TVORÍME VEDOMOSTNÚ SPOLOČNOSŤ
Európsky fond regionálneho rozvoja

www.opis.gov.sk

Riadiaci orgán OPIS

www.nsrr.sk

MINISTERSTVO FINANCIÍ SLOVENSKEJ REPUBLIKY

Sprostredkovateľský orgán OPIS

www.informatizacia.sk

EURÓPSKA ÚNIA

www.europa.eu

Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky

www.minedu.sk

NÁRODNÝ PROJEKT: DIGITÁLNE UČIVO NA DOSAH

EDUcentrum:

BEZPEČNOSTNÝ PROJEKT PRE KAMEROVÝ SYSTÉM PRE PRIESTORY PRÍSTUPNÉ VEREJNOSTI

Operačný program informatizácia spoločnosti

Programové obdobie 2007 – 2013

Obsah

Prílohy

1. Úvod

Tento dokument predstavuje bezpečnostný projekt na ochranu osobných údajov podľa zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 84/2014 Z. z., ktorým sa mení a dopĺňa zákon č.122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a ktorým sa mení zákon Národnej rady Slovenskej republiky č. 145/1995 Z. z. o správnych poplatkoch v znení neskorších predpisov (ďalej len „ZOOÚ“). Bezpečnostný projekt sa týka osobných údajov spracúvaných v rámci monitorovania priestorov prístupných verejnosti kamerovým systémom v <doplniť názov, adresu a identifikačné údaje školy> (ďalej len „Škola“).

1.1. Základné pojmy

- **Dotknutou osobou** je každá fyzická osoba, ktorej osobné údaje sa spracúvajú.
- **Informačný systém** (ďalej aj ako „IS“) je akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií alebo súbor osobných údajov, ktorý je spracúvaný čiastočne alebo plne automatizovanými prostriedkami spracúvania.
- **Oprávnená osoba** je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie. Fyzická osoba sa stáva oprávnenou osobou dňom poučenia.
- **Osobnými údajmi** (ďalej aj ako „OÚ“) sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, ktorú možno priamo alebo nepriamo určiť na základe všeobecne použiteľného identifikátora (napr. rodné číslo), alebo ľubovoľnou kombináciou charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu (napr. kombinácia údajov meno, adresa, dátum narodenia, dosiahnuté vzdelanie, hmotnosť, majetkové pomery, atď.).
- **Prevádzkovateľ** je každý subjekt, ktorý určuje účel a podmienky spracúvania osobných údajov alebo koho na jeho plnenie ustanoví Zákon, právne záväzný akt Európskej únie alebo medzinárodná zmluva.
- **Spracúvanie osobných údajov** je vykonávanie akýchkoľvek operácií s osobnými údajmi, najmä ich získavanie, zhromažďovanie, poskytovanie, sprístupňovanie, zverejňovanie, cezhraničný prenos a likvidácia.
- **Sprostredkovateľ** je každý subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa v rozsahu a za podmienok dojednaných v písomnej zmluve podľa § 8 ods. 4 ZOOÚ.
- **Subdodávateľ sprostredkovateľa** je každý subjekt, ktorý spracúva osobné údaje a zabezpečuje ich ochranu na zodpovednosť sprostredkovateľa v rozsahu a za podmienok dojednaných v písomnej zmluve podľa § 8 ods. 5 ZOOÚ.
- **Zodpovednou osobou** je oprávnená osoba, písomne poverená výkonom dohľadu nad ochranou osobných údajov.

1.2. Účel spracúvania osobných údajov

Monitorovanie priestoru prístupného verejnosti je špecificky adresované v ZOOÚ a v Metodickom usmernení Úradu na ochranu osobných údajov SR č. 1/2014 (ďalej len „Usmernenie“).

Osobné údaje snímané kamerovým systémom sú podľa Usmernenia považované za osobitnú kategóriu osobných údajov.

Podľa § 15 ods. 7 ZOOÚ je možné monitorovať priestor prístupný verejnosti iba za účelom Ochrany verejného poriadku a bezpečnosti, odhaľovania kriminality, narušenia bezpečnosti štátu, ochrany majetku alebo zdravia.

Okruh dotknutých osôb tvoria osoby, ktoré sa vedia dostať do monitorovaných priestorov prístupných verejnosti v rámci školy - t.j. žiaci, učitelia, zamestnanci školy, návštevníci školy a pod. Vymedzenie účelu podľa § 15 ods. 7 ZOOÚ a jeho následná aplikácia je právnym základom a na takéto spracúvanie osobných údajov sa nevyžaduje súhlas dotknutých osôb.

1.3. Stručná špecifikácia informačného systému

Kamerový systém pre priestor prístupný verejnosti je doplnková služba (Bezpečnostné monitorovanie škôl) v rámci národného projektu „Digitálne učivo na dosah“ a eGOV služby „Prístup k digitálnym službám školy“. Súčasťou projektu „Digitálne učivo na dosah“ je vybudovanie vyhradenej infraštruktúry (pozostáva z vysokokapacitnej prístupovej siete a prislúchajúcich aktívnych sieťových zariadení, transportnej časti siete a zo zariadení pre zabezpečenie lokálnych prístupov v samotných školských zariadeniach), ktorá slúži na prenos kamerových záznamov z jednotlivých škôl a vybudovanie tzv. Centrálneho bodu, ktorého súčasťou je modul Centrálny manažment kamerových systémov a archivácia kamerových záznamov.

