Obec Bušince, Obecný úrad Bušince so sídlom Železničná 4/320, 991 22 Bušince

Pravidlá technických a organizačných opatrení o ochrane osobných údajov, zásadách bezpečnosti pri prevádzke informačných a komunikačných technológií informačného systému – IS KAMEROVÝ SYSTÉM

Čl. 1
Všeobecné ustanovenia

1. Tieto **Pravidlá technických a organizačných opatrení /PTOO/** upravuje základné pravidlá pre ochranu osobných údajov v elektronickej forme a pre zaistenie bezpečnej a spoľahlivej prevádzky informačných a komunikačných technológií informačného systému prevádzkovateľa (ďalej len "IS").

2. Prevádzku informačných a komunikačných technológií IS zabezpečujú oprávnené osoby podľa záznamu spracovateľských činnosti IS. KAMEROVÝ IS

VYMEDZENIE ZÁKLADNÝCH POJMOV

- **Osobné údaje (OÚ)** - údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.

- **Oprávnená osoba** - každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie, a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným v poučení podľa § 21.

- **Zodpovedná osoba** - osoba poverená výkonom dohľadu, ktorú prevádzkovateľ informačného systému písomne poveril dozerať na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov.

- **Dotknutá osoba** - každá fyzická osoba, ktorej sa osobné údaje týkajú.

- **Servisný technik** - fyzická osoba poverená vykonávateľom kontrolnej činnosti a pozáručného servisu, vykonávaní pravidelnej odbornej prehliadky, funkčných skúšok systému