vụ Web dạng RESTful	RESTful web service	Representational state transfer	Khuyến nghị áp dụng
1.16	Dịch vụ đặc tả Web	WS BPEL v2.0	Web Services Business Process Execution Language Version 2.0	Khuyến nghị áp dụng
		WS-I Simple SOAP Binding Profile Version 1.0	Simple SOAP Binding Profile Version 1.0	Khuyến nghị áp dụng
		WS- Federation v1.2	Web Services Federation Language Version 1.2	Khuyến nghị áp dụng
		WS- Addressing v1.0	Web Services Addressing 1.0	Khuyến nghị áp dụng
		WS-Coordination Version 1.2	Web Services Coordination Version 1.2	Khuyến nghị áp dụng
		WS-Policy v1.2	Web Services Coordination Version 1.2	Khuyến nghị áp dụng
		OASIS Web Services Business Activity Version 1.2	Web Services Business Activity Version 1.2	Khuyến nghị áp dụng

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		WS- Discovery Version 1.1	Web Services Dynamic Discovery Version 1.1	Khuyến nghị áp dụng
		WS-MetadataExchange	Web Services Metadata Exchange	Khuyến nghị áp dụng
1.17	Dịch vụ đồng bộ thời gian	NTPv3	Network Time Protocol version 3	Bắt buộc áp dụng một trong hai tiêu chuẩn
		NTPv4	Network Time Protocol version 4	
2	**Tiêu chuẩn về tích hợp dữ liệu**			
2.1	Ngôn ngữ định dạng văn bản	XML v1.0 (5th Edition)	Extensible Markup Language version 1.0 (5th Edition)	Bắt buộc áp dụng một trong hai tiêu chuẩn
		XML v1.1 (2ndEdition)	Extensible Markup Language version 1.1	
2.2	Ngôn ngữ định dạng văn bản cho giao dịch điện tử	ISO/TS 15000:2014	Electronic Business Extensible Markup Language (ebXML)	Bắt buộc áp dụng
2.3	Định nghĩa các lược đồ trong tài liệu XML	XML Schema V1.1	XML Schema version 1.1	Bắt buộc áp dụng
2.4	Biến đổi dữ liệu	XSL	Extensible Stylesheet Language	Bắt buộc áp dụng phiên bản mới nhất.
2.5	Mô hình hóa đối tượng	UML v2.5	Unified Modelling Language version 2.5	Khuyến nghị áp dụng
2.6	Mô tả tài nguyên dữ liệu	RDF	Resource Description Framework	Khuyến nghị áp dụng
		OWL	Web Ontology Language	Khuyến nghị áp dụng

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
2.7	Trình diễn bộ kí tự	UTF-8	8-bit Universal Character Set (UES)/Unicode Transformation Format	Bắt buộc áp dụng
2.8	Khuôn thức trao đổi thông tin địa lý	GML v3.3	Geography Markup Language version 3.3	Bắt buộc áp dụng
2.9	Truy cập và cập nhật các thông tin địa lý	WMS v1.3.0	OpenGIS Web Map Service version 1.3.0	Bắt buộc áp dụng
		WFS v1.1.0	Web Feature Service version 1.1.0	Bắt buộc áp dụng
2.10	Trao đổi dữ liệu đặc tả tài liệu XML	XMI v2.4.2	XML Metadata Interchange version 2.4.2	Khuyến nghị áp dụng
2.11	Sổ đăng ký siêu dữ liệu (MDR)	ISO/IEC 11179:2015	Sổ đăng ký siêu dữ liệu (Metadata registries - MDR)	Khuyến nghị áp dụng
2.12	Bộ phần tử siêu dữ liệu Dublin Core	ISO 15836-1:2017	Bộ phần tử siêu dữ liệu Dublin Core	Khuyến nghị áp dụng(*)
2.13	Định dạng trao đổi dữ liệu mô tả đối tượng dạng kịch bản JavaScript	JSON RFC 7159	JavaScript Object Notation	Khuyến nghị áp dụng
2.14	Ngôn ngữ mô hình quy trình nghiệp vụ	BPMN 2.0	Business Process Model and Notation version 2.0	Khuyến nghị áp dụng
3	**Tiêu chuẩn về truy cập thông tin**			
3.1	Chuẩn nội dung Web	HTML v4.01	Hypertext Markup Language version 4.01	Bắt buộc, áp dụng
		WCAG 2.0	W3C Web Content Accessibility Guidelines (WCAG) 2.0	Khuyến nghị áp dụng
		HTML 5	Hypertext Markup Language version 5	Khuyến nghị áp dụng

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
3.2	Chuẩn nội dung Web mở rộng	XHTML v1.1	Extensible Hypertext Markup Language version 1.1	Bắt buộc áp dụng
3.3	Giao diện người dùng	CSS2	Cascading Style Sheets Language Level 2	Bắt buộc áp dụng một trong ba tiêu chuẩn
		CSS3	Cascading Style Sheets Language Level 3	
		XSL	Extensible Stylesheet Language version	
3.4	Văn bản	(.txt)	Định dạng Plain Text (.txt): Dành cho các tài liệu cơ bản không có cấu trúc	Bắt buộc áp dụng
		(.rtf) v1.8, v1.9.1	Định dạng Rich Text (.rtf) phiên bản 1.8, 1.9.1: Dành cho các tài liệu có thể trao đổi giữa các nền khác nhau	Bắt buộc áp dụng
		(.docx)	Định dạng văn bản Word mở rộng của Microsoft (.docx)	Khuyến nghị áp dụng
		(.pdf) v1.4, v1.5, v1.6, v1.7	Định dạng Portable Document (.pdf) phiên bản 1.4, 1.5, 1.6, 1.7: Dành cho các tài liệu chỉ đọc	Bắt buộc áp dụng một, hai hoặc cả ba tiêu chuẩn
		(.doc)	Định dạng văn bản Word của Microsoft (.doc)	
		(.odt) v1.2	Định dạng Open Document Text (.odt) phiên bản 1.2	
3.5	Bảng tính	(.csv)	Định dạng Comma eparated Variable/Delimited (.csv): Dành cho các bảng tính cần	Bắt buộc áp dụng

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
			trao đổi giữa các ứng dụng khác nhau.	
		(.xlsx)	Định dạng bảng tính Excel mở rộng của Microsoft (.xlsx)	Khuyến nghị áp dụng
		(.xls)	Định dạng bảng tính Excel của Microsoft (.xls)	Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn
		(.ods) v1.2	Định dạng Open Document Spreadsheets (.ods) phiên bản 1.2	
3.6	Trình diễn	(.htm)	Định dạng Hypertext Document (.htm): cho các trình bày được trao đổi thông qua các loại trình duyệt khác nhau	Bắt buộc áp dụng
		(.pptx)	Định dạng PowerPoint mở rộng của Microsoft (.pptx)	Khuyến nghị áp dụng
		(.pdf)	Định dạng Portable Document (.pdf): cho các trình bày lưu dưới dạng chỉ đọc	Bắt buộc áp dụng một, hai hoặc cả ba tiêu chuẩn
		(.ppt)	Định dạng PowerPoint (.ppt) của Microsoft	
		(.odp) v1.2	Định dạng Open Document Presentation (.odp) phiên bản 1.2	
3.7	Ảnh đồ họa	JPEG	Joint Photographic Expert Group (.jpg)	Bắt buộc áp dụng một, hai, ba hoặc cả bốn tiêu chuẩn
		GIF v89a	Graphic Interchange (.gif) version 89a	