V rámci Školy sú umiestnené kamery, ktoré monitorujú priestor prístupný verejnosti (podrobnejšie informácie o počte a umiestnení kamier sú uvedené v prílohe č. 2 tohto dokumentu). Kamerové záznamy snímané kamerami sú okamžite automaticky prenášané prostredníctvom vyhradenej infraštruktúry a ukladané do dátového úložiska v rámci modulu Centrálny manažment kamerových systémov a archivácia kamerových záznamov. Po uplynutí Zákonom stanovenej lehoty 15 dní sú kamerové záznamy automaticky zlikvidované.

1.4. Prevádzkovateľ, sprostredkovateľ a subdodávateľ sprostredkovateľa

Z pohľadu ZOOÚ je prevádzkovateľom Kamerového systému pre priestory prístupné verejnosti Škola. Škola je povinná monitorovaný priestor zreteľne označiť. Škola je ďalej povinná viesť evidenciu (evidenčný list) o informačnom systéme osobných údajov, ktorý je Prílohou č. 1 tohto Bezpečnostného projektu.

Škola v súlade s §8 ZOOÚ zmluvne poverí spracúvaním osobných údajov sprostredkovateľa Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky (ďalej len „MŠVVaŠ SR“). MŠVVaŠ SR je vlastníkom centrálneho úložiska kamerových záznamov, pričom uchovávanie sa podľa ZOOÚ považuje za spracúvanie osobných údajov.

MŠVVaŠ SR ako sprostredkovateľ v súlade s §8 zmluvne poverí subdodávateľa Národnú agentúru pre sieťové a elektronické služby (ďalej ako „NASES“) zabezpečovaním administrácie kamerového systému, pričom NASES bude vykonávať operácie definované ako spracúvanie osobných údajov, napr. získavanie, zhromažďovanie, zaznamenávanie, usporadúvanie, vyhľadávanie, likvidácia, poskytovanie alebo sprístupňovanie. Osoby, ktoré v mene NASES vykonávajú uvedené operácie sú v postavení oprávnených osôb. Podľa Usmernenia, osoby, ktoré vykonávajú iba činnosti týkajúce sa funkčnosti kamerového systému, nemusia mať z pohľadu ZOOÚ postavenie oprávnených osôb. Vzťahuje sa však na nich povinnosť mlčanlivosti.

Likvidáciu kamerových záznamov po uplynutí zákonom stanovenej lehoty 15 kalendárnych dní odo dňa nasledujúceho po dni vytvorenia kamerového záznamu bude vykonávať subdodávateľ sprostredkovateľa - NASES.

V prípade trestného alebo priestupkového konania poskytne NASES súčinnosť príslušným orgánom činným v trestnom alebo priestupkovom konaní tým, že na základe ich žiadosti poskytne, respektíve sprístupní relevantné kamerové záznamy a zabezpečí ich uchovanie na nevyhnutnú dobu aj nad rámec 15 dní.

Sprostredkovateľ a subdodávateľ sprostredkovateľa zodpovedajú za implementáciu primeraných opatrení informačnej bezpečnosti, ktoré sa týkajú aktív v ich správe.

2. Bezpečnostný zámer

2.1. Základné bezpečnostné ciele

Základné ciele prevádzkovateľa v oblasti ochrany osobných údajov sú:

- Dôvernosť (Confidentiality) – zaistenie, že k údajom majú prístup len oprávnené osoby; ochrana pred neoprávneným prístupom, sprístupnením, poskytnutím alebo zverejnením.
- Integrita (Integrity) – zaistenie, že údaje nie sú pozmenené, respektíve nie sú pozmenené bez povšimnutia; ochrana pred poškodením a zmenou údajov.
- Dostupnosť (Availability) – zaistenie, že údaje sú k dispozícii oprávneným osobám, kedykoľvek to požadujú; ochrana pred zničením a stratou údajov; taktiež likvidácia údajov po splnení účelu spracúvania.
- Auditovateľnosť (Accountability) – zaistenie, že k udalostiam v informačnom systéme je možné jednoznačne priradiť entitu, ktorá ich vykonala.

2.2. Minimálne požadované bezpečnostné opatrenia

Aby prevádzkovateľ dosahoval primeranú ochranu osobných údajov v súlade s uvedenými cieľmi, aplikuje bezpečnostné opatrenia považované za „najlepšie praktiky“ („best practice“) v organizáciách obdobného typu:

- v súlade s požiadavkami Úradu a usmerneniami regulačných orgánov:
  - ZOOÚ,
  - vyhláška Úradu na ochranu OÚ č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení v znení vyhlášky č. 117/2014 Z. z. , ktorou sa mení a dopĺňa vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení (ďalej len "vyhláška č. 164/2013 Z. z."),
  - metodické usmernenia, záväzné stanoviská a odporúčania Úradu, a iné;
- požiadavkami a záväzkami vyplývajúcimi so zmluvných vzťahov;
- s prihliadnutím k relevantným bezpečnostných štandardom (napr. ISO/IEC 27001, ISO/IEC 27002).

