

Návrh systému elektronické evidence událostí

K zadávacímu řízení s názvem

„Zajištění fyzické ostrahy objektů Dopravního podniku hl. m. Prahy, a.s.“

Zadavatel

Dopravní podnik hl. m. Prahy, akciová společnost

Zpracoval:



V Praze: 6. 2. 2025

Obsah

1	Úvod	3
2	Vybavení osob mobilním zařízením	5
3	Přístup do systému	5
4	Záznam docházky	6
5	Trasy a časy pochůzek	6
6	Vyhodnocování pochůzek.....	7
7	Úkoly a pokyny při výkonu pochůzek.....	7
8	Tíseň	7
9	Záznam činností	8
10	Fotodokumentace.....	8
11	Technické parametry mobilního zařízení	8
12	Archivace dat při výpadku spojení	9
13	Podpora systému	9
14	Tok dat	10
15	Závěr	10

1 Úvod

CENTR GUARD vznikl jako online pochůzkový systém vyvinutý a provozovaný společností TTC TELSYS. Jedná se o ryze českou aplikaci, která je v současnosti využívána v 8 zemích světa. Ve spolupráci se společností CENTR GROUP se z pochůzkového systému vyvinul užitečný software pro elektronickou evidenci událostí z průběhu směny, evidenci mimořádných událostí. V čase na přání klientů jsme systém rozšířili o další moduly jako jsou:

- evidence osob,
- evidence vozidel,
- evidence školení BOZP a PO pro vstup do objektu vč. sledování expirace doby platnosti,
- v neposlední řadě modul zápůjčování majetku, který lze využít pro zápůjčku vozidel, klíčů, náradí apod., výhodou modulu je, že ke každé věci je klientem přidělení seznam oprávněných osob, kterou bezpečnostní pracovník vidí a může tak rovnou ověřit u žadatele zápůjčky, zda na to má právo, či nikoliv.

Pro provoz systému CENTR GUARD je třeba pouze mobilní telefon s operačním systémem Android, NFC čipy jako kontrolní body a připojení k internetu. Další alternativou pro využití systému je tablet, který je využíván mimo terénní působení, převážně recepce.

Telefon lze kompletně spravovat vzdáleně. Uživatel mobilního terminálu může používat jen to, co mu správce nastaví přes webové rozhraní. Například povolení pouze vybraných funkcí systému, volání, SMS. Do nastavení telefonu nelze zasahovat bez svolení správce, stejně tak nelze používat nežádoucí aplikace, které nesouvisejí s výkonem práce.

Průběh práce ostrahy lze sledovat online na webovém rozhraní ve webovém prohlížeči (není třeba nikam nic instalovat).

Protože mobilní telefon má na rozdíl od jiných, jednoúčelových systémů mnohem širší možnosti použití, lze prostřednictvím naší aplikace kromě vykonávání pochůzek posílat fotky, videa, GPS souřadnice, vyplňovat formuláře, volat a posílat SMS pouze na povolená telefonní čísla, díky akcelerometru zjišťovat polohu telefonu a chránit tak pracovníka (systém monitoringu osamocených pracovníků) atd. Dále lze využívat

vybrané aplikace třetích stran – různé komunikátory, emailový klient, aplikace pro připojení na CCTV systémy apod.

Pochůzky s automatickým vyhodnocováním – pro koncového zákazníka zcela transparentní. Report chodí ve formátu PDF přímo ze systému a je tak mnohem důvěryhodnější než report v tabulce, kterou lze snadno upravit. Parametry pochůzek lze nastavit zcela individuálně.

Kontrolní body jsou bezkontaktní. Kromě NFC čipů je možné použít i variantu s tzv. iBeacony, které lze načítat ze vzdálenosti několika metrů bez nutnosti vyndávat telefon z kapsy.

Formuláře slouží pro reporting nenadálých událostí. **Avšak očekávané události ať už standardní z výkonu služby nebo mimořádné události jsou předdefinované po dohodě se zákazníkem v roletce, kde si může bezpečnostní pracovník vybrat. Pak už jen doplní vlastní komentář.** Kromě fotky z místa incidentu, která obsahuje i GPS souřadnice místa, kde byla pořízena, **je možné napsat komentář bez omezení znaků, bez kontroly pravopisu,** popř. lze vybírat kategorii události v již zmíněné roletce, na základě, níž systém automaticky informuje pouze osoby odpovědné za konkrétní oblast, opět se nastavuje s klientem.