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		TIFF	Tag Image File (.tif)	
		PNG	Portable Network Graphics (.png)	
3.8	Ảnh gắn với tọa độ địa lý	GEO TIFF	Tagged Image File Format for GIS applications	Bắt buộc áp dụng
3.9	Phim ảnh, âm thanh	MPEG-1	Moving Picture Experts Group-1	Khuyến nghị áp dụng
		MPEG-2	Moving Picture Experts Group-2	Khuyến nghị áp dụng
		MPEG-4	Moving Picture Experts Group-4	Khuyến nghị áp dụng
		MP3	MPEG-1 Audio Layer 3	Khuyến nghị áp dụng
		AAC	Advanced Audio Coding	Khuyến nghị áp dụng
3.10	Luồng phim ảnh, âm thanh	(.asf), (.wma), (.wmv)	Các định dạng của Microsoft Windows Media Player (.asf), (.wma), (.wmv)	Khuyến nghị áp dụng
		(.ra), (.rm), (.ram), (.rmm)	Các định dạng Real Audio/Real Video (.ra), (.rm), (.ram), (.rmm)	Khuyến nghị áp dụng
		(.avi), (.mov), (.qt)	Các định dạng Apple Quicktime (.avi), (.mov), (.qt)	Khuyến nghị áp dụng
3.11	Hoạt họa	GIF v89a	Graphic Interchange (.gif) version 89a	Khuyến nghị áp dụng
		(.swf)	Định dạng Macromedia Flash (.swf)	Khuyến nghị áp dụng

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		(.swf)	Định dạng Macromedia Shockwave (.swf)	Khuyến nghị áp dụng
		(.avi), (.qt), (.mov)	Các định dạng Apple Quicktime (.avi),(.qt),(.mov)	Khuyến nghị áp dụng
3.12	Chuẩn nội dung cho thiết bị di động	WML v2.0	Wireless Markup Language version 2.0	Bắt buộc áp dụng
3.13	Bộ ký tự và mã hóa	ASCII	American Standard Code for Information Interchange	Bắt buộc áp dụng
3.14	Bộ ký tự và mã hóa cho tiếng Việt	TCVN 6909:2001	TCVN 6909:2001 "Công nghệ thông tin - Bộ mã ký tự tiếng Việt 16-bit"	Bắt buộc áp dụng
3.15	Nén dữ liệu	Zip	Zip (.zip)	Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn
		.gz v4.3	GNU Zip (.gz) version 4.3	
3.16	Ngôn ngữ kịch bản phía trình khách	ECMA 262	ECMAScript version 6 (6thEdition)	Bắt buộc áp dụng
3.17	Chia sẻ nội dung Web	RSS v1.0	RDF Site Summary version 1.0	Bắt buộc áp dụng một trong hai tiêu chuẩn
		RSS v2.0	Really Simple Syndication version 2.0	
		ATOM v1.0	ATOM version 1.0	Khuyến nghị áp dụng
3.18	Chuẩn kết nối ứng dụng cổng thông tin điện tử	JSR 168	Java Specification Requests 168 (Portlet Specification)	Bắt buộc áp dụng
		JSR286	Java Specification Requests 286 (Portlet Specification)	Khuyến nghị áp dụng
		WSRP v1.0	Web Services for Remote Portlets version 1.0	Bắt buộc áp dụng

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		WSRP v2.0	Web Services for Remote Portlets version 2.0	Khuyến nghị áp dụng
4	**Tiêu chuẩn về an toàn thông tin**			
4.1	An toàn thư điện tử	S/MIME v3.2	Secure Multi-purpose Internet Mail Extensions version 3.2	Bắt buộc áp dụng
		OpenPGP	OpenPGP	Khuyến nghị áp dụng
4.2	An toàn tầng giao vận	SSH v2.0	Secure Shell version 2.0	Bắt buộc áp dụng
		TLS v1.2	Transport Layer Security version 1.2	Bắt buộc áp dụng
4.3	An toàn truyền tệp tin	HTTPS	Hypertext Transfer Protocol Secure	Bắt buộc áp dụng
		FTPS	File Transfer Protocol Secure	Khuyến nghị áp dụng
		SFTP	SSH File Transfer Protocol	Khuyến nghị áp dụng
4.4	An toàn truyền thư điện tử	SMTPS	Simple Mail Transfer Protocol Secure	Bắt buộc áp dụng
4.5	An toàn dịch vụ truy cập hộp thư	POP3S	Post Office Protocol version 3 Secure	Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn
		IMAPS	Internet Message Access Protocol Secure	
4.6	An toàn dịch vụ DNS	DNSSEC	Domain Name System Security Extenssions	Khuyến nghị áp dụng
4.7	An toàn tầng mạng	IPsec - IP ESP	Internet Protocol security với IP ESP	Bắt buộc áp dụng

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
4.8	An toàn thông tin cho mạng không dây	WPA2	Wi-fi Protected Access 2	Bắt buộc áp dụng
4.9	Giải thuật mã hóa	TCVN 7816:2007	Công nghệ thông tin. Kỹ thuật mật mã thuật toán mã dữ liệu AES	Khuyến nghị áp dụng
		3DES	Triple Data Encryption Standard	Khuyến nghị áp dụng
		PKCS #1 V2.2	RSA Cryptography Standard - version 2.2	Khuyến nghị áp dụng, sử dụng lược đồ RSAES-OAEP để mã hóa
		ECC	Elliptic Curve Cryptography	Khuyến nghị áp dụng
4.10	Giải thuật chữ ký số	PKCS #1 V2.2	RSA Cryptography Standard - version 2.2	Bắt buộc áp dụng, sử dụng lược đồ RSASSA-PSS để ký
		ECDSA	Elliptic Curve Digital Signature Algorithm	Khuyến nghị áp dụng
4.11	Giải thuật băm cho chữ ký số	SHA-2	Secure Hash Algorithms-2	Khuyến nghị áp dụng
4.12	Giải thuật truyền khóa	RSA-KEM	Rivest-Shamir-Adleman - KEM (Key Encapsulation Mechanism) Key Transport Algorithm	Bắt buộc áp dụng
		ECDHE	Elliptic Curve Diffie Hellman Ephemeral	Khuyến nghị áp dụng
4.13	Giải pháp xác thực người sử dụng	SAML v2.0	Security Assertion Markup Language version 2.0	Khuyến nghị áp dụng

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
4.14	An toàn trao đổi bản tin XML	XML Encryption Syntax and Processing	XML Encryption Syntax and Processing	Bắt buộc áp dụng
		XML Signature Syntax and Processing	XML Signature Syntax and Processing	Bắt buộc áp dụng
4.15	Quản lý khóa công khai bản tin XML	XKMS v2.0	XML Key Management Specification version 2.0	Khuyến nghị áp dụng
4.16	Giao thức an toàn thông tin cá nhân	P3P v1.1	Platform for Privacy Preferences Project version 1.1	Khuyến nghị áp dụng
4.17	Hạ tầng khóa công khai			Khuyến nghị áp dụng
	Cú pháp thông điệp mật mã cho ký, mã hóa	PKCS#7 v1.5 (RFC 2315)	Cryptographic message syntax for file-based signing and encrypting version 1.5	
	Cú pháp thông tin thẻ mật mã	PKCS#15 v1.1	Cryptographic token information syntax version 1.1	
	Cú pháp thông tin khóa riêng	PKCS#8 V1.2 (RFC 5958)	Private-Key Information Syntax Standard version 1.2	
	Giao diện thẻ mật mã	PKCS#11 v2.20	Cryptographic token interface standard version 2.20	
	Cú pháp trao đổi thông tin cá nhân	PKCS#12 v1.1	Personal Information Exchange Syntax version 1.1	