2.3. Špecifikácia bezpečnostných opatrení

V súlade s vyhláškou č. 164/2013 Z. z. sú na zabezpečenie ochrany osobných údajov v informačnom systéme špecifikované opatrenia v nasledovných oblastiach:

2.3.1. Technické opatrenia

- Technické opatrenia realizované prostriedkami fyzickej povahy
- Ochrana pred neoprávneným prístupom
- Riadenie prístupu oprávnených osôb
- Ochrana proti škodlivému kódu
- Sieťová bezpečnosť
- Zálohovanie

- Likvidácia osobných údajov a dátových nosičov
- Aktualizácia operačného systému a programového aplikačného vybavenia

2.3.2. Organizačné opatrenia

- Vedenie zoznamu aktív a jeho aktualizácia
- Riadenie prístupu oprávnených osôb k osobným údajom
- Organizácia spracúvania osobných údajov
- Likvidácia osobných údajov
- Bezpečnostné incidenty
- Kontrolná činnosť

2.3.3. Personálne opatrenia

- Poučenie oprávnených osôb
- Oboznámenie oprávnených osôb s bezpečnostnými smernicami
- Vzdelávanie oprávnených osôb
- Postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby

Detailný popis bezpečnostných opatrení a spôsob ich uplatňovania v konkrétnych podmienkach je popísaný v kapitole 4.1.

2.4. Vymedzenie okolia informačného systému

Osobné údaje – kamerové záznamy sú spracúvané výlučne v elektronickej podobe. Kamerové záznamy sú vytvárané kamerami vo vlastníctve Školy umiestnenými vo verejne prístupných priestoroch školy (podrobnejšie údaje o umiestení jednotlivých kamier a snímanom priestore sú v prílohe č.2).

Kamerové záznamy sú po nasnímaní prenášané prostredníctvom vyhradenej infraštruktúry MŠVVaŠ SR a ukladané do dátového úložiska v rámci modulu Centrálny manažment kamerových systémov a archivácia kamerových záznamov. Modul Centrálny manažment kamerových systémov a archivácia kamerových záznamov je umiestnený v dátovom centre v Trnave, ktoré zabezpečuje NASES.

2.5. Vymedzenie hraníc určujúcich množinu zostatkových rizík

Hranica určujúca množinu zostatkových rizík je stanovená na základe Metodického usmernenia č. 15/2011 k vypracovaniu analýzy rizík informačnej bezpečnosti MŠVVaŠ SR (ďalej len "MU č. 15/2011"). Z celkovej škály rizík 0 až 8 sú ako tolerovateľné stanovené riziká na úrovni 4 a nižšie. Zostatkové riziká súvisia najmä:

- so zlyhaním ľudského faktora, ako aj
- s prejavmi „vyššej moci“.

3. Analýza bezpečnosti informačného systému

3.1. Identifikácia aktív

Na spracúvaní osobných údajov sa podieľajú nasledovné aktíva, nad ktorými je realizovaná analýza rizík:

Druh aktíva	Popis aktíva	Hodnota aktíva
Informačné aktíva	Kamerové záznamy	3
Softvérové aktíva	Modul Centrálny manažment kamerových systémov a archivácia kamerových záznamov	3
	Operačné systémy a firmware	3
Fyzické aktíva / Lokality	Kamery v škole	2
	Sieť - posledná míľa školy	2
	Kostrová sieť	3
	Sieť - posledná míľa Centrálneho bodu	3
	HW vybavenie (server) a dátové úložisko	3

3.2. Metodika analýzy rizík

Vykonanie analýza rizík metodicky vychádza z MU č. 15/2011.

Hodnota aktív je stanovená na základe popisu uvedeného v čl. 6 ods. 6 MU č. 15/2011.

Zoznam zraniteľností v závislosti od kategórie hrozby je uvedený v nasledovnej tabuľke:

Kategória hrozby	Hrozba	Zraniteľnosť
Fyzické poškodenie	Oheň	• citlivosť na vlhkosť • citlivosť na prašnosť • citlivosť na znečistenie • chýbajú záložné kópie (údajov, programového vybavenia)
	Poškodenie vodou	
	Znečistenie	
	Významná nehoda	
	Deštrukcia zariadenia alebo média	
	Prach, korózia, mráz	
Prírodné katastrofy	Klimatické javy	• umiestnenie v oblastiach ohrozených prírodnými javmi • citlivosť na výkyvy teplôt
	Seizmické javy	
	Meteorologické javy	
	Záplavy	

