**PŘÍLOHA Č. 1**

k Zadávací dokumentaci

# TECHNICKÁ SPECIFIKACE

1. Specifikace dodávky

Předmětem je implementace komplexního řešení zajištění bezpečnostního procesu na principu automatizované detekce podezřelého chování prostřednictvím inteligentního kamerového systému a softwarových aplikací v prostředí základní školy Generála Janouška v Praze 14 (dále jen „Škola“). Dodávka se dělí na:

a) Dodání, instalaci, konfiguraci, nastavení a zprovoznění inteligentního kamerového systému a aplikací (dále také „IKS“, nebo „Systém“) dle následující specifikace (dále „Dodávka“)
b) Zajištění údržby a provozu dodaného Systému (dále „Zajištění údržby“)

Systém bude na základě speciálního softwarového a hardwarového vybavení samostatně vyhodnocovat chování osob ve vybraných místech areálu školy (vně budov). Situace a podezřelé jevy (hrozby), které budou systémem automatizovaně vyhodnoceny jako alarmové, budou ve formě upozornění prostřednictvím mobilní aplikace zasílány vybraným osobám (subjektům) k vyhodnocení a rozhodnutí o přijatém opatření. Systém bude zároveň zaznamenávat videostreamy jednotlivých kamer a uchovávat je. Celé řešení musí zajišťovat adekvátní míru zabezpečení dat a v maximální míře respektovat ochranu osobních údajů. Videoanalytické funkce musí být nastavitelné na konkrétních kamerách pro konkrétní časové rámce.

Výčet základních hrozeb, které musí být systémem detekovatelné při optimální míře falešných alarmů:

a) Útok aktivního útočníka – vytažení / útok palnou zbraní, umístění NVS – odložené zavazadlo
b) Obecná kriminalita – shlukování (výtržnosti) osob (např. pád osoby při výtržnostech)
c) Vandalismus – sprejerství

Tyto základní hrozby a principy jejich detekce budou dále rozvíjeny za účelem předcházení dalších typů hrozeb dle potřeb školy.

1.1 Místo dodání

Místem dodání je areál základní školy Generála Janouška v Praze 14 se sídlem Praha 9 – Černý Most II, Generála Janouška 1006.

1.2 Předpoklady dodávky

Zadavatel zajistí připravenost místa dodání a to zejména:

- Možnost propojení do místní lokální sítě a jejím prostřednictvím do sítě internet včetně potřebných prostupů na FW.
- Elektrické připojení 230 V.
- Součinnost při nastavování systému, poskytnutí všech informací nutných k správnému nastavení detekčních funkcí, instalace aplikací apod.

A. DODÁVKA

1. Základní součásti dodávky

Dodávka musí zahrnovat zejména následující součásti, které budou dále podrobněji specifikovány:

1.1 HW a SW

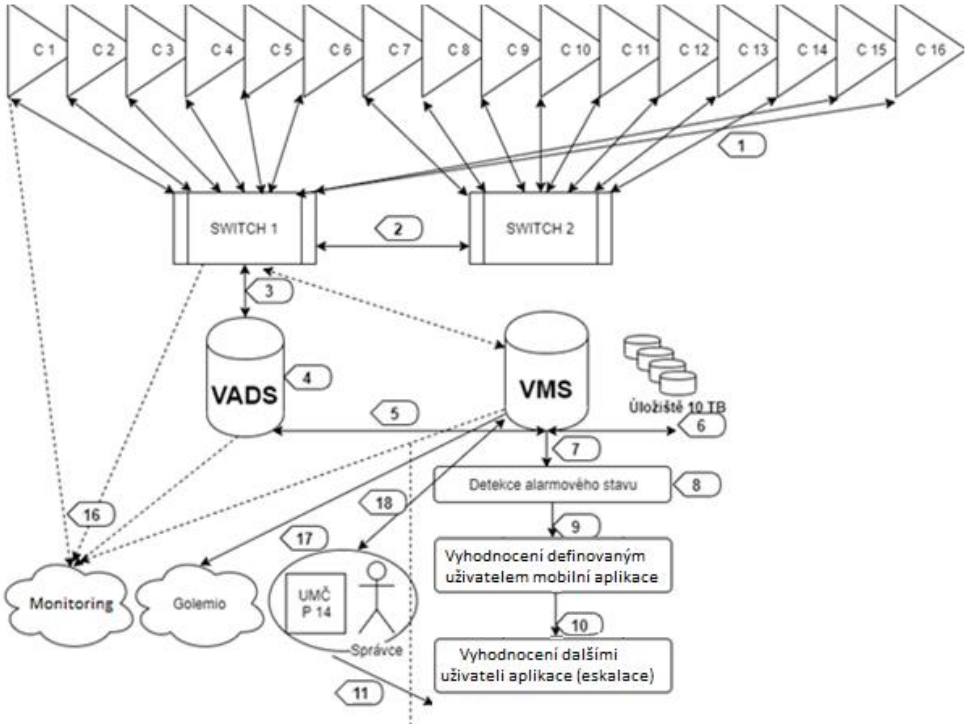
- 16 senzorických prvků (IP kamer) včetně příslušenství
- infrastrukturu (kabeláže, síťové prvky, UPS a ostatní materiál)
- HW a SW pro videoanalýzu („VADS“ – videoanalytický a detekční software)
- HW a SW pro řízení kamer („VMS“ – videomanagement software)
- Řešení pro provozní monitoring systému
- Webová a mobilní aplikace pro řízení detekčních funkcí a alarmových stavů

1.2 Implementační práce

- Instalace kamer a infrastruktury včetně potřebných stavebních úprav a kamerových zkoušek
- Instalace HW a SW včetně potřebných licencí
- Návrh a spolupráce na provedení DPIA analýzy ve součinnosti s určenými osobami školy
- Nastavení a zprovoznění systému
- Vyladění systému za účelem minimalizace falešných alarmů
- Školení pro obsluhu systému

2. Popis požadavků na procesy v rámci Systému

Dodaný Systém musí zahrnovat komplexní řešení bezpečnostního procesu dle následujícího funkčního schématu.