V rámci události může bezpečnostní pracovník přiložit nejen fotografii nebo video, ale **libovolnou přílohu, kterou např. obdržel emailem. Takovéto přílohy jsou kontrolovány antivirovým programem před odesláním do serveru.**

Docházka slouží k evidenci příchodů/odchodů všech pracovníků objektu. Pomocí funkce plánování směn lze automaticky monitorovat, že je na objektu přítomný požadovaný počet osob.

KPI neboli klíčové ukazatele výkonnosti slouží k automatickému vyhodnocování počtu událostí. Například počet pochůzek za den, počet chyb za měsíc, zahájení pochůzky v určitém časovém okně apod. Lze tak automatizovat činnosti, které bylo většinou třeba počítat ručně. **Jedná se o vytváření statistik zjištěných dat, na jejich základě je možné dělat nápravná opatření nebo sledovat efektivitu opatření.**

Záznam (deník) obsahuje veškeré události z objektu, které lze komentovat. Vznikne tak ucelená zpráva o dění na objektu a lze jím zcela nahradit papírovou provozní knihu.

Objednatel – zákazník nahlíží do portálu pomocí webového prohlížeče a má přehled nad všemi stavy snímačů, načtenými daty a provedenými záznamy. Může

následně data dále zpracovávat, filtrovat podle zvolených údajů jako je čas, místo, události vyhodnocovat a tisknout, nebo exportovat pro další zpracování.

Na vybrané stavy a skutečnosti je schopen portál reagovat aktivně (samostatně) odesláním e-mailu, nebo SMS a tím uživatele, nebo odpovědnou osobu ihned informovat. Tím se obchůzkový systém stává podstatným aktivním bezpečnostním prvkem jako například systémy PZTS nebo EPS. Současně podporuje bezpečnost pracovníků ostrahy, kteří mohou v případě nebezpečí využít PANIC tlačítko, nebo oboustrannou hlasovou komunikaci. Operátor pak může okamžitě reagovat na vzniklou situaci.

Rozmístění kontrolních bodů a obchůzkových tras s variantním řešením bude graficky znázorněno v Plánu kontrolní činnosti. Kontrolní body budou instalovány zejména v místech dislokace pracovišť se zvláštním režimem a na „rizikových místech“ (riziková místa jsou stanovena na základě „bezpečnostního posouzení“ objektu, resp. na základě doporučení objednatele).

2 Vybavení osob mobilním zařízením

Mobilním zařízením bude vybaven každý bezpečnostní pracovník a člen mobilní hlídky, který vykonává pochůzkovou a kontrolní činnost tak, aby byl zajištěn komplexní obraz činnosti bezpečnostních pracovníků ve službě.

3 Přístup do systému

Do systému, který obsahuje záznamy z průběhu směny mohou vstupovat:

zvolený zástupce zákazníka

- operátor dispečinku
- manažer systému CENTR GUARD
- provozní manažer a členové vedení CENTR GROUP

Do systému se vstupuje přes zabezpečené webové rozhraní nebo aplikaci v mobilním zařízení.

V systému je možné zapnout multifaktorové ověření, se zasláním kódu na jiný telefon nebo do emailu.

Editace záznamu není standartně možná, aby nedocházelo manipulaci dat. **Pomocí logované editace je ve výjimečných případech dovolená editace dat. O takovém kroku je proveden záznam. Tento krok je povolen pouze pro vybrané uživatele, kterým bylo uděleno oprávnění.**

Systém je možné u Objednatele dělit dle jednotlivých kritérií, nejmenším článkem je směna či bezpečnostní pracovník. Jinak je možné v systému vytvářet lokality podle osob, objektů, stanoviště apod.

Systém je vybaven zabezpečením serveru klienta. Data jsou šifrována.