Kategória hrozby	Hrozba	Zraniteľnosť
Odmietnutie podporných služieb	Porucha klimatizácie alebo dodávky vody	• citlivosť na kolísanie napätia • nestabilná elektrická sieť • zlé prepojenie káblov • neadekvátna správa siete (routing) • nedostatočne bezpečná architektúra siete • nedostatočné/chýbajúce potvrdenie zaslania alebo prijatia správy
	Strata dodávok elektrickej energie	
	Porucha telekomunikačných zariadení	
Narušenie v dôsledku radiácie	Elektromagnetické žiarenie	• citlivosť na elektromagnetické žiarenie • citlivosť na výkyvy teplôt
	Tepelné vyžarovanie	
	Elektromagnetické výboje	
Kompromitácia / únik informácií	Odchytenie nežiaduceho elektromagnetického vyžarovania	• nechránený prenos citlivých správ • nechránené komunikačné linky • zanedbanie alebo nedostatočná úroveň fyzického riadenia prístupu do budovy alebo miestností • nedostatočná fyzická ochrana budov, dverí, okien • nechránené úložisko • nedostatočná starostlivosť pri vyraďovaní dokumentov • práca externých pracovníkov alebo upratovacieho personálu bez dohľadu; všeobecne známe vady programového vybavenia • nesprávne pridelenie prístupových práv • vyradenie alebo opätovné používanie pamäťových médií bez poriadneho vymazania údajov • povolená nepotrebná služba • nedostatočné alebo chýbajúce monitorovacie mechanizmy
	Špionáž	
	Odpočúvanie	
	Krádež médií / dokumentov	
	Krádež zariadení	
	Zneužitie nefunkčných / vyradených médií	
	Únik informácií	
	Použitie údajov z nedôveryhodného zdroja	
	Nedovolená manipulácia s hardvérom	
	Nedovolená manipulácia so softvérom	
	Určenie polohy	
Zlyhania technického charakteru	Poruchy / chyby zariadení	• žiadne alebo nedostatočné testovanie programového vybavenia • nedostatočná údržba alebo chybná inštalácia • nedokončený alebo nový softvér • single point of failure (úzke miesto alebo kritický prvok systému)
	Poškodenie zariadenia	
	Preťaženie informačného systému	
	Chyby softvéru	
	Porušenie udržiavateľnosti informačného systému	

Kategória hrozby	Hrozba	Zraniteľnosť
Neautorizovaná činnosť	Neautorizované použitie zariadení	• nerobí sa pravidelný audit (dohľad, kontrola) • chýba monitorovanie prostriedkov/zariadení na spracovanie informácie • nekontrolované sťahovanie a používanie softvéru • nedostatky v identifikácii odosielateľa a príjemcu
	Neautorizované kopírovanie softvéru	
	Použitie falošného / nelegálneho softvéru	
	Poškodenie údajov	
	Neautorizované spracúvanie údajov	
Narušenie funkčnosti	Chyba pri použití	• chýbajúce alebo nedostatočné mechanizmy pre identifikáciu a autentizáciu • nechránené tabuľky hesiel • slabý manažment hesiel (slabé heslá, ukladanie nešifrovaných hesiel, rovnaké heslá pre rozličné účely, nedostatočne časté menenie hesiel) • prenos hesiel v otvorenej forme • komplikované používateľské rozhranie
	Zneužitie oprávnení	
	Falšovanie oprávnení	
	Odmietnutie činností	
	Narušenie dostupnosti ľudských zdrojov	
Organizačné a personálne hrozby	Nedostatok zdrojov (finančných, ľudských, časových)	• nerobia sa pravidelné revízie manažmentu (systému) • nedostatočný bezpečnostný tréning • chýbajú procedúry upravujúce narábanie s informáciami, na ktoré sa vzťahuje ochrana duševného vlastníctva • nedostatočné bezpečnostné povedomie
	Organizačné problémy	
	Nedodržanie legislatívnych požiadaviek	
	Nedostatočná príprava zamestnancov	
	Nedodržanie požiadaviek bezpečnostných štandardov	
	Nejasná stratégia a koncepcia	
	Nedodržanie interných predpisov	
	Nespokojnosť zamestnancov	

Ohodnotenie hrozieb, ohodnotenie zraniteľností, ako aj rozhodovanie o riadení rizík bližšie špecifikuje MU č. 15/2011.

3.3. Výsledky analýzy rizík - súhrnná tabuľka

Služba - Bezpečnostné monitorovanie škôl		Ohodnotenie aktíva	Fyzické poškodenie			Prírodné katastrofy			Odmietnutie podporných služieb			Narušenie v dôsledku radiácie			Kompromitácia / únik informácií			Zlyhania technického charakteru			Neautorizovaná činnosť			Narušenie funkčnosti			Organizačné a personálne hrozby		
			Hrozba	Zraniteľnosť	Riziko	Hrozba	Zraniteľnosť	Riziko	Hrozba	Zraniteľnosť	Riziko	Hrozba	Zraniteľnosť	Riziko	Hrozba	Zraniteľnosť	Riziko	Hrozba	Zraniteľnosť	Riziko	Hrozba	Zraniteľnosť	Riziko	Hrozba	Zraniteľnosť	Riziko	Hrozba	Zraniteľnosť	Riziko
Informačné aktíva	Kamerové záznamy - verejný priestor	3			-			-			-			-	V	V	6			-			-	V	V	6			-
Softvérové aktíva	Modul Monitoring	3			-			-			-			-			-	S	V	5	S	S	4			-	S	S	4
	Operačné systémy a firmware	3			-			-			-			-			-	S	V	5	S	S	4			-	S	S	4
Fyzické aktíva/Lokality	Kamery v školách	2	N	V	3	N	V	3	S	V	4	N	S	2			-	S	V	4			-			-	S	N	2
	Sieť - posledná míľa školy	2	N	V	3	N	V	3	S	V	4	N	S	2			-	S	V	4			-			-	S	S	3
	Kostrová sieť	3	N	V	4	N	V	4	S	V	5	N	S	3			-	S	V	5			-			-	S	S	4
	Sieť - posledná míľa centrál. bodu	3	N	V	4	N	V	4	S	V	5	N	S	3			-	S	V	5			-			-	S	S	4
	Server a dátové úložisko kamer. systému	3	N	V	4	N	V	4	S	V	5	N	S	3			-	S	V	5			-			-	S	S	4