1. Přenos kamerového záznamu – videostreamu – do síťového rozvaděče.

2. Komunikace, propojení mezi síťovými rozvaděči.

3. Komunikace síťových rozvaděčů se serverem pro analytickou činnost.

4. Server VADS provádí výpočet zjištění (analýzu), zdali se v aktuálním streamu nenachází nežádoucí situace (alarmový stav).

5. Server VADS komunikuje s VMS, předávají si data včetně zjištěných alarmových stavů.

6. Server ukládá videostreamy na zabezpečené úložiště včetně metadat.

7+8. V případě detekce alarmového stavu je tato informace zpracována do publikovatelné formy.

9. Předání alarmového stavu předem nadefinovaným uživatelům prostřednictvím k tomu určenému software a mobilní aplikace.

10. – 14. Vyhodnocení alarmového stavu a přijmutí reakce (eskalace na jinou osobu, přijetí). Aktuálně není vyžadováno napojení na informační systémy policejních složek, nicméně do budoucna se tato varianta nevylučuje.

15. V případě oprávněného zájmu export uložených dat.

16. Provozní dohled nad prostředky (monitoring funkčnosti a stavu).

17. Export statistik do datové platformy MHMP – Golemio.

18. Správa a obsluha celého systému.

## 3. Minimální požadavky na součásti systému

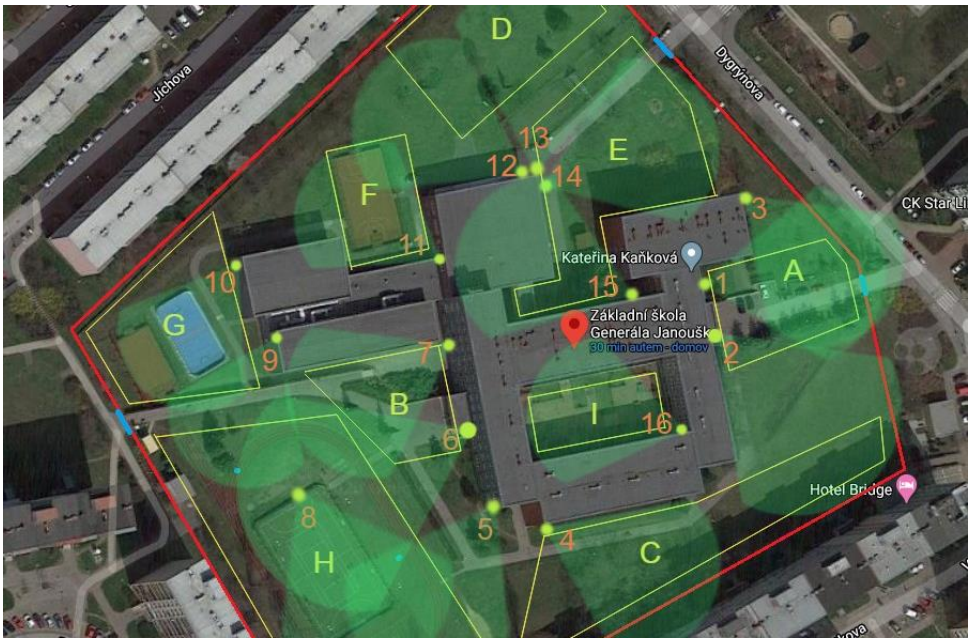
### 3.1 Senzory (IP kamery)

#### 3.1.1 Minimální požadavky na senzory

- 16 kusů IP kamer, plně využitelných pro zamýšlené videoanalytické činnosti
- Kompatibilita s ONVIF a RTSP
- Rozlišení min. FullHD (1920 x 1080@30fps)
- Proměnný objektiv s IR korekcí – optický zoom min. rozsah proměnného ohniska 4-12 mm
- Pracovní teplota -30°C až 60°C
- Externí IR přísvit osazen na venkovním krytu pro noční provoz na vzdálenost minimálně 40 m, IR přísvit musí být oddělen od těla kamery z důvodu eliminace odrazu světla od kapek, pavučin a jiných nečistot, které snižují úspěšnost prováděných analýz.
- Video komprese min H.264/H.265/MJPEG
- Kamerový kryt s odolností (dle EN60529) IP66/IP67 včetně upevnění na fasádu
- Na některých kamerových bodech bude nutné mít data a napájení kamerového setu (kamera, vyhřívání, napájení přísvitu) – vedeno po jednom kabelu ve standardu PoE+ (IEEE 802.3at)

#### 3.1.2 Umístění senzorů (IP kamer)

Kamery musí být připevněny na fasádu budovy, případně k tomu vhodné jiné umístění, přičemž výchozím umístěním v rámci areálu je následující schéma. Konkrétní umístění senzorů musí být provedeno tak, aby bylo přístupné k technickým kontrolám. Konečné umístění včetně výšky musí být určeno v rámci kamerové zkoušky daného umístění s cílem maximalizovat detekční schopnosti a minimalizovat slepá místa. Kamera č. 16 může být alternativně umístěna zvenku budovy za účelem vykrytí slepých míst.