Všechny záznamy jsou opatřené časovým razítkem času serveru, a to za bezpečnostních důvodů.

Objednatel má možnost v systému CENTR GUARD udělovat a spravovat skupinová oprávnění k dané zakázce v předem stanoveném rozsahu a v souladu s bezpečnostními normami pro přístup k informacím.

4 Záznam docházky

Evidence docházky je možná dokonce dvojím způsobem, a to buď prostřednictvím přihlášení se do systému pomocí osobních údajů (přihlašovací jméno a heslo) nebo přidělením osobních NFC čipu na pevném stanovišti ostrahy a jejich načtením na začátku a konci směny, případně přítomnosti.

Systémem CENTR GUARD budou vybaveni i oblastní manažeři a členové revize, aby mohli evidovat kontrolní činnost do systému vč. své přítomnosti na objektu. Tím bude zajištěn komplexní přehled zákazníka o dění na jednotlivých objektech.

5 Trasy a časy pochůzek

Trasy pochůzek mohou být nepravidelné nastavené automaticky nebo uživatelem (Objednatelem, pokud mu jsou přidělena práva), avšak vždy musejí mít řád z pohledu systému, který zároveň vyhodnocuje odchýlení se od plánu a on-line upozorňuje operátora, který je záložní/sekundární kontrolou nad dodržováním tras a časů. Odchylkou od trasy je považováno i nezahájení pochůzky, vynechání kontrolního bodu, nedodržení času či pořadí kontrolních bodů.

6 Vyhodnocování pochůzek

Přesto, že na systém v režimu 24/7 dohlíží operátor dispečinku, systém sám vyhodnocuje, zda byly všechny pochůzky vykonány, nebyl vynechán žádný kontrolní bod, body byly načteny ve správném pořadí. Případně je dispečer upozorněn, že pochůzka nebyla zahájena.

Zároveň v případě aktivace Tísňového tlačítka nebo poplachu při spuštění „polohy mrtvého muže“ reaguje na situaci a zajišťuje bezpečnostnímu pracovníkovi podporu.

7 Úkoly a pokyny při výkonu pochůzek

Po sepsání seznamu čipů a jejich zadání do systému má oprávněný uživatel možnost vytvořit libovolný počet pochůzek a jejich různých variant, u kterých můžete vpisovat speciální úkoly pro každý jednotlivý čip, GPS pozici každého bodu a minimální + maximální dobu pochůzky či přesunu mezi jednotlivými body. V plánování následně můžeme nastavit časy kdy má BP vyrazit na pochůzku – v tento čas je pochůzka automaticky započata a BP je upozorněn zvukovým signálem (není nutný startovní bod). K ukončení pochůzky dojde po načtení ukončovacího čipu, nebo po uplynutí stanovené doby, ale průběh pochůzky lze neustále sledovat on-line na portálu. Pochůzku lze i během jejího provádění on-line přeplánovat, přidat úkoly k bodům, nebo jen přidat povinnost BP v určeném čase něco vykonat.

Na základě nastavení práv při vstupu do systému přes webové rozhraní je možné, aby oprávněná osoba zasílala, měnila a aktualizovala úkoly na jednotlivých zařízeních, a to v reálném čase. Tato funkcionalita může být zpřístupněna i klientovi.

8 Tíseň

Na mobilním zařízení je možné naprogramovat tlačítko, které bude jako tíšňové. K tomuto tlačítku bude vytvořen systém reakce operátora na danou tíseň, a to v závislosti na lokalitě použití zařízení, avšak není výjimkou, že v případě tísně a následné verifikaci je na místo volána policie.

9 Záznam činností

CENTR GUARD ve spojení s mobilním zařízením dovoluje provádět záznam činnosti, mimořádných událostí, poškození majetku apod. Pak jen záleží na nastavení systému, přiřazení do kategorie, kdo má být o tomto typu události informován prostřednictvím notifikace formou SMS nebo e-mailu.

Při přístupu do systému je možné provést požadovaný export dat do několika možných formátů vč. vytvoření databáze v tabulkovém editoru.

Pro rychlý náhled systém umožňuje data filtrovat přímo v aplikaci nebo náhledu přes webové rozhraní, bez nutnosti exportu dat.