3.4. Výsledky analýzy rizík - zhrnutie

3.4.1. Ohodnotenie aktív

Takmer všetky identifikované aktíva boli v súlade s vyššie popísanou metodikou ohodnotené zo 4-stupňovej škály druhým najvyšším stupňom **„3“**, jedine fyzické aktíva Kamery v školách a Sieť - posledná míľa školy získali ohodnotenie nižšieho stupňa **„2“**.

3.4.2. Ohodnotenie hrozieb a zraniteľností

Hrozby a zraniteľnosti boli v súlade s vyššie citovanou metodikou ohodnotené na trojstupňovej škále so stupňami nízka, stredná a vysoká. Hrozby a zraniteľnosti boli ohodnotené pre tie typy aktív, kde existuje medzi hrozbou a aktívom relevantný vzťah. Napríklad hrozba Fyzické poškodenie je ohodnotená iba v súvislosti s Fyzickými aktívami/Lokalitami, alebo hrozba Kompromitácia/únik informácií je ohodnotená iba v súvislosti s Informačnými aktívami. Kompletné výsledky ohodnotenia hrozieb a zraniteľností sa nachádzajú vo vyššie uvedenej súhrnnej tabuľke.

3.4.3. Ohodnotenie a ošetrenie rizík

Na základe ohodnotenia aktív, hrozieb a zraniteľností a podľa matice výpočtu rizík vo vyššie citovanej metodike bola vypočítaná úroveň individuálnych rizík. Z vyššie uvedenej súhrnnej tabuľky vyplýva, že celkovo bolo identifikovaných 38 individuálnych rizík s úrovňami od 2 do 6 (podľa dosiahnutej hodnoty sú tieto riziká v tabuľke odlíšené taktiež farebne), pričom každé riziko predstavuje jedinečnú kombináciu aktíva, hrozby a zraniteľnosti.

Identifikované riziká sú tzv. inherentné riziká, t.j. predstavujú potenciál realizácie negatívneho dopadu pri výskyte hrozby a využití zraniteľnosť aktíva, pričom nie sú zohľadnené žiadne zavedené bezpečnostné opatrenia.

Zavádzaním vhodných bezpečnostných opatrení sa úroveň inherentných rizík znižuje. Po zohľadnení zavedených opatrení hovoríme o tzv. reziduálnych alebo zostatkových rizikách.

Spôsoby ošetrenia rizík s najvyššou úrovňou 6 a 5 sú uvedené v nasledovnej tabuľke:

Kategória hrozby	**Aktívum**	**Úroveň rizika**	**Spôsob ošetrenia rizika**	**Návrh opatrení**
Kompromitácia / únik informácií	*Informačné* Kamerové záznamy - verejný priestor	6	Aplikovanie bezpečnostných opatrení	Šifrová ochrana kamerového záznamu; Ochrana pred neoprávneným prístupom; Riadenie prístupu
Narušenie funkčnosti		6	Prenesenie na tretie strany	Ochrana pred neoprávneným prístupom; Riadenie prístupu
Zlyhania technického charakteru	*Softvérové* Modul Monitoring	5	Prenesenie na tretie strany	Riadenie incidentov; Zálohovanie
	Softvérové Operačné systémy a firmware	5	Prenesenie na tretie strany	Riadenie incidentov; Zálohovanie
Odmietnutie podporných služieb	*Fyzické* Kostrová sieť; Sieť - posledná míľa centrálneho bodu; Server a dátové úložisko kamerového systému	5	Prenesenie na tretie strany	Riadenie incidentov; Sieťová bezpečnosť

Kategória hrozby	Aktívum	Úroveň rizika	Spôsob ošetrenia rizika	Návrh opatrení
Zlyhania technického charakteru	*Fyzické* Kostrová sieť; Sieť - posledná míľa centrálneho bodu; Server a dátové úložisko kamerového systému	5	Prenesenie na tretie strany	Riadenie incidentov; Sieťová bezpečnosť

4. Závery vyplývajúce z bezpečnostného zámeru a z analýzy bezpečnosti informačného systému

4.1. Popis bezpečnostných opatrení

Popis bezpečnostných opatrení a spôsob ich uplatňovania v konkrétnych podmienkach.

