

Požadavky na serverovou část

Architektura systému bude umožňovat systém flexibilně rozšiřovat jak o jednotlivé kamerové body, kamery a pracoviště operátorů. Základní sestava musí umožňovat bezproblémové rozšiřování systému o další kamery při zachování současných parametrů i funkčnosti. Řešení musí být rozšiřitelné. K použitému softwaru požadujeme technickou podporu v českém jazyce. Software pro kamerový systém a aplikace pro provozní deník kamerového systému musejí být v české lokalizaci a to včetně návodů. Všechny použité softwarové licence budou uvedeny v nabídce.

Centrální část systému (server nebo servery) budou umístěny v serverovně dodavatele. Server bude s kamerovými body a pracovišti spojen pomocí datového okruhu zajištěného dodavatelem.

Může se jednat o fyzický nebo virtualizovaný server či servery. Toto záleží na volbě dodavatele.

Základní požadavky na server:

- kapacita pro OS a kamerový software a pro provozní logy dat s roční historií (přihlášení uživatelů, práce se záznamy, logy serveru, dohledu kamer apod.), data budou zálohována na externí úložiště
- kapacita pro ukládání obrazu ze všech kamer po dobu minimálně 16 dnů (kapacita pro počet kamer x 35 hodin x 16 dnů), data budou zálohována např. formou zrcadlení disků, zálohování na externí úložiště se nevyžaduje
- kapacita 16 dnů se uvažuje pro záznam v plném rozlišení kamery a 10 snímků za sekundu
- server musí mít zálohované úložiště dat pro případ poruchy disku / provozní data jako jsou logy činnosti operátorů, logy po výpočet SLA, záznamy provozního deníku se budou zálohovat na externí úložiště, aby se zabránilo jejich ztrátě
- server musí mít záložní zdroj napájení (UPS), doba zálohování serveru musí být minimálně 8 hodin v případě výpadku napájení od distributora
- server i ostatní síťové prvky budou mít redundantní zdroje a UPS budou také redundantní
- rezerva pro záznamy označené tak, aby nedošlo k jejich vymazání bude 2 TB

Základní požadavky na serverovnu:

- plně klimatizované datové centrum
- redundantní zdroje UPS
- redundantní konektivita
- záloha motorgenerátorem
- dohled 7x24 (non-stop)
- detekce požáru
- kamerový dohled nad data centrem
- bezprašné prostředí
- uzamykatelné stojany
- zabezpečení a ostraha objektu (alarm, napojení na pult centrální ochrany)
- fyzický přístup pouze autorizovaným osobám s logováním historie přístupu

Pro přístup ze sítě internet (pracoviště operátora, náhled na živý obraz z MÚ) bude server disponovat VPN s ochranou certifikátem a heslem na úrovni uživatele nebo zařízení. V případě ztráty

(zcizení) daného zařízení (PC, notebook apod.) musí být možné zabránit přístupu ke kamerovému systému, např. formou smazání certifikátu pro dané zařízení na straně serveru.

Server a celý kamerový systém musí být zajištěn proti zneužití cizí osobou.