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
	Khuôn dạng danh sách chứng thư số thu hồi	RFC 5280	Certificate Revocation List Profile	
	Khuôn dạng chứng thư số	RFC 5280	Public Key Infrastructure Certificate	
	Cú pháp yêu cầu chứng thực	PKCS#10 v1.7 (RFC 2986)	Certification Request Syntax Specification version 1.7	
	Giao thức trạng thái chứng thư trực tuyến	RFC 6960	On-line Certificate status protocol	
	Giao thức gắn tem thời gian	RFC 3161	Time stamping protocol	
	Dịch vụ tem thời gian	ISO/EEC 18014-1:2008 ISO/EEC 18014-2:2009 ISO/EEC 18014-3:2009 ISO/EEC 18014-4:2015	Information technology Security techniques - Time stamping services Part 1: Framework Part 2: Mechanisms producing independent tokens Part 3: Mechanisms producing linked tokens Part 4: Traceability of time sources	
4.18	An toàn cho dịch vụ Web	WS-Security v1.1.1	Web Services Security: SOAP Message Security Version 1.1.1	Khuyến nghị áp dụng
4.19	Khuôn dạng dữ liệu trao đổi sự cố an toàn mạng	RFC 7970	The Incident Object Description Exchange Format version 2 (IODEF)	Khuyến nghị áp dụng

3.12. Yêu cầu về an toàn bảo mật thông tin, dữ liệu, việc sở hữu các thông tin, dữ liệu hình thành trong quá trình cung cấp dịch vụ và phương án quản lý, chuyển giao cho bên thuê và các yêu cầu khác.

3.12.1. Yêu cầu về an toàn bảo mật thông tin, dữ liệu:

3.12.1.1. Yêu cầu bảo mật truyền dẫn, lưu trữ

Dữ liệu quản lý đang trở thành tài sản ngày càng quý giá của mọi cơ quan, tổ chức và doanh nghiệp. Mất mát hoặc lộ thông tin dữ liệu hoặc bị sửa đổi trái phép sẽ gây ra thiệt hại rất lớn không những về tài chính và thời gian để đảm bảo hoạt động bình thường của hệ thống mà quan trọng hơn nhiều là có những dữ liệu không thể khôi phục lại được nếu không có giải pháp sao lưu. Để giảm thiểu nguy cơ mất mát dữ liệu, lộ thông tin, hệ thống phải đảm bảo các yêu cầu bảo mật cần thiết. Thời gian lưu trữ chế độ sự kiện nhận diện AI tối thiểu 90 ngày trên hệ thống. Dữ liệu Camera thuộc sở hữu bản quyền của Ban Quản lý khu kinh tế tỉnh An Giang được toàn quyền sử dụng và khai thác.

*** Bảo mật đường truyền**

Sử dụng đường truyền L2VPN của nhà cung cấp dịch vụ để phục vụ kết nối mạng, đảm bảo được vấn đề triển khai giải pháp kết nối, đảm bảo đáp ứng về mặt lưu lượng dữ liệu sử dụng.

Cụ thể là sử dụng đường truyền L2VPN dùng riêng để thu gom tín hiệu từ các Camera về hệ thống quản lý và lưu trữ tập trung.

*** Tốc độ đường truyền, ghi dữ liệu thực tế**

Hiện nay, các server lưu trữ dữ liệu, kèm theo phần mềm camera thông minh để lưu trữ thông tin và xử lý thông tin tập trung tại trung tâm lưu trữ thông tin (và có thể nâng cấp mở rộng băng thông thêm tùy nhu cầu thực tế sử dụng sau này).

*** Tốc độ ghi dữ liệu của HDD chuyên dụng: 6Gbps/s**

Đây là những HDD lưu trữ chuyên dụng. Có các tính năng tối ưu hóa cho DVR và NVRs, ổ cứng được điều chỉnh để làm việc 24x7 với dung lượng lên tới 10TB. Được trang bị tăng cường firmware, giúp giảm thiểu thời gian chết, đồng thời xử lý công việc nhanh hơn 3 lần so với ổ cứng máy tính để bàn và hỗ trợ lên đến 64 camera HD.

- Được thiết kế để ghi lại 90% thời gian - hỗ trợ lên đến 64 camera Full HD.

- Xử lý 180TB khối lượng công việc 1 năm, gấp 3 lần khối lượng công việc của một ổ cứng máy tính để bàn.

- Không bị bỏ lỡ bất cứ một khung hình nào ngay cả trong môi trường khắc nghiệt nhất, có thể hoạt động trong khoảng nhiệt độ từ 0°C - 70°C.

3.12.1.2. Yêu cầu an toàn hệ thống thông tin theo cấp độ

Yêu cầu bảo đảm an toàn hệ thống thông tin đáp ứng theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông về việc quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Hệ thống camera AI của dự án là hệ thống cơ sở hạ tầng thông tin và thực hiện kết nối, đồng bộ với Cơ sở dữ liệu quốc gia về dân cư theo hướng dẫn tại Công văn số 1552/BTTTT-THH ngày 26/4/2022 của Bộ Thông tin và Truyền thông về việc hướng dẫn kỹ thuật triển khai Đề án 06 (phiên bản 1.0). Nên được xác định là hệ thống thông tin cấp độ 3 trở lên theo quy định tại Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017,

Đơn vị vận hành hệ thống camera an ninh (theo quy định tại khoản 3, Điều 5 Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông), trước khi triển khai thực hiện có trách nhiệm lập hồ sơ đề xuất cấp độ an toàn thông tin và trình cơ quan có thẩm quyền thẩm định, phê duyệt hồ sơ đề xuất cấp độ (theo quy định tại khoản 1, Điều 14 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ), đảm bảo đáp ứng các yêu cầu cơ bản (theo quy định tại khoản 3, Điều 10 Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông), như sau:

I	**Yêu cầu quản lý**
1.1	**Thiết lập chính sách an toàn thông tin**
1.1.1	**Chính sách an toàn thông tin**
	a) Xác định các mục tiêu, nguyên tắc bảo đảm an toàn thông tin
	b) Xác định trách nhiệm của đơn vị chuyên trách về an toàn thông tin, các cán bộ làm về an toàn thông tin và các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin
	c) Xác định phạm vi chính sách an toàn thông tin: - Phạm vi quản lý về vật lý và logic của tổ chức; - Các ứng dụng, dịch vụ hệ thống cung cấp; - Nguồn nhân lực bảo đảm an toàn thông tin

	d) Xây dựng chính sách an toàn thông tin bao gồm: - Quản lý an toàn mạng; - Quản lý an toàn máy chủ và ứng dụng; - Quản lý an toàn dữ liệu; - Quản lý an toàn thiết bị đầu cuối; - Quản lý phòng chống phần mềm độc hại; - Quản lý điểm yếu an toàn thông tin; - Quản lý giám sát an toàn hệ thống thông tin; - Quản lý an toàn người sử dụng đầu cuối.
1.1.2	**Xây dựng và công bố**
	a) Chính sách được tổ chức/bộ phận được ủy quyền thông qua trước khi công bố áp dụng
	b) Chính sách được công bố trước khi áp dụng
1.1.3	**Rà soát, sửa đổi**
	Định kỳ 02 năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.
1.2	**Tổ chức bảo đảm an toàn thông tin**
1.2.1	**Đơn vị chuyên trách về an toàn thông tin**
	a) Thành lập hoặc chỉ định đơn vị/bộ phận chuyên trách về an toàn thông tin trong tổ chức
	b) Phân định vai trò, trách nghiệm, cơ chế phối hợp với các bộ phận, cán bộ trong đơn vị chuyên trách về an toàn thông tin
1.2.2	**Phối hợp với những cơ quan/tổ chức có thẩm quyền**
	a) Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin
	b) Có quy định về đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin
	c) Tham gia các hoạt động, công tác bảo đảm ATTT khi có yêu cầu của tổ chức có thẩm quyền
1.3	**Đảm bảo nguồn nhân lực**
1.3.1	**Tuyển dụng**
	a) Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực an toàn thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng

	b) Có quy định, quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ
1.3.2	**Trong quá trình làm việc**
	a) Có quy định về thực hiện nội quy, quy chế đảm bảo an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống
	b) Có kế hoạch và định kỳ hàng năm có tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng
	c) Định kỳ hàng năm tổ chức, đào tạo các kỹ năng cơ bản về an toàn thông tin cho người sử dụng
1.3.3	**Chấm dứt hoặc thay đổi công việc**
	a) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức
	b) Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc
	c) Có quy định về việc cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc
1.4	**Quản lý thiết kế, xây dựng hệ thống thông tin**
1.4.1	**Thiết kế an toàn hệ thống thông tin**
	a) Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.
	b) Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.
	c) Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ
	d) Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin
	đ) Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.
1.4.2	**Phát triển phần mềm thuê khoán**
	a) Có biên bản hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán
	b) Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm

	c) Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng
	d) Kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.
1.4.3	**Thử nghiệm và nghiệm thu hệ thống**
	a) Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng
	b) Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống
	c) Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống.
	d) Có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống
	đ) Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.
1.5	**Quản lý vận hành hệ thống thông tin**
1.5.1	**Quản lý an toàn mạng**
	a) Quản lý, vận hành hoạt động bình thường của hệ thống
	b) Cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố
	c) Truy cập và quản lý cấu hình hệ thống
	d) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành
1.5.2	**Quản lý an toàn máy chủ và ứng dụng**
	a) Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ
	b) Truy cập mạng của máy chủ
	c) Truy cập và quản trị máy chủ và ứng dụng
	d) Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố
	đ) Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng
	e) Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống

	g) Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác
1.5.3	**Quản lý an toàn dữ liệu**
	a) Xây dựng và thực thi chính sách, quy trình dự phòng và khôi phục dữ liệu
	b) Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: Tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ
1.5.4	**Quản lý an toàn thiết bị đầu cuối**
	a) Quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối
	b) Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa
	c) Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống
1.5.5	**Quản lý phòng chống phần mềm độc hại**
	a) Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động
	b) Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng
	c) Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động
	d) Định kỳ thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống
1.5.6	**Quản lý giám sát an toàn hệ thống thông tin**
	a) Quản lý, vận hành hoạt động bình thường của hệ thống giám sát
	b) Đối tượng giám sát bao gồm: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống (nếu có)
	c) Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát
	d) Truy cập và quản trị hệ thống giám sát
	đ) Loại thông tin cần được giám sát
	e) Lưu trữ và bảo vệ thông tin giám sát (nhật ký hệ thống)
	g) Đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát

	h) Theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin
1.5.7	**Quản lý điểm yếu an toàn thông tin**
	a) Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin: thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác (nếu có)
	b) Quản lý, cập nhật nguồn cung cấp điểm yếu an toàn thông tin; phân nhóm và mức độ của điểm yếu cho các thành phần trong hệ thống đã xác định
	c) Cơ chế phối hợp với các nhóm chuyên gia, cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin
	d) Kiểm tra, đánh giá và xử lý điểm yếu an toàn cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng
	đ) Định kỳ kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.
1.5.8	**Quản lý sự cố an toàn thông tin**
	a) Phân nhóm sự cố an toàn thông tin mạng
	b) Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng
	c) Kế hoạch ứng phó sự cố an toàn thông tin mạng
	d) Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin
	đ) Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường
	e) Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng
	g) Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin
	h) Định kỳ tổ chức diễn tập phương án xử lý sự cố an toàn thông tin
1.5.9	**Quản lý an toàn người sử dụng đầu cuối**
	a) Quản lý truy cập, sử dụng tài nguyên nội bộ
	b) Quản lý truy cập mạng và tài nguyên Internet
	c) Cài đặt và sử dụng máy tính an toàn

1.6	**Phương án Quản lý rủi ro an toàn thông tin**
	Có chính sách, quy trình quản lý rủi ro an toàn thông tin
1.7	**Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ**
	Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ phải được xây dựng trong Quy chế bảo đảm an toàn, trong đó cần làm rõ các nội dung sau đây:
	1. Quy định về bảo đảm an toàn thông tin khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ.
	2. Quy trình xử lý thông tin trên hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ.
	3. Phương án kỹ thuật thực hiện xử lý thông tin trên hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ.
II. Yêu cầu kỹ thuật:	
1	**Yêu cầu về thiết kế hệ thống**
	a) Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm:
	i. Vùng mạng nội bộ
	ii. Vùng mạng biên
	iii. Vùng DMZ
	iv. Vùng máy chủ nội bộ
	v. Vùng mạng máy chủ cơ sở dữ liệu
	vi. Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác
	vii. Vùng quản trị
	b) Có phương án thiết kế đảm các yêu cầu sau:
	i. Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương; sử dụng sản phẩm Mạng riêng ảo đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP
	ii. Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập sử dụng sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc sản phẩm Phòng, chống xâm nhập lớp mạng

	iii. Phương án cân bằng tải và dự phòng nóng cho các thiết bị mạng chính, tối thiểu bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm, tường lửa ứng dụng web, hệ thống lưu trữ tập trung, tường lửa cơ sở dữ liệu (nếu có)
	iv. Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu; sử dụng sản phẩm Tường lửa cơ sở dữ liệu đối với hệ thống cơ sở dữ liệu tập trung, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP
	v. Phương án chặn lọc phần mềm độc hại trên môi trường mạng sử dụng Tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc phương án tương đương
	vi. Phương án phòng chống tấn công từ chối dịch vụ; sử dụng dịch vụ của doanh nghiệp hoặc sản phẩm Phòng, chống tấn công từ chối dịch vụ đối với các hệ thống Trung tâm dữ liệu, điện toán đám mây, hệ thống Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số và hệ thống Kết nối tích hợp, chia sẻ dữ liệu, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP
	vii. Phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng sản phẩm Tường lửa ứng dụng web đối với các hệ thống thông tin được quy định tại khoản 2, Điều 9 Nghị định 85/2016/NĐ-CP
	viii. Phương án đảm bảo an toàn thông tin cho hệ thống thư điện tử; sử dụng sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với hệ thống Thư điện tử, đáp ứng tiêu chí quy định tại khoản 2, Điều 9 Nghị định 85/2016/NĐ-CP
	ix. Phương án quản lý truy cập lớp mạng; sử dụng sản phẩm Quản lý truy cập lớp mạng đối với hệ thống Mạng nội bộ, Trung tâm giám sát điều hành an toàn thông tin mạng, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP
	x. Phương án giám sát hệ thống thông tin tập trung
	xi. Phương án giám sát an toàn hệ thống thông tin tập trung sử dụng sản phẩm Quản lý và phân tích sự kiện an toàn thông tin hoặc sản phẩm tương đương
	xii. Phương án quản lý sao lưu dự phòng tập trung sử dụng hệ thống lưu trữ tập trung và sản phẩm lưu trữ tập trung
	xiii. Phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng, sử dụng sản phẩm Phòng, chống mã độc

	và/hoặc sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối, có chức năng quản lý tập trung
	xiv. Phương án phòng, chống thất thoát dữ liệu; sử dụng sản phẩm Phòng, chống thất thoát dữ liệu đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c, khoản 2, Điều 9 Nghị định 85/2016/NĐ-CP
	xv. Phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ
	xvi. Phương án bảo đảm an toàn cho mạng không dây (nếu có)
2	**Thiết lập, cấu hình hệ thống**
2.1	**Đảm bảo an toàn mạng**
2.1.1	**Kiểm soát truy cập từ bên ngoài mạng**
	a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet
	b) Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài
	c) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng.
	d) Phân quyền và cấp quyền truy cập từ bên ngoài vào hệ thống theo từng người dùng hoặc nhóm người dùng căn cứ theo yêu cầu nghiệp vụ, yêu cầu quản lý.
	đ) Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ được hệ thống cung cấp theo năng lực thực tế của hệ thống
2.1.2	**Kiểm soát truy cập từ bên trong mạng**
	a) Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài theo yêu cầu nghiệp vụ, chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức
	b) Giới hạn truy cập các ứng dụng, dịch vụ bên ngoài theo thời gian
	c) Có phương án kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ theo chức năng và chính sách của tổ chức

2.1.3	**Nhật ký hệ thống**
	a) Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống (nếu hỗ trợ), bao gồm các thông tin sau: - Thời gian kết nối; - Thông tin kết nối mạng (địa chỉ IP, cổng kết nối); - Hành động đối với kết nối (cho phép, ngăn chặn); - Thông tin các thiết bị đầu cuối kết nối vào hệ thống theo địa chỉ vật lý và logic; - Thông tin cảnh báo từ các thiết bị; - Thông tin hiệu năng hoạt động của thiết bị và tài nguyên mạng.
	b) Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống tham gia hoạt động giám sát;
	c) Lưu trữ và quản lý tập trung nhật ký hệ thống thu thập được từ các thiết bị hệ thống
	d) Lưu trữ nhật ký hệ thống của thiết bị tối thiểu 03 tháng.
2.1.4	**Phòng chống xâm nhập**
	a) Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống
	b) Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng
	c) Bảo đảm năng lực hệ thống đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp
2.1.5	**Phòng chống phần mềm độc hại trên môi trường mạng**
	a) Có phương án phòng chống phần mềm độc hại trên môi trường mạng
	b) Định kỳ cập nhật dữ liệu cho hệ thống phòng chống phần mềm độc hại
	c) Bảo đảm năng lực hệ thống đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp
2.1.6	**Bảo vệ thiết bị hệ thống**
	a) Cấu hình chức năng xác thực trên các thiết bị hệ thống để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa;
	b) Thiết lập cấu hình chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa;

	c) Cấu hình thiết bị (nếu hỗ trợ) chỉ cho phép hạn chế các địa chỉ mạng có thể kết nối từ xa
	d) Hạn chế được số lần đăng nhập sai khi quản trị hoặc kết nối quản trị từ xa theo địa chỉ mạng
	đ) Phân quyền truy cập, quản trị thiết bị đối với các tài khoản quản trị có quyền hạn khác nhau;
	e) Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng;
	g) Xóa bỏ thông tin cấu hình, dữ liệu trên thiết bị hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ khỏi hệ thống
2.2	**Bảo đảm an toàn máy chủ**
2.2.1	**Xác thực**
	a) Thiết lập chính sách xác thực trên máy chủ
	b) Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa
	c) Thiết lập chính sách mật khẩu an toàn - Yêu cầu thay đổi mật khẩu mặc định - Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự - Thiết lập thời gian yêu cầu thay đổi mật khẩu - Thiết lập thời gian mật khẩu hợp lệ
	d) Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định
	đ) Vô hiệu hóa tài khoản nếu tài khoản đó đăng nhập sai nhiều lần vượt số lần quy định
2.2.2	**Kiểm soát truy cập**
	a) Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa
	b) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng
	c) Thay đổi cổng quản trị mặc định của máy chủ
	d) Giới hạn địa chỉ mạng được phép truy cập, quản trị máy chủ từ xa
2.2.3	**Nhật ký hệ thống**

	a) Thiết lập lập chức năng ghi nhật ký hệ thống trên các máy chủ - Thông tin kết nối mạng tới máy chủ (Firewall log) - Thông tin đăng nhập vào máy chủ - Lỗi phát sinh trong quá trình hoạt động - Thông tin thay đổi cấu hình máy chủ - Thông tin truy cập dữ liệu và dịch vụ quan trọng trên máy chủ (nếu có)
	b) Đồng bộ thời gian giữa máy chủ với máy chủ thời gian
	c) Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống để không mất hoặc tràn nhật ký hệ thống
	d) Quản lý và lưu trữ tập trung nhật ký hệ thống thu thập được từ máy chủ
	đ) Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 03 tháng
2.2.4	**Phòng chống xâm nhập**
	a) Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ
	b) Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ
	c) Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng
	d) Có phương án cập nhật bản vá, xử lý điểm yếu ATTT cho hệ điều hành và các dịch vụ hệ thống trên máy chủ
	đ) Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng
2.2.5	**Phòng chống phần mềm độc hại**
	a) Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật
	b) Kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt
	c) Quản lý tập trung (cập nhật, cảnh báo và quản lý) các phần mềm phòng chống mã độc cài đặt trên máy chủ
2.2.6	**Xử lý máy chủ khi chuyển giao**
	a) Có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng

	b) Sao lưu dự phòng thông tin, dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành
	c) Có biện pháp kiểm tra, bảo đảm dữ liệu không thể khôi phục sau khi xóa
2.3	**Bảo đảm an toàn ứng dụng**
2.3.1	**Xác thực**
	a) Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng
	b) Lưu trữ có mã hóa thông tin xác thực hệ thống
	c) Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng bao gồm các yêu cầu sau: - Yêu cầu thay đổi mật khẩu mặc định; - Thiết lập quy tắc đạt mật khẩu về số ký tự, loại ký tự; - Thiết lập thời gian yêu cầu thay đổi mật khẩu; - Thiết lập thời gian mật khẩu hợp lệ.
	d) Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định
	đ) Mã hóa thông tin xác thực trước khi gửi qua môi trường mạng
	e) Thiết lập cấu hình ứng dụng để ngăn cản việc đăng nhập tự động đối với các ứng dụng, dịch vụ cung cấp và xử lý dữ liệu quan trọng trong hệ thống
2.3.2	**Kiểm soát truy cập**
	a) Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa
	b) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng
	c) Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa
	d) Phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của ứng dụng với từng người/nhóm sử dụng
	e) Giới hạn số lượng các kết nối đồng thời (kết nối khởi tạo và đã thiết lập) đối với các ứng dụng, dịch vụ máy chủ cung cấp
2.3.3	**Nhật ký hệ thống**

	a) Thiết lập lập chức năng ghi nhật ký hệ thống trên các máy chủ - Thông tin truy cập ứng dụng; - Thông tin đăng nhập khi quản trị ứng dụng; - Thông tin các lỗi phát sinh trong quá trình hoạt động; - Thông tin thay đổi cấu hình ứng dụng
	b) Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung;
	c) Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 03 tháng
2.3.4	**Bảo mật thông tin liên lạc**
	a) Mã hóa thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trước khi truyền đưa, trao đổi qua môi trường mạng; sử dụng phương án mã hóa theo quy định về bảo vệ bí mật nhà nước đối với thông tin mật
	b) Sử dụng kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền
2.3.5	**Chống chối bỏ**
	Sử dụng chữ ký số khi trao đổi thông tin, dữ liệu quan trọng
2.3.6	**An toàn ứng dụng và mã nguồn**
	a) Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý
	b) Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu
	c) Có chức năng kiểm soát lỗi, thông báo lỗi từ ứng dụng
	d) Có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: noSQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF
2.4	**Bảo đảm an toàn dữ liệu**
2.4.1	**Nguyên vẹn dữ liệu**
	Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn
2.4.2	**Bảo mật dữ liệu**
	a) Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ

	b) Sử dụng các phương pháp mã hóa mạnh (chưa được các tổ chức quốc tế công bố điểm yếu ATTT) để mã hóa dữ liệu
2.4.3	**Sao lưu dự phòng**
	a) Thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ
	b) Phân loại và quản lý các dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau
	c) Có hệ thống/phương tiện lưu trữ độc lập để sao lưu dự phòng

3.12.2. Xác định, làm rõ việc sở hữu các thông tin, dữ liệu hình thành trong quá trình cung cấp dịch vụ:

Thông tin, dữ liệu hình thành trong quá trình thuê dịch vụ công nghệ thông tin thuộc sở hữu của cơ quan, đơn vị thuê. Nhà cung cấp dịch vụ có trách nhiệm bảo đảm an ninh, an toàn thông tin, chuyển giao đầy đủ cho cơ quan, đơn vị thuê các thông tin, dữ liệu khi kết thúc hợp đồng thuê dịch vụ công nghệ thông tin.

3.12.3. Phương án quản lý, chuyển giao cho bên thuê, yêu cầu về an toàn bảo mật thông tin, dữ liệu và các yêu cầu khác:

3.12.3.1. Yêu cầu về phương án quản lý, chuyển giao

- Sau khi hết thời gian thuê bên cho thuê bàn giao toàn bộ hiện trạng hệ thống cho chủ đầu tư bao gồm: hạ tầng hệ thống, máy chủ server, ổ cứng lưu trữ, camera AI tại các cổng.

- Các thông tin, dữ liệu hình thành trong quá trình triển khai, vận hành hệ thống Camera AI nhận diện khuôn mặt công nhân ra vào thuộc quyền quản lý của Ban Quản lý khu kinh tế. Bên cho thuê dịch vụ có trách nhiệm bảo đảm an toàn thông tin và bảo mật các thông tin, dữ liệu hình thành trong quá trình cho thuê dịch vụ.

- Các thiết bị của hệ thống trong quá trình vận hành sử dụng bị hư hỏng phải được thay thế trong vòng 12 giờ; phần mềm lỗi, có sự cố phải được xử lý trong vòng 08 giờ (từ khi có thông báo của chủ đầu tư, tính theo giờ làm việc).

- Đơn vị thuê có quyền sở hữu các thông tin, dữ liệu liên quan đến hoạt động cung cấp dịch vụ CNTT theo hợp đồng.

- Yêu cầu và quy trình chuyển giao thông tin, dữ liệu hình thành trong quá trình cung cấp dịch vụ CNTT bao gồm:

+ Phương pháp, công cụ, quy trình và vai trò, trách nhiệm của mỗi bên trong quá trình chuyển giao.

+ Phương án kiểm tra xác định tình trạng thông tin, dữ liệu hình thành trước khi chuyển giao.

+ Phương án sao lưu dữ liệu, hệ thống trước khi bàn giao (nếu cần thiết).

+ Phương án kiểm tra tình trạng thông tin, dữ liệu hình thành sau khi chuyển giao.

+ Phương án kiểm tra, đối soát dữ liệu sau khi chuyển giao.

+ Phương án xóa toàn bộ dữ liệu hoặc hệ thống tại nhà cung cấp dịch vụ sau khi chuyển giao.

- Yêu cầu về chuyển giao tài liệu kỹ thuật liên quan, bao gồm: Tài liệu đặc tả và thiết kế của hệ thống trong suốt quá trình thực hiện hợp đồng (tài liệu phân tích yêu cầu nghiệp vụ; tài liệu thiết kế hoặc đặc tả về hệ thống; tài liệu thiết kế cơ sở dữ liệu; tài liệu hướng dẫn sử dụng hệ thống; tài liệu hướng dẫn quản trị hệ thống; tài liệu hướng dẫn cài đặt, cấu hình hệ thống; tài liệu quản lý cấu hình hệ thống (bao gồm các nội dung thay đổi, cập nhật hệ thống trong quá trình cung cấp dịch vụ CNTT); các tài liệu liên quan khác (nếu có).

- Các cam kết của nhà cung cấp dịch vụ sau khi chuyển giao:

+ Nhà thầu thông báo cho Chủ trì thuê dịch vụ bằng hình thức văn bản, email, điện thoại, nhắn tin nhắc nhở trước 90 ngày khi hợp đồng thuê kết thúc để tiếp tục duy trì phương án thuê theo quy định hiện hành.

+ Nếu như Chủ trì thuê dịch vụ không tiếp tục thuê mà muốn đầu tư xây dựng hệ thống cho riêng mình, thì nhà thầu phải hỗ trợ Chủ trì thuê dịch vụ tối đa trong việc sao chép hệ thống và back up dữ liệu về máy chủ của Chủ trì thuê dịch vụ chỉ định.

3.12.3.2. Yêu cầu về an toàn thông tin mạng, bảo vệ thông tin của người sử dụng dịch vụ và các yêu cầu khác liên quan đến việc thuê dịch vụ CNTT

- Bên cho thuê dịch vụ phải cam kết thiết bị Camera giám sát phải có đầy đủ các tính năng đảm bảo đạt yêu cầu an toàn thông tin mạng cơ bản theo Quyết định số 724/QĐ-BTTTT ngày 07/5/2024 của Bộ Thông tin và Truyền thông về việc ban hành Bộ tiêu chí về yêu cầu an toàn thông tin mạng cơ bản cho camera giám sát

- Bên cho thuê dịch vụ phải cam kết cung cấp tất cả các thiết bị, dịch vụ và giải pháp hoàn chỉnh, đáp ứng đúng và đủ nhu theo nhu cầu của chủ đầu tư. Có kinh nghiệm triển khai hoàn chỉnh và mở rộng hệ thống khi có yêu cầu, có giải pháp, dịch vụ hỗ trợ kỹ thuật có tiêu chuẩn tốt nhất và nhanh chóng nhất trong các năm cho thuê.