4.1.1. Technické opatrenia

Technické opatrenia realizované prostriedkami fyzickej povahy

- Subdodávateľ sprostredkovateľa zabezpečuje vhodné mechanické zábranné prostriedky a technické zabezpečovacie prostriedky pre serverovňu, v ktorej je umiestnený modul Centrálny manažment kamerových systémov a archivácia kamerových záznamov.
- Subdodávateľ sprostredkovateľa zabezpečuje oddelenie serverovne, v ktorej je umiestnený modul Centrálny manažment kamerových systémov a archivácia kamerových záznamov pomocou stien od ostatných častí objektu.
- Prevádzkovateľ zabezpečuje, že kamery sú umiestnené v dostatočnej výške tak, aby neboli bežne dosiahnuteľné. Prevádzkovateľ zabezpečuje, že kamery sú v prevedení Vandal Resistant (odolné voči vandalizmu). Prevádzkovateľ ďalej zabezpečuje, že každá kamera je primerane vybavená priestoru v ktorom sa nachádza - externé kamery majú ochranu proti nepriaznivým poveternostným podmienkam a pod.
- Subdodávateľ sprostredkovateľa zabezpečuje, že zobrazovacie jednotky, ktoré používajú oprávnené osoby sú umiestnené tak, aby zamedzovali náhodnému odpozeraniu osobných údajov.

Ochrana pred neoprávneným prístupom

- Subdodávateľ sprostredkovateľa zabezpečuje, že kamerové záznamy premiestňované prostredníctvom počítačových sietí a ukladané v rámci modulu Centrálny manažment kamerových systémov a archivácia kamerových záznamov sú šifrované.

Riadenie prístupu oprávnených osôb

- Subdodávateľ sprostredkovateľa zabezpečuje, že oprávnené osoby sú pri prihlasovaní do informačného systému identifikované a autentifikované pomocou prihlasovacieho mena a hesla a zároveň pomocou eID karty voči modulu riadenia prístupov ústredného portálu verejnej správy.
- Subdodávateľ sprostredkovateľa zabezpečuje, že každé prihlásenie oprávnenej osoby do informačného systému je zaznamenávané v auditnom logu modulu Centrálny manažment kamerových systémov a archivácia kamerových záznamov.

Ochrana proti škodlivému kódu

- Subdodávateľ sprostredkovateľa zabezpečuje na pracovných staniciach oprávnených osôb detekciu prítomnosti škodlivého kódu v prichádzajúcej elektronickej pošte a v súboroch.
- Subdodávateľ sprostredkovateľa zabezpečuje na pracovných staniciach oprávnených osôb ochranu pred nevyžiadanou elektronickou poštou.
- Subdodávateľ sprostredkovateľa zabezpečuje v rámci informačného systému používanie iba legálneho a schváleného softvéru.

- Subdodávateľ sprostredkovateľa definuje v rámci informačného systému pravidlá sťahovania súborov z verejne prístupnej počítačovej siete.

Sieťová bezpečnosť

- Subdodávateľ sprostredkovateľa zabezpečuje kontrolu, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou pomocou firewallu.
- Subdodávateľ sprostredkovateľa zabezpečuje evidenciu všetkých miest prepojenia sietí vrátane verejne prístupnej počítačovej siete.
- Subdodávateľ sprostredkovateľa zabezpečuje ochrana vonkajšieho a vnútorného prostredia informačného systému prostredníctvom firewallu.
- Subdodávateľ sprostredkovateľa definuje pre pracovné stanice oprávnených osôb pravidlá prístupu do verejne prístupnej počítačovej siete.
- Subdodávateľ sprostredkovateľa zabezpečuje ochranu proti hrozbám pochádzajúcim z verejne prístupnej počítačovej siete.

Zálohovanie

- Subdodávateľ sprostredkovateľa pravidelne vykonáva test funkcionality dátového nosiča zálohy.
- Subdodávateľ sprostredkovateľa zabezpečuje vytváranie záloh kamerových záznamov s vopred zvolenou periodicitou.
- Subdodávateľ sprostredkovateľa pravidelne vykonáva test obnovy údajov zo zálohy.
- Subdodávateľ sprostredkovateľa zabezpečuje ukladanie záloh bezpečným spôsobom na inom geografickom oddelenom mieste.

Likvidácia osobných údajov a dátových nosičov

- Subdodávateľ sprostredkovateľa zabezpečuje automatické vymazanie kamerových záznamov po uplynutí zákonom stanovenej lehoty. V prípade použitia kamerového záznamu v rámci trestného alebo priestupkového konania zabezpečuje subdodávateľ sprostredkovateľa vymazanie príslušného záznamu až po splnení účelu.

Aktualizácia operačného systému a programového aplikačného vybavenia

- Subdodávateľ sprostredkovateľa zabezpečuje pravidelnú aktualizáciu (aplikáciu bezpečnostných záplat) operačného systému a programového aplikačného vybavenia modulu Centrálny manažment kamerových systémov a archivácia kamerových záznamov a pracovných staníc oprávnených osôb v zmysle .

4.1.2. Organizačné opatrenia

Personálne opatrenia

- Subdodávateľ sprostredkovateľa zabezpečuje poučenie oprávnených osôb pred uskutočnením prvej spracovateľskej operácie s osobnými údajmi.
- Subdodávateľ sprostredkovateľa zabezpečuje poučenie oprávnených osôb o postupoch spojených s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach.
- Subdodávateľ sprostredkovateľa zabezpečuje oboznámenie oprávnených osôb s bezpečnostnými smernicami.