## 3.2 Síťové prvky

### 3.2.1 Minimální parametry síťových rozvaděčů (switch) a kabeláže

- Podpora jumbo packet
- Porty pro kamery min. 100BASE-TX
- Porty pro server min. 1000BASE-T
- SFP slot pro uplink mezi podružnými rozvaděči
- Podpora PoE dle směrnice IEEE 802.3at-2009 s budgetem min. 500 W
- Metalická kabeláž – minimálně CAT5e
- Optická kabeláž – multimod (vícevidové optické vlákno), min. 24 AWG

### 3.2.2 Umístění, vedení a architektura síťových prvků

Síťová architektura typu strom s dvěma sběrnými racky se síťovými rozvaděči, odtud jsou připojeny do hvězdy jednotlivé senzory. Mezi těmito rozvaděči je optické spojení a senzory jsou připojeny metalickým spojením. Pro napájení sensorů se využívá technologie PoE. Kabelové trasy musí být voleny tak, aby bylo v maximální míře využito volných podhledů, které tvoří cca 50 % plánovaných tras. V případě, kdy není možné využít volné podhledy, musí být kabely umisťovány do nástěnných lišt. Kabely mimo budovu musí být umisťovány do ohebných trubek o minimálních vlastnostech odpovídajících typu 2320/LPE-1, UV stabilní, sloužící k mechanické ochraně kabelů. Spojení kamery uchycené na stožáru by mělo být provedeno formou vhodně zvolených antén, které budou umístěny na stožáru vedle kamery a na římse vchodu budovy tak, aby byla zajištěna přímá viditelnost. Napájení kamery bude řešeno ze sloupu osvětlení. V případě, kdy při realizaci bude zjištěna nemožnost provedení instalace na sloup hřiště, bude vybrána alternativní lokalita kamery s pevným spojením (na plášti budovy).

### 3.2.3 Minimální parametry pro zařízení UPS

- Musí být schopen zajistit ochranu proti výpadkům elektrické sítě a záložní napájení serveru po dobu minimálně 20 minut
- Minimální výkon 2200 VA / 1950 W s dobou zálohování min. 5 minut při maximální zátěži
- Minimálně 6 výstupních zásuvek C13
- Vstupní napětí 1 x 230V
- Konstrukce vhodná pro montáž do racku 2U
- Konektor ethernet pro vzdálenou správu a monitoring, ovládání minimálně na úrovni vypnutí, zapnutí, restartu, stavových hodnot přes SNMP a zároveň předávání formou mailu
- Napájecí kabely a konektory o minimální délce 2 m

## 3.3 Serverové vybavení

### 3.3.1 Umístění a architektura serveru/ů

Dodaný serverový HW musí být umístěn ve školní budově v místnosti označené jako serverovna. Ta se nachází v přízemí v pomyslném středu budovy a je tak vhodná k dosažení co nejkratších tras kabeláže. Server/y musí být umístěny ve vlastním racku, který bude zabezpečený a uzamykatelný. Server, stejně jako všechny aktivní prvky systému musí být zálohovány zařízením UPS proti výpadkům elektrické energie a proti nestandardním závadám na elektrické síti.

Požaduje se nasazení multiGPU serveru s možnou virtualizací. Analytické nástroje s neuronovými sítěmi vyžadují pro svou činnost velké množství souběžných procesů a proto je zapotřebí nasazení výkonných externích grafických karet. Jejich počet se bude odvíjet od požadavků VADS, přičemž musí být schopny vyhodnocovat všech 16 detekčních kamer najednou.

### 3.3.2 Provozní požadavky

Pro potřeby případného následného důkazního řízení je nezbytné realizovat i záznam ze všech kamer. Tomu musí odpovídat i záznamová kapacita. Dle dané konfigurace a počtu kamer je zapotřebí kapacita minimálně 10 TB vzhledem k rychlé dostupnosti dat na HDD v RAID konfiguraci. Minimálním požadavkem je doba uchování 120/168 hodin záznamu.

### 3.3.3 Minimální požadavky na server pro videoanalytický a detekční systém (VADS)

- Min. 128GB RAM DDR4
- Min. 2x procesor s 16 jádry (32 vláken)
- Optimální počet grafických karet o parametrech: nVidia RTX obsahující Tensor i Cuda jádra, Cuda minimálně 2176 jader, frekvence 1470 Mhz, paměť 8GB GDDR6
- Úložiště minimálně 2 TB
- Hardware serveru založen na běžně dostupných IT komponentech (nízké náklady na budoucí servis – repas serverů)
- Minimální záruka na server 5 let

### 3.3.4 Minimální požadavky na server pro videomanagement systém (VMS) včetně video archivu

- Min. 16 GB RAM
- Procesorový výkon na úrovni i7 gen.9
- SQL databáze pro přijatá metadata událostí
- Úložiště 10 TB v RAID konfiguraci
- Hardware serveru založen na běžně dostupných IT komponentech (nízké náklady na budoucí servis – repas serverů)

- Minimální záruka na server 5 let

4. Minimální požadavky na software a analytické funkce

4.1 Videoanalytický detekční systém (VADS)

4.1.1 Požadavky na VADS

Software VADS musí pracovat na principu vyhodnocování chování a charakteru objektů na bázi neuronových sítí a ne metodou „background extraction“. Toto řešení je nezbytné zejména proto, že se jedná o venkovní prostory a je nutné zabezpečit nízkou míru falešných poplachů v reálném čase. Zpětné vyhodnocení prostřednictvím forenzních analýz není pro tento účel nejefektivnější právě z důvodu potřeby rychlé reakce na zjištěnou situaci.