Export dat je možné provádět pouze na základě přiděleného oprávnění, které se bezpečnostním pracovníkům neuděluje.

Přístup k datům se opět nastavuje dle potřeb zákazníka. Bezpečnostním pracovníkům se standardně umožňuje přistupovat k datům ze své směny, aby mohli adekvátně reagovat na vzniklé situace. V případě využití formulářů evidence osob, evidence vozidel a modulu zapůjčení majetku se přístup k datům nastavuje na bez omezené času, což je možné opět změnit dle dohody se zákazníkem. K datům přistupují pomocí mobilního zařízení na svém stanovišti. Bezpečnostní pracovník nemá přístup k datům z jiného pracoviště, nemá možnost exportu dat, ani do systému přistupovat přes webové rozhraní.

10 Fotodokumentace

Mobilní zařízení je vybaveno fotoaparátem, a tak může být k jednotlivým událostem pořízena fotodokumentace, která se ukládá na serveru a je tedy kdykoliv k dispozici odkudkoliv.

11 Technické parametry mobilního zařízení

Mobilní zařízení určené pro výkon fyzické ostrahy a mobilních patrol je vybíráno z řad se zvýšenou odolností, který má krytí IP 68 a bezproblémový provoz je zajištěn v teplotním rozmezí -25 až 55 °C a vodotěsný, prachu, písku, blátu, sněhu, vysokým a nízkým teplotám a hrubé špíně odolný; výdrž až 60 min v hloubce 2 m, pád z výšky

1,8 m, což zajišťuje je vysokou odolnost proti vodě, prachu, pádu a hrubému zacházení, zajišťuje tím provozuschopnost i v náročných podmínkách.

12 Archivace dat při výpadku spojení

V případě, že dojde k ztrátě spojení se serverem, kde se ukládají všechna data, je zařízení nadále provozuschopné, je možné s ním vykonávat pochůzky i evidovat události. Jakmile je konektivita obnovena, jsou data odeslána na server.

Systém je tedy vybaven RTO a RPO po dobu výdrže baterie zařízení nebo naplnění vnitřní paměti zařízení. S ohledem na nízkou datovou náročnost záznamů je při dnešní datové kapacitě zařízení složité tyto funkcionality kvantifikovat. Rozhodně bez problému vydrží po celou směnu.

Systém CENTR GUARD si trvale hlídá konektivitu se serverem. **V případě výpadku konektivity hlídá bod obnovy, při opětovném navázání konektivity se vrací k bodu obnovy / místě výpadku a vše uložené v interní paměti zařízení odesílá na server.**

13 Podpora systému

Systém má technickou podporu v režimu 24/7, a to prostřednictvím operátora dispečinku CENTR GUARD, tedy v případě technických potíží se bezpečnostní pracovník může obrátit s žádostí o pomoc.

Další podporu zajišťuje manažer systému CENTR GUARD, který se podílí na vývoji systému, jeho údržbě, školení bezpečnostních pracovníků a klientů.

Dalším podporou systému je český dodavatel TTC Telsys, který je schopný vytvořit podporu na programátorské úrovni.

Na žádost Objednatele bude umožněn online přístup k logům v rámci „jeho zakázky“ vč. analýzy logů pro jejich snazší vyhodnocení.

14 Tok dat

Komunikace mezi zařízením a serverem je zajištěna pomocí šifrovaného toku dat prostřednictvím služeb operátora, zařízení lze také připojit pro zajištění konektivity pomocí wifi.

15 Závěr

CENTR GUARD je špičkový moderní systém, který je neustále vyvíjen. Jeho nespornou výhodou je, že se jedná o systém domácí (české firmy), a tak je možné s programátory diskutovat nad možnými vylepšeními a funkcemi na míru. Po zavedení systému se stalo standardem, že jsme připraveni jej upgradovat na přání zákazníka, tem může komunikovat nejen se zástupci klienta, ale jsme připraveni ke zprostředkování schůzky s programátorem. Ze zkušenosti víme, že se jedná o efektivní komunikaci a významné zkrácení času pro implementaci změn.