- Subdodávateľ sprostredkovateľa zabezpečuje vzdelávanie oprávnených osôb.
- Subdodávateľ sprostredkovateľa zabezpečuje definuje a uplatňuje postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby (napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti)

Vedenie zoznamu aktív a jeho aktualizácia

- Prevádzkovateľ zabezpečuje vedenie a aktualizáciu zoznamu kamier v prílohe č.2 tohto dokumentu.
- Subdodávateľ sprostredkovateľa zabezpečuje vedenie a aktualizáciu zoznamu aktív, ktoré spravuje a ktoré sa podieľajú na spracovaní osobných údajov.

Riadenie prístupu oprávnených osôb k osobným údajom

- Subdodávateľ sprostredkovateľa zabezpečuje kontrola vstupu do objektu a do serverovne, v ktorej sa nachádza modul Centrálny manažment kamerových systémov a archivácia kamerových záznamov.
- Subdodávateľ sprostredkovateľa zabezpečuje správu kľúčov (individuálne prideľovanie kľúčov, bezpečné uloženie rezervných kľúčov) v rámci objektu, v ktorom sa nachádza modul Centrálny manažment kamerových systémov a archivácia kamerových záznamov.
- Subdodávateľ sprostredkovateľa zabezpečuje prideľovanie prístupových práv a úrovní prístupu (rolí) oprávnených osôb do modulu Centrálny manažment kamerových systémov a archivácia kamerových záznamov.
- Subdodávateľ sprostredkovateľa zabezpečuje správu hesiel v rámci modulu Centrálny manažment kamerových systémov a archivácia kamerových záznamov.
- Subdodávateľ sprostredkovateľa zabezpečuje vzájomné zastupovanie oprávnených osôb (napr. v prípade nehody, dočasnej pracovnej neschopnosti, ukončenia pracovného alebo obdobného pomeru).

Organizácia spracúvania osobných údajov

- Subdodávateľ sprostredkovateľa zabezpečuje nepretržitá prítomnosť oprávnenej osoby v serverovni, v ktorej je umiestnený modul Centrálny manažment kamerových systémov a archivácia kamerových záznamov, ak sa v nej nachádzajú aj iné ako oprávnené osoby.
- Subdodávateľ sprostredkovateľa zabezpečuje režim údržby a upratovania v serverovni, v ktorej je umiestnený modul Centrálny manažment kamerových systémov a archivácia kamerových záznamov.

Likvidácia osobných údajov

- Subdodávateľ sprostredkovateľa určuje postupy likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých oprávnených osôb a zabezpečuje ich aplikáciu v prípade zlyhania automatického vymazania kamerových záznamov.
- Subdodávateľ sprostredkovateľa určuje postupy pre bezpečnú likvidáciu dátových nosičov po skončení ich používania s vymedzením súvisiacej zodpovednosti jednotlivých oprávnených osôb (bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov).

Bezpečnostné incidenty

- Sprostredkovateľ prevádzkuje pre účely riadenia bezpečnostných incidentov call centrum.

- Prevádzkovateľ a subdodávateľ sprostredkovateľa nahlasujú bezpečnostné incidenty a zistené zraniteľné miesta informačného systému na call centrum sprostredkovateľa."
- Call centrum sprostredkovateľa zabezpečuje evidenciu bezpečnostných incidentov a použitých riešení.
- Call centrum sprostredkovateľa zabezpečuje v spolupráci so subdodávateľom sprostredkovateľa riešenie bezpečnostných incidentov a použitých riešení.

Kontrolná činnosť

- Subdodávateľ sprostredkovateľa zabezpečuje kontrolnú činnosť zameranú na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie (napr. pravidelné kontroly prístupov k informačnému systému).
- Subdodávateľ sprostredkovateľa informuje oprávnené osoby o kontrolnom mechanizme, ak je u subdodávateľa sprostredkovateľa zavedený (rozsah kontroly a spôsoby jej uskutočňovania).

4.2. Rozsah oprávnení, popis povolených činností a spôsob identifikácie a autentizácie

Princíp oddelenia povinností

Roly a zodpovednosti pri spracúvaní OÚ musia byť definované spôsobom, aby žiadna osoba nemala jedinečnú kontrolu nad kľúčovými aspektmi spracúvania.

Prístup k informačnému systému

Prístup k spracúvaniu údajov pomocou informačného systému sa riadi princípom minimálnych potrebných oprávnení, t.j. pre udelenie prístupu k aktívam je potrebný oprávnený dôvod, pričom každá žiadosť o prístup je posudzovaná jednotlivo s dodržaním princípu oddelenia povinností.

Oprávnené osoby sú pri prihlasovaní do informačného systému identifikované a autentifikované pomocou jedinečného prihlasovacieho mena a hesla a zároveň pomocou eID karty voči modulu riadenia prístupov ústredného portálu verejnej správy.

Oprávnené osoby môžu vykonávať získavanie, zhromažďovanie, zaznamenávanie, usporadúvanie, vyhľadávanie, likvidáciu, poskytovanie a sprístupňovanie osobných údajov. Na vykonávanie týchto činností majú pridelené primerané oprávnenia v súlade s princípom oddelenia povinností a princípom minimálnych potrebných oprávnení.

4.3. Výkon kontrolných činností

Kontrolné činnosti zamerané na dodržiavanie bezpečnostných opatrení implementovaných sprostredkovateľom a subdodávateľom sprostredkovateľa vykonávajú v súlade s smernicou MŠVVaŠ SR č. 40/2013 o ochrane osobných údajov zodpovedné osoby MŠVVaŠ SR. Interný audit je v pravidelných dvojročných cykloch zabezpečovaný prostredníctvom odboru vnútorného auditu MŠVVaŠ SR. Plnenie povinností zodpovedných osôb MŠVVaŠ SR kontroluje manažér informačnej bezpečnosti MŠVVaŠ SR. Manažér informačnej bezpečnosti MŠVVaŠ SR v spolupráci s jednotlivými zodpovednými osobami MŠVVaŠ SR vypracováva jedenkrát ročne správu o kontrolnej činnosti v oblasti ochrany osobných údajov. Správu predkladá bezpečnostnému výboru MŠVVaŠ SR.

4.4. Postupy pri haváriách, poruchách a iných mimoriadnych udalostiach

Havárie, poruchy alebo mimoriadne udalosti týkajúcim sa spracovania OÚ sú udalosti, pri ktorých dochádza k ohrozeniu štandardného a autorizovaného spôsobu spracúvania OÚ, respektíve narušeniu dostupnosti, dôvernosti alebo integrity OÚ.

Pri haváriách, poruchách alebo mimoriadnych udalostiach týkajúcich sa spracovania OÚ sa aplikuje postup riadenia bezpečnostných incidentov. Sprostredkovateľ prevádzkuje pre účely riadenia bezpečnostných incidentov call centrum. Prevádzkovateľ a subdodávateľ sprostredkovateľa nahlasujú bezpečnostné incidenty na call centrum sprostredkovateľa. Call centrum sprostredkovateľa zabezpečuje evidenciu bezpečnostných incidentov a použitých riešení. Call centrum sprostredkovateľa zabezpečuje v spolupráci so subdodávateľom sprostredkovateľa riešenie bezpečnostných incidentov a použitých riešení.

Príloha č. 1

EVIDENCIA INFORMAČNÉHO SYSTÉMU OSOBNÝCH ÚDAJOV

podľa § 43 ods. 1 ZOOÚ

I. NÁZOV INFORMAČNÉHO SYSTÉMU OSOBNÝCH ÚDAJOV
Kamerový systém pre priestory prístupné verejnosti

II. ÚDAJE O PREVÁDZKOVATEĽOVI	
Názov prevádzkovateľa	
Identifikačné číslo organizácie (IČO)	
Obec a PSČ	
Ulica a číslo	
Štát	
Právna forma	
Štatutárny orgán prevádzkovateľa (alebo osoba oprávnená konať v jeho mene)	
Zástupca prevádzkovateľa ak bol vymenovaný a jeho IČO, sídlo a štatutárny orgán	
Počet oprávnených osôb	Prevádzkovateľ nemá oprávnené osoby

III. ÚDAJE O INFORMAČNOM SYSTÉME OSOBNÝCH ÚDAJOV	
Účel spracúvania osobných údajov	Ochrana verejného poriadku a bezpečnosti, odhaľovanie kriminality, ochrana majetku alebo zdravia.
Právny základ spracúvania osobných údajov	§ 15 ods. 7 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 84/2014 Z. z., ktorým sa mení a dopĺňa zákon č.122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a ktorým sa mení zákon Národnej rady Slovenskej republiky č. 145/1995 Z. z. o správnych poplatkoch v znení neskorších predpisov (ďalej len "ZOOÚ“)
Okruh dotknutých osôb	Osoby, ktoré sa vedia dostať do monitorovaných priestorov prístupných verejnosti v rámci školy - t.j. žiaci, učitelia, zamestnanci školy, návštevníci školy a pod.

Zoznam osobných údajov (alebo rozsah)	Kamerový záznam dotknutých osôb - tvár a celá postava.
Označenie bezpečnostných opatrení	Bezpečnostný projekt

IV. SPRACOVATEĽSKÉ OPERÁCIE S OSOBNÝMI ÚDAJMI	
Poskytovanie osobných údajov	
Tretie strany (prípadne okruh tretích strán)	Právny základ
Orgány činné v trestnom alebo priestupkovom konaní	§ 15 ods. 7 ZOOÚ
Sprístupňovanie osobných údajov	
Okruh príjemcov	Právny základ
Orgány činné v trestnom alebo priestupkovom konaní	§ 15 ods. 7 ZOOÚ
Zverejňovanie osobných údajov	
Spôsob zverejnenia	Právny základ
Údaje sa nezverejňujú	
Cezhraničný prenos osobných údajov	
Tretia krajina	Právny základ
Z informačného systému sa neuskutočňuje prenos do tretích krajín	

V. ZAČIATOK SPRACÚVANIA OSOBNÝCH ÚDAJOV

.....

Odtlačok pečiatky prevádzkovateľa

.....

Dátum, meno a podpis štatutárneho orgánu prevádzkovateľa

Príloha č. 2

Špecifikácia umiestnenia bezpečnostných kamier a snímaných priestorov

Por. č.	Špecifikácia umiestnenia bezpečnostnej kamery	Špecifikácia snímaného priestoru
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		