- Bên cho thuê phải cam kết triển khai sử dụng, đào tạo, chuyển giao công nghệ để khai thác, sử dụng dịch vụ cho các cơ quan có liên quan; đồng thời sẵn sàng nguồn nhân lực trong tỉnh để hỗ trợ 24/24 giờ khi có yêu cầu.

- Bên cho thuê dịch vụ phải cam kết bảo đảm an toàn bảo mật thông tin, dữ liệu của Bên thuê dịch vụ từ cấp độ 3 trở lên theo quy định tại Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017, để thực hiện kết nối, đồng bộ với Cơ sở dữ liệu quốc gia về dân cư theo hướng dẫn tại Công văn số 1552/BTTTT-THH ngày 26/4/2022 của Bộ Thông tin và Truyền thông về việc hướng dẫn kỹ thuật triển khai Đề án 06 (phiên bản 1.0).

Các yêu cầu về an toàn thông tin mạng, bảo vệ thông tin của người sử dụng dịch vụ và các yêu cầu khác liên quan đến việc thuê dịch vụ CNTT. Các bên tham gia ký kết hợp đồng thuê dịch vụ CNTT thoả thuận thống nhất các yêu cầu về an toàn thông tin mạng và bảo vệ thông tin của người sử dụng trên cơ sở các nội dung chính sau:

+ Phương án, giải pháp đảm bảo an toàn thông tin mạng cho việc cung cấp các dịch vụ CNTT (bao gồm cả công tác giám sát, kiểm soát hệ thống); vai trò, trách nhiệm của mỗi bên trong công tác đảm bảo an toàn thông tin mạng.

+ Các yêu cầu về tổ chức, trình độ chuyên môn, năng lực, kinh nghiệm của các nhân sự tham gia công tác đảm bảo an toàn thông tin mạng, ví dụ: Cơ cấu, bố trí nhân sự; số lượng nhân sự; các yêu cầu về bằng cấp, chứng chỉ chuyên môn; kinh nghiệm trong công việc tương tự,…

+ Các yêu cầu về phân loại vấn đề và kiểm tra, đánh giá mức độ an toàn thông tin mạng định kỳ trong quá trình cung cấp dịch vụ CNTT. Bên cho thuê phải xây dựng thuyết minh Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin đối với Hệ thống camera AI kiểm soát ra vào tại các khu công nghiệp trên địa bàn tỉnh An Giang theo hướng dẫn tại Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông, trình cấp có thẩm quyền phê duyệt và triển khai đầy đủ phương án bảo đảm an toàn thông tin trước khi được đưa vào vận hành, khai thác, hoạt động chính thức.

+ Các yêu cầu về quy trình tiếp nhận, xử lý và báo cáo về các vấn đề về an toàn thông tin mạng (bao gồm cả công tác ứng cứu sự cố) trong quá trình cung cấp dịch vụ CNTT.

+ Các yêu cầu về quy trình xử lý tài sản hình thành liên quan đến hợp đồng thuê dịch vụ CNTT sau khi kết thúc hợp đồng thuê dịch vụ CNTT; ví dụ như: Phương pháp xử lý xoá dữ liệu, thông tin hoặc hệ thống ứng dụng tại nhà cung cấp dịch vụ.

+ Các cam kết về an toàn thông tin mạng, bảo vệ thông tin người sử dụng trong và sau khi kết thúc hợp đồng thuê dịch vụ CNTT.

3.13. Nội dung đào tạo, tập huấn:

a) Tập huấn kỹ thuật quản trị phần mềm quản lý hệ thống camera.

Nội dung:

- Mô hình nghiệp vụ.

- Các chức năng sử dụng của thiết bị

- Kết nối và vận hành kỹ thuật

- Mô hình cài đặt vật lý của hệ thống

- Kỹ thuật quản trị hệ thống

- Chức năng thiết lập mẫu báo cáo.

- Kết nối và vận hành kỹ thuật giữa các phân hệ.

Yêu cầu:

- Nắm vững các hồ sơ liên quan đến hệ thống

- Nắm vững các qui trình quản lý, qui trình vận hành của hệ thống

- Có thể hỗ trợ được cho người sử dụng cuối.

- Có thể quản trị được các yêu cầu thay đổi hay các yêu cầu mới đối với hệ thống.

b) Đào tạo, tập huấn sử dụng cho người dùng:

Nội dung:

- Quy trình luân chuyển và xử lý nghiệp vụ.

- Quy tắc cập nhật dữ liệu, xử lý dữ liệu.

- Quy tắt xử lý thông tin và khai thác thông tin.

- Tìm kiếm, báo cáo và tổng hợp trên các mẫu biểu.

- Cài đặt và xử lý lỗi kỹ thuật.

- Khai thác thông tin.

- Thực hành trực tiếp trên máy tính.

Yêu cầu:

- Hiểu biết đầy đủ về tất cả các chức năng của thiết bị

- Sử dụng thành thạo thiết bị

- Biết cách tuân thủ các qui tắc sử dụng.

- Thời gian: Trước khi triển khai và vận hành thử hệ thống

3.14. Biện pháp an toàn vận hành, phòng chống cháy nổ

- Các phương tiện phòng cháy chữa cháy phải để ở nơi dễ thấy, có đủ bình bọt và máy bơm, bể nước cứu hỏa dự phòng.

- Lập hệ thống biển cấm, biển báo, có phương án và thực tập kiểm tra ứng cứu khi có sự cố.

- Quản lý chặt chẽ vật liệu dễ cháy nổ. Không có bất kỳ ai tự ý mang vật liệu dễ cháy nổ vào khu vực thi công.

- Thường xuyên kiểm tra đường điện, cầu dao điện, các thiết bị dùng điện và phổ biến cho công nhân có ý thức trong công việc dùng điện, dùng lửa để đề phòng cháy. Có bể nước, bình bọt và máy bom nước đề phòng dập lửa khi có hỏa hoạn xảy ra.

- Nghiêm chỉnh chấp hành các quy định, biện pháp thi công hàn hơi và cắt hơi,… Đường ra về và mặt bằng trong khu vực phải thông thoáng, không có vật cản trở.

- Đảm bảo xe cứu hỏa của khu vực vào thuận lợi khi có hỏa hoạn xảy ra.

- Khi thi công cải tạo bể chứa phải kiểm tra xem có độc tố, khí dễ nổ, dễ cháy hoặc thiếu oxi và việc thông gió trước khi cũng như trong thời gian làm viêc…

- Khi tiến hành hàn cốt thép hoặc hàn bulông vào lưới thép phải sử dụng mọi biện pháp để đảm bảo an toàn lao động không để xảy ra cháy nổ. Phải sử dụng hệ thống thông gió đầy đủ và thích hợp, cần có người giám sát, hỗ trợ bên ngoài bể để canh chừng sự an toàn cho những công nhân làm việc trong đó.

- Các biện pháp an toàn, nội quy về an toàn phải được thể hiện công khai để mọi người biết và chấp hành. Ở những vị trí nguy hiểm phải bố trí người hướng dẫn, cảnh báo đề phòng tai nạn.

- Nhà thầu thi công xây dựng có trách nhiệm cung cấp đầy đủ các trang bị bảo hộ lao động, an toàn lao động cho người lao động theo qui định.

Trong quá trình làm việc và sau khi kết thúc công việc phải đảm bảo vệ sinh nơi thi công và khu vực xung quanh.

3.15. Phương thức triển khai, lắp đặt, chuyển giao, bảo hành

3.15.1. Phương thức triển khai

- Nhà thầu cung cấp dịch vụ sẽ đầu tư cung cấp toàn bộ các dịch vụ hệ thống trang thiết bị Camera, đường truyền, ứng dụng, lưu trữ, cài đặt và công tác quản trị, hỗ trợ người dùng phục vụ giám sát an ninh ra vào khu công nghiệp hình thức thuê dịch vụ trong thời gian 05 năm (60 tháng).

- Tổng chi phí thuê trong 05 năm, đơn vị chủ trì sử dụng Hệ thống Camera AI ra vào Khu Công nghiệp sẽ thanh toán cho Nhà thầu cung cấp dịch vụ chia làm 10 đợt, mỗi năm thanh toán 02 đợt, theo phương thức trả trước. Trong đó đợt 01 thanh toán trong vòng 15 ngày sau khi hai bên ký biên bản nghiệm thu, bàn giao dịch vụ để đưa vào sử dụng.

3.15.2. Lắp đặt, chuyển giao, vận hành hệ thống

- Nhà thầu cung cấp dịch vụ sẽ thực hiện lắp đặt thiết bị Camera, đường truyền, hệ thống quản lý, thiết bị phụ trợ, kết nối, thiết lập, bàn giao tài khoản, tài liệu hướng dẫn và thiết bị, phần mềm, tạo lập cơ sở dữ liệu ban đầu trong vòng 90 ngày, kể từ khi hai bên ký hợp đồng.

- Nhà thầu chịu trách nhiệm tạo lập cơ sở dữ liệu ban đầu, kết nối cơ sở dữ liệu về dân cư, bên thuê không phải trả chi phí này cho Nhà thầu**.**

- Nhà thầu cung cấp dịch vụ có trách nhiệm hướng dẫn, đào tạo sử dụng dịch vụ tốt nhất cho đơn vị sử dụng dịch vụ trong suốt thời gian cung cấp.

- Đơn vị sử dụng Hệ thống Camera AI ra vào Khu Công nghiệp có trách nhiệm tự bố trí địa điểm để sử dụng dịch vụ theo hướng dẫn của Nhà thầu cung cấp dịch vụ. Tự quản lý, vận hành và quản trị các account, hệ thống thiết bị đã được trang bị. Không tự ý thay đổi kết nối, cấu hình hệ thống.

3.15.3. Bảo trì, bảo hành

- Định kỳ Nhà thầu cung cấp dịch vụ sẽ thực hiện bảo trì, bảo hành các thiết bị, phần mềm đã cung cấp.

- Trong thời gian cho thuê thiết bị 05 năm (60 tháng), thiết bị có sự cố về kỹ thuật Nhà thầu cung cấp dịch vụ phải có nhiệm vụ sửa chữa, cập nhật hoặc thay thế thiết bị khác.

- Sau khi triển khai xong hệ thống đơn vị trúng thầu sẽ bàn giao cho chủ đầu tư khai thác, đơn vị cho thuê chịu trách nhiệm duy trì và vận hành. Bảo trì hệ thống là công việc bắt buộc thực hiện để đảm bảo tính liên tục của dịch vụ. Việc bảo trì có thể được lên kế hoạch thực hiện vào bất kỳ ngày nào trong tuần (bao gồm cả ngày cuối tuần) và có thể vào bất kỳ thời điểm nào trong ngày. Tuy nhiên, bên cho thuê sẽ nỗ lực hết sức để tiến hành việc bảo trì ở các thời điểm ít ảnh hưởng đến việc sử dụng dịch vụ của bên thuê nhất, cụ thể:

+ Những bảo trì không ảnh hưởng tới bên thuê sẽ được tiến hành bất cứ ngày nào mà không cần thông báo trước.

+ Những bảo trì ảnh hưởng tới bên thuê sẽ được thông báo trước: 48 giờ so với thời điểm bắt đầu bảo trì bằng hình thức email; ít nhất 15 phút trước thời điểm bắt đầu bảo trì bằng hình thức email hoặc điện thoại với những bảo trì khẩn cấp; Tổng thời gian bảo trì không ảnh hưởng tới thời gian sử dụng dịch vụ của bên thuê quá 02 giờ (120 phút).

- Thời gian thực hiện: 60 tháng (theo thời gian thuê hệ thống Camera).

3.16. Thời gian thực hiện thuê dịch vụ CNTT:

- Thời gian chuẩn bị cung cấp dịch vụ: 90 ngày (kể cả ngày nghỉ và ngày lễ theo quy định của pháp luật), bao gồm: thời gian phát triển hình thành dịch vụ, thời gian kiểm thử/vận hành thử, thời gian đào tạo chuyển giao công nghệ.

- Thời gian thuê dịch vụ: 60 tháng (5 năm) kể từ khi nghiệm thu, bàn giao dịch vụ để đưa vào sử dụng đến khi kết thúc thời gian thuê dịch vụ. Sau khi hết thời gian thuê bên cho thuê bàn giao toàn bộ hiện trạng hệ thống cho chủ đầu tư bao gồm: hạ tầng hệ thống, máy chủ server, ổ cứng lưu trữ, camera AI tại các cổng.

3.17. Yêu cầu về các phát sinh trong quá trình khai khác, sử dụng dịch vụ:

- Đơn vị cung cấp dịch vụ thực hiện sự cố phát sinh (nếu có): Xử lý sự cố mất dịch vụ, mất kết nối mạng trong vòng 4 giờ; Trường hợp phải thay thế thiết bị do hỏng hóc từ nhà cung cấp thì thời gian thay thế tối thiểu 24 giờ.

- Những phát sinh trong phạm vi dự toán này và hợp đồng ký kết, đơn vị cung cấp dịch vụ có trách nhiệm thực hiện theo quy định của hợp đồng.

- Những phát sinh ngoài phạm vị dự toán này, ngoài phạm vi hợp đồng, chủ đầu tư và đơn vị cung cấp dịch vụ thực hiện thương lượng và thỏa thuận để thực hiện theo quy định pháp luật hiện hành.

4. Giải pháp và phương pháp luận:

Nhà thầu chuẩn bị đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định tại Chương này, gồm các phần như sau:

1. Giải pháp và phương pháp luận;

2. Kế hoạch công tác.

5. Quy định về kiểm tra, nghiệm thu sản phẩm: Thực hiện theo Thông tư 16/2024/TT-BTTTT ngày 30/12/2024 của Bộ Thông tin và Truyền thông quy định chi tiết nội dung công tác triển khai, giám sát công tác triển khai, nghiệm thu đối với dự án đầu tư ứng dụng công nghệ thông tin; xác định yêu cầu về chất lượng dịch vụ và các nội dung đặc thù của hợp đồng thuê dịch vụ đối với thuê dịch vụ công nghệ thông tin theo yêu cầu riêng