Minimálním požadavkem je vybavení minimálně osmi licencemi pro analýzu, přičemž analýza bude prováděna na těch kamerách, které monitorují aktuálně nejrizikovější oblasti. V případě přesunu rizik na jiné oblasti bude možné přepnutí analytických procesů na jinou kameru.

Systém musí umožňovat:

- operátorské rozhraní s velikým množstvím funkcionalit, kompletním auditem všech operací, podporou map a propracovanou správou poplachů (alarmů);
- plnou synchronizaci s provozem školy, možnost nastavit systém tak, že analytické funkce budou aplikovány tam, kde aktuálně existují rizika a to v souladu s plánovaným provozem školy.

4.1.2 Požadované videoanalytické detekční funkce

Systém musí umožňovat pokročilé videoanalytické funkce na principu neuronových sítí zajišťující minimálně tyto funkce:

- Detekce pohybu osob v prostoru a v daném časovém okně
- Detekce změny směru toku a rychlosti pohybu osob
- Detekce narušení perimetru – překročení předdefinovaného prostoru či vkročení do předdefinovaného prostoru + detekce opuštění prostoru nepovoleným způsobem (například přelezení plotu směrem ven – obousměrný perimetr)
- Detekce výskytu osoby poblíž zájmové oblasti po delší časový úsek
- Detekce zanechání objektů ve vytipovaných prostorech
- Detekce dle rozpoznávacích parametrů jako např.
    - detekce pádu osoby
    - detekce shlukování osob
    - detekce palné zbraně
    - detekce odlišného pohybu oproti pohybu v dané lokalitě očekávaného

### 4.2 Videomanagement systém (VMS)

#### 4.2.1 Požadavky na VMS

Musí být využito SW licence řídícího VMS, schopného pracovat i na HW třetích stran, tzn. pracující na operačním systému MS Windows, nebo VMS schopném pracovat v libovolném operačním systému.

Musí být zajištěna plná integrita se stávajícími VMS systémy využívanými v MKS Praha. Musí být zajištěna plná integrita s aktuálně využívanou integrační nadstavbou MKS Praha. Připojení do těchto systémů není plánované v rámci projektu, nicméně je požadována pouze možnost bezproblémové případné integrace.

S ohledem na zvýšené požadavky v oblasti ochrany osobních údajů a tím zvýšeného zabezpečení uchovávaných záznamů se požaduje použití proprietárních kodeků.

Požaduje se škálovatelná serverová licence, s možností doplňování kamer až do počtu 128 kamer.

#### 4.2.2 Minimální technické požadavky na VMS

Systém musí:

- umožňovat dynamické zobrazování víceúrovňových map s možností zobrazení kamer
- umožňovat různá nastavení víceobrazového (multiscreen) zobrazení kamer pro každého operátora zvlášť, včetně vzdáleného ovládání rozložení multiscreenu
- být schopen plnit různé požadavky na zobrazení dle aktuální situace a uživatele
- disponovat uživatelsky definovatelnými tlačítky na ovládání dodatečných speciálních funkcí (například vynucení speciálního módu kamery)
- umožňovat operativní zásahy dle oprávnění uživatelů v návaznosti na řešení dané situace
- umožňovat grupování a možnost dělení do „zájmových skupin“ kamer
- disponovat propracovaným alarm managementem s možností:
    - Definicí alarmových oken
    - Doplnění komentářů s textem
    - Delegování a eskalace poplachů na jiné uživatele
    - Možnosti nastavení úkolů pro jednotlivé uživatele
    - Komunikace mezi operátory (chatování)
    - Kompletního auditu všech činností operátorů, minimálně v rozsahu:
        - Identifikace toho na na co se díval
        - Co vyexportoval
- umožňovat audit všech ostatních operací (přihlášení, odhlášení, atd.)
- podporovat dynamické mapy a dynamická okna na všech monitorech
- podporovat virtuální videomatice
- umožňovat přesunutí kamery z map a naopak
- umožňovat dynamické přesouvání všech funkcionalit do jednotlivých sekcí (např. seznam kamer do jakého chci okna atd.)
- umožňovat práci s propojenými daty (například SPZ/RZ)
- umožňovat jednoduchou tvorbu uživatelských sekvencí na monitorech (sekvence kamer, případně presetů otočných kamer)
- umožňovat tvorbu reportů (např. pro poplachy z venku)
- umožňovat propojení s Active Directory pro správu velkého množství operátorů, práv atd.
- disponovat kapacitou připojitelného počtu kamer, rozšiřitelnou až do počtu 128 kamer na server, a až do 320TB on-line databáze.
- umožňovat zapojení více serverů do jednoho celku (virtuální matice)
- disponovat datovým tokem pro záznam do databáze min. 450Mbit/s
- disponovat možností nastavení různé délky záznamu pro každou kameru zvlášť (16 ringů a 3 úrovně archivu)

- disponovat automatickým zálohováním s možností nastavení pro každou kameru nezávisle na různá úložiště a s možností kryptování
- disponovat možností nastavení různé kvality a rychlosti záznamu pro záznam a živý obraz zvlášť (každá kamera má jiné nároky)
- disponovat možností změny kvality, rychlosti a rozlišení kamery v závislosti na detekci aktivity na kameře i s možností nastavení časových pásem.
- disponovat možností exportu záznamů s možností šifrování (ochrana proti zneužití exportovaných dat)
- disponovat kompresí záznamu určenou pro bezpečnostní aplikace – ne standardní multimediální H.264, H.265, MPEG4. Standardní multimediální rozdílová komprese často způsobuje ztrátu detailů na rozdílových snímcích a hrozí zde ztráta důležitých obrazových dat.
- disponovat možností filtrování počtu snímků za sekundu záznamu ve více časových stupních (například 10 dnů se vybrané kamery budou nahrávat 25fps, potom pouze 5fps a záznamy starší než měsíc budou mít už jenom 2fps. Tato vlastnost nemění kvalitu záznamu, ale pouze jeho snímkovou rychlost a ušetří výrazně nároky na velikost databáze.
- disponovat univerzálním výstupním streamem (například pro možnost integrace)
- disponovat možností definování limitů maximálního datového toku, použitého pro přenos živých snímků a záznamu na uživatelské stanice. Pro případ zahlcení sítě v místě serveru.
- disponovat podporou ONVIF a RTSP.
- mít otevřené rozhraní SDK pro integrování systému do platforem třetích stran – ZDARMA (včetně technické podpory od výrobce pro programátory)

5. Zajištění provozního monitoringu

Systém musí obsahovat kontrolní funkcionality, které budou zajišťovat:

- Upozornění na nefunkčnost systému jako celku
- Upozornění na nefunkčnost konkrétních kamerových prvků
- Upozornění na nefunkčnost systému předávání alarmových stavů
- Upozornění na nefunkčnost VMS nebo VADS

Systém musí umožňovat vzdálený přístup a správu pro řešení hlášených závad na systému.

6. Aplikace pro řešení alarmových stavů

6.1.1 Požadované řešení aplikace

V případech, kdy dojde k vyhodnocení alarmového stavu systémem VADS, musí být předána informace o tomto alarmu prostřednictvím mobilní aplikace předem stanoveným osobám / subjektům.

Aplikace musí umožňovat obdržet zaslaná upozornění na alarmové stavy a přijmout patřičné řešení včetně možné delegace na jiného uživatele. Zároveň řídit aktivaci nebo deaktivaci detekčních funkcí a zobrazovat další informace

Za účelem snadné správy se požaduje nasazení speciálního software zajišťující možnost řídit a předávat alarmové stavy a to ve formě:

a) Webová aplikace – dostupná z internetu obsahující a umožňující:
    a. Všechny funkce mobilní aplikace
    b. Správu uživatelů a jejich úrovní přístupu

c. Tvorbu a správu rolí pro předávání alarmových stavů s možností přiřazení postupu předávání alarmu k jednotlivým typům alarmu
d. Zajistit otevřené rozhraní pro možnou budoucí zdarma integraci na PCO různých složek

a zároveň

b) Mobilní aplikace – jejíž minimální parametry jsou:

- Forma PWA
- Řízený přístup uživatelů dle nastavení ve webové aplikaci / serveru
- Aplikace musí umět přijmout alarmový stav upozornit její obsluhu zvukem a notifikačním textem, umožnit obsluze přijetí alarmu, nebo jeho eskalaci na jiného uživatele.
- Aplikace musí umět kontinuálně kontrolovat spojení se serverem a podávat upozornění o offline (nežádoucích) stavech.
- Aplikace musí umožňovat zastřežení a odstřežení detekčních funkcionalit jednotlivých kamer a souhrnně všech kamer najednou.
- Aplikace musí umožňovat podání informace o funkčním stavu jednotlivých kamer (zapnuta / vypnuta), detekčním stavu kamer (zastřeženo, odstřeženo)
- Všechny uvedené funkcionality musí být uživatelsky intuitivně proveditelné a zjistitelné
- Aplikace musí umožňovat zobrazení podrobností o alarmovém stavu:
    - Datum a čas
    - Označení kamery
    - Typ alarmu
    - Náhledové foto bez možnosti uložení a dalšího šíření.
- Aplikace musí umožňovat historický přehled alarmových stavů a jejich způsobu řešení, včetně informace, který uživatel a v jaký den a čas alarm řešil a to včetně uživatelů, na které bylo řešení delegováno
- Řešení musí logovat minimálně činnosti týkající se:
    - přijetí a vyhodnocení alarmových stavů včetně uživatelů, kteří se řešení účastnili
    - autentizace a správy uživatelů

#### 6.1.2 Bezpečnostní požadavky

- Mobilní aplikace i webové rozhraní musí být v souladu s aktuálními standardy pro informační a kybernetickou bezpečnost (zejména v oblasti autorizace a autentizace uživatelů) a požadavky na ochranu osobních údajů.

## 7. Statistické výstupy

Systém musí být schopen nastavení automatizovaného generování statistických výstupů za konkrétní časová období a připraven předávat data do datové platformy MHMP – GOLEMIO. Datové sady musí být strukturované dle potřeb datové platformy. Data budou předávána skrze API rozhraní postavené na filozofii REST API ve formátu JSON. Struktura dat bude vytvořena dle implementovaných prvků a zavedených typů algoritmů a to na základě konkrétního požadavku OICT.

8. Ochrana osobních údajů

Dodavatel musí být od počátku v komunikaci s vedením Školy a pověřencem pro ochranu osobních údajů Školy. Dodavatel musí provést DPIA (Analýzu dopadu na ochranu osobních údajů), přičemž musí zvažovat možnosti a schopnosti dodávaných technologií, projednat je s pověřencem a předložit vedení školy.

Vzhledem k tomu, že většina osob, které budou zaznamenávány a vyhodnocovány kamerovým systémem jsou nezletilí, jedná se o citlivá data.

Veškeré části systému musí být instalovány, nastaveny a provozovány tak, aby minimalizovaly riziko úniku osobních údajů, neoprávněného přístupu nebo zásahu do systému. Veškeré činnosti s osobními údaji musí být v systému logovány. Úložiště musí být zabezpečena, případně šifrována.

9. Implementační práce

Dodavatel zajistí kompletní zprovoznění dodaného systému do funkčního stavu a provede nastavení detekčních funkcí. Všechny HW a SW součásti systému budou implementovány tak, aby byl minimalizován dopad na provoz školy.

Nastavení detekčních funkcí do časových programů bude provedeno po konzultacích se zástupci školy.

Na základě kamerových zkoušek budou určeny finální pozice umístění kamer, v případě, kdy se umístění některých kamer výrazně odliší od umístění zvoleného po kamerové zkoušce, musí k tomu být dostatečný důvod odsouhlasený zástupcem školy. Umístění kamer musí minimalizovat slepá místa.

10. Školení pro obsluhu systému

Dodavatel musí zajistit prvotní proškolení osob, které budou mít jakékoliv úkoly týkající se předmětu dodávky.

B. ZAJIŠTĚNÍ PROVOZU A ÚDRŽBY

1. Dodavatel zajistí podporu provozu a údržby dodaného systému a to na 2 roky od doby převzetí dodávky.

Údržba systému zahrnuje:

2. Zajištění potřebných licencí pro celý systém.
   Dodavatel zajistí na svůj účet dodání všech licencí potřebných pro provozování systému.
3. Zajištění pravidelných činností – zejména profylaxe a ověření funkčnosti v následujícím rozsahu:

- Kontrola nahrávacího zařízení (rekordér / IP SW)
- Kontrola živých obrazů kamer
- Kontrola správnosti rozvrhu nahrávání
- Přehrání částí záznamu
- Kontrola systémové konfigurace – čas, datum, SMART HDD
- Kontrola logů rekordéru/SW
- Vyčištění nebo výměna filtrů
- Kontrola všech zařízení komunikujících s kamerovým systémem
- Test komunikace s nadřazeným systémem (Mobilní aplikace, EZS, PCO) v případě, že je využita
- Kontrola obrazu senzorů a pozic, případné doostření objektivu
- Vyčištění krytu a optiky senzorů
- Vizuální kontrola konektorů, případné dotáhnutí svorkovnic v rozvaděčích kamer
- Test výpadku napájení – funkce UPS/záložního zdroje
- Test výpadku sensoru (kamery)
- Test výpadku serveru/rekordéru (v případě FailOver architektury)
- Restart zařízení – test bezchybného startu systému
- Kontrola konektorů a izolací v rozvaděči
- Kontrola vlhkosti v rozvaděči / instalační krabici
- Kontrola serverového nastavení a logů
- Kontrola funkčnosti aplikací pro předávání alarmových stavů

3.1 Pravidelnost jednotlivých činností je odvislá od doporučení stanovených výrobcem / dodavatelem daných částí systému
3.2 Za účelem možnosti kontroly vzdáleně umožní škola vzdálený přístup k systému.

4. Nepravidelné činnosti – zejména úpravy a opravy a požadavky na změny v nastavení systému hlášené prostřednictvím service desku dodavatele zahrnující:

- Požadavky na změny v detekčních funkcích
- Požadavky na změnu časového rozvrhu detekčních funkcí
- Požadavky na změnu v nastavení serveru a aplikací spojených s alarmovými stavy
- Provedení potřebných aktualizací software
- Výměny prvků systému případně jejich úpravy a nastavení

4.1 Veškerý materiál, zařízení a jejich části, které nejsou předmětem záručního nebo reklamačního řízení, hradí zadavatel dle předem odsouhlasené ceny.
4.2 Požadavky na změny v detekčních funkcích, časového rozvrhu a úpravy workflow alarmových stavů provádí dodavatel v rámci paušální částky za údržbu maximálně 3x měsíčně v prvních 6

měsících od převzetí dodávky a následně maximálně 1x měsíčně po zbytek trvání smlouvy. V ostatních případech tyto požadavky hradí zadavatel dle předem odsouhlasené ceny.

5. Způsob předávání hlášení a požadavku dodavateli

Zadavatel umožní přístup dodavateli do svého service desku, který bude sloužit jako oficiální evidence hlášení a požadavků.

Dodavatel zajistí reakční doby na hlášení závad dle následující tabulky.

| **Typ závady** | **Reakční doba** |
|---|---|
| Závada kategorie A – Vysoká – stav celkové nefunkčnosti systému a nemožnost využívat klíčové funkcionality systému. | Přijetí do 8 hodin od okamžiku nahlášení v pracovních dnech (pondělí-pátek) vyjma státních svátků v době od 8 do 16 hodin. Odstranění do 2 pracovních dnů od přijetí. |
| Závada kategorie B – Střední – stav, kdy klíčové komponenty vykazují částečné závady a/nebo některé běžné komponenty nejsou funkční. | Přijetí do 8 hodin od okamžiku nahlášení v pracovních dnech (pondělí-pátek) vyjma státních svátků v době od 8 do 16 hodin. Odstranění do 5 pracovních dnů od přijetí. |
| Závada kategorie C – Nízká – stav, kdy jsou všechny komponenty systému funkční, ale některé běžné komponenty vykazují částečné závady. | Přijetí do 8 hodin od okamžiku nahlášení v pracovních dnech (pondělí-pátek) vyjma státních svátků v době od 8 do 16 hodin. Odstranění do 10 pracovních dnů od přijetí. |

Změnové požadavky jsou prováděny v termínech dle předchozí domluvy, přičemž se vychází z časových předpokladů Závad kategorie C přiměřeně upravené dle náročnosti.

V případě nedodržení reakční doby a/nebo doby odstranění závady, je Dodavatel povinen poskytnout Objednateli slevu z fakturace v daném období ve výši dle následující tabulky, pokud nebude dohodnuto jinak:

| **Typ závady** | **Sleva z fakturace** |
|---|---|
| Závada kategorie A | 75% |
| Závada kategorie B | 50% |
| Závada kategorie C | 25% |

## C. FUNKČNÍ ZKOUŠKY

Účelem této části je vymezit provedení testování funkcí vzorku a podmínky provedení funkčních zkoušek, stejně jako vymezení technických podmínek a zařízeních dodaných účastníkem v rámci posouzení vzorku.

Funkční zkoušky musí být provedeny a vyhodnoceny před kompletní instalací Systému tak, aby byla ověřena funkčnost dodaného systému. Bez úspěšného výsledku funkčních zkoušek nebude přistoupeno k dodání kompletního Systému.

### 1.1 Způsob provedení

V rámci funkčního vzorku budou testovány na vybraných nabízených komponentách funkce a vlastnosti dle ZD. Pro testování budou použity celkem tři sensory (kamery), analytická část, záznamová a distribuční technologie včetně monitorů, na kterých budou jednotlivé vlastnosti prezentovány. Součástí testování bude i aplikace pro zobrazení výsledků / událostí / alarmů analytického modulu.

Účastník naistaluje jím nabízené zařízení na dočasnou kabeláž / bezdrátové pojítko a postupně vyzkouší funkce dle níže uvedeného zkušebního protokolu.

### 1.2 Testování analytických funkcí

Protože analytická část je klíčovým prvkem nabízeného systému, bude mu věnována maximální pozornost a korektní funkce analytických nástrojů je klíčová pro úspěšné dokončení funkčního vzorku. Budou testovány tyto scénáře:

a) Útok aktivního útočníka – vytažení / útok palnou zbraní (FUNKCE A)
b) Umístění NVS (odložení a zanechání batohu v místě pravděpodobného shluku osob) (FUNKCE B)
c) Obecná kriminalita – shlukování osob, pád osoby při rvačce (FUNKCE C)
d) Vandalismus – sprejerství (FUNKCE D)

### 1.3 Podmínky testování jednotlivých funkcí

FUNKCE A:

Figurant 1 stojící ve vzdálenosti 10 metrů od kamery umístěné před vstupem do školy vytáhne znehodnocenou palnou zbraň a namíří ji na figuranta 2, který stojí 4 metry od figuranta 1. Test proběhne za běžné denní viditelnosti.

FUNKCE B:

Figurant 1 jde volným krokem před vstupem do školy a následně odloží běžný školní batoh ve vzdálenosti 12 metrů od kamery umístěné před vstupem do školy. Test proběhne za běžné denní viditelnosti.

FUNKCE C:

Figurant 1 bude simulovat rvačku s figurantem 2 ve vzdálenosti 15 metrů od kamery umístěné na fasádě budovy. Při této rvačce jeden z figurantů bude simulovat pád na zem po strčení druhým figurantem. Test proběhne za běžné denní viditelnosti.

FUNKCE D:

Figurant projde po chodníku podél zdi školy, která je pokryta kamerou. Vprostřed stěny se zastaví a z chodníku přijde až ke stěně. V ruce bude držet sprej a bude předstírat kreslení po zdi. Test proběhne za noční viditelnosti ve vzdálenosti maximálně 30 metrů od kamery umístěné na fasádě budovy.

### 1.4 Technická zajištění

Pro provedení zkoušky funkčního vzorku bude ze strany zadavatele připraveno:

- konstrukce pro uchycení pevné kamery na definovaných bodech
- stůl pro instalaci serverové a další technologie
- zajištění dostatečného množství přívodů 230V u stolu

Dodavatel pro otestování vzorku zajistí:

- Komplet nabízené venkovní kamery včetně IR přísvitu v potřebném počtu kusů
- Záznamovou a serverovou technologii (SW, HW, switche) nutnou k otestování funkcí dle níže uvedeného protokolu – konkrétní podobu nespecifikujeme, záleží na nabízené technologii
- Analytické servery a HW potřebný pro testování nabízených analytických funkcí
- Minimálně 2 ks libovolných Full HD monitorů pro testování obrazu a funkcí VMS
- Mobilní zařízení pro prezentování uživatelské aplikace
- Další nutné zařízení pro testování dle potřeby

### 1.5 Testování vzorku

Příloha obsahuje zkušební protokol, dle kterého bude postupně proveden test zkušebního vzorku, korektní reakce systému v jednotlivých krocích je podmínkou přijetí vzorku jako celku.

### 1.6 Hodnocení

Za úspěšný výsledek zkoušky vzorků bude považováno jen splnění všech bodů ve zkušebním protokolu.

## 2. Akceptace

Akceptací díla se rozumí předání kompletního funkčního systému dle zadání včetně nastavení uživatelů aplikací, zaškolení dotčených osob a předání zkušebního protokolu s úspěšným výsledkem zkoušky.

## 3. Prohlídka místa

Zadavatel umožní termín obhlídky objektu a umožní náhled do studie proveditelnosti tohoto projektu. Tato studie z bezpečnostních důvodů nebude předávána třetím stranám, ale pouze k nahlédnutí bez možnosti kopie.

4. Zkušební protokol

| Číslo | Testovaná funkce | Splňuje | Nesplňuje |
|---|---|---|---|
| **1** | **Vzorek je korektně sestaven, kamery jsou funkční, monitorovací pracoviště v sestavě dle zadání** | | |
| **2** | **Funkce VMS** | | |
| | Přepínání kamer na jednotlivé monitory v případě alarmového stavu (minimální rozsah matice 2x2 na jednom monitoru) | | |
| | Spuštění, zastavení sekvence 2 kamer s přepínáním 5 sekund pro konkrétní sekci multiscreenového zobrazení | | |
| | Synchronizované přehrávání záznamu ve zvolených sekcích pomocí myši | | |
| | Vyhledávání v záznamu podle změn v definované oblasti | | |
| | Uživatelské nastavení zóny v obrazu, kde pohyb způsobí upozornění obsluhy zvukovým signálem | | |
| | Vyhledávání analytických funkcí v archívu a jejich zobrazení | | |
| **3** | **Sabotáž u pevné venkovní kamery**<br>**zakrytí**<br>**natočení**<br>**rozostření**<br>**úplné odpojení** | | |
| | SW registruje a ukládá alarm sabotáž | | |
| | Je proveden alarmový střih na monitor č. 1 | | |
| | Zobrazení poruchy v mobilní aplikaci | | |
| **4** | **Analytické funkce sensoru (u venkovní kamery)** | | |
| | SW registruje, zobrazuje a ukládá alarm analytické funkce ve VMS – analytická funkce A | | |
| | SW registruje, zobrazuje a ukládá alarm analytické funkce v uživatelském SW – analytická funkce A | | |
| | Je proveden alarmový střih na monitor č. 1 – analytická funkce A | | |
| | SW registruje, zobrazuje a ukládá alarm analytické funkce ve VMS – analytická funkce B | | |
| | SW registruje, zobrazuje a ukládá alarm analytické funkce v uživatelském SW – analytická funkce B | | |

| | | | |
|---|---|---|---|
| | Je proveden alarmový střih na monitor č. 1 – analytická funkce B | | |
| | SW registruje, zobrazuje a ukládá alarm analytické funkce ve VMS – analytická funkce C | | |
| | SW registruje, zobrazuje a ukládá alarm analytické funkce v uživatelském SW – analytická funkce C | | |
| | Je proveden alarmový střih na monitor č. 1 – analytická funkce C | | |
| | SW registruje, zobrazuje a ukládá alarm analytické funkce ve VMS – analytická funkce D | | |
| | SW registruje, zobrazuje a ukládá alarm analytické funkce v uživatelském SW – analytická funkce D | | |
| | Je proveden alarmový střih na monitor č. 1 – analytická funkce D | | |
| **5** | **Funkce uživatelského SW na mobilním zařízení** | | |
| | Vytvoření nového uživatele | | |
| | Bude zadáno jméno a heslo pro danou osobu a provedeno přihlášení. | | |
| | Přidání sensoru včetně popisu, včetně zobrazení obrazu ze sensoru. | | |
| | Aplikace zobrazí alarmový stav danému uživateli a ten ho přijme k řešení | | |
| | Uživatel eskaluje v aplikaci poplach na další oprávněné osoby | | |
| | Všichni uživatelé mají možnost alarm uzavřít jako vyřešený. | | |
| | Uživatel si zobrazí přehled všech alarmových stavů řazených od posledního k prvnímu | | |
| | Aplikace zobrazuje vizuálně stav konkrétních senzorů (kamera mimo provoz, zapnutá detekce, vypnutá detekce) | | |
| | Aplikace běží na pozadí, alarmové stavy jsou zobrazovány textem a zvukem | | |

## D. SEZNAM ZKRATEK

- NVS – Nástražný výbušný systém
- FW – Firewall
- UPS – zdroj nepřerušovaného napájení
- VADS – Videoanalytický a detekční software
- VMS – Videomanagement software
- DPIA – Data protection impact assessment (posouzení vlivu na ochranu osobních údajů)
- ONVIF – Open Network Video Interface Forum (otevřený standard pro komunikaci bezpečnostních systémů založených na IP technologii)
- RTSP – Real Time Streaming Protocol (Streamovací protokol v reálném čase)
- PoE – Power over Ethernet (napájení po datovém síťovém kabelu)
- SNMP – Simple Network Management Protocol
- MKS Praha – Městský kamerový systém Praha
- SPZ/RZ – Státní poznávací značka/Registrační značka
- SDK – Software development kit (sada vývojových nástrojů)
- PWA – Progresivní webové aplikace
- REST API – Representational State Transfer, rozhraní konektoru
- JSON – JavaScript Object Notation
- OICT – Operátor ICT, a.s.
- EZS – Elektronická zabezpečovací signalizace
- PCO – Pult centrální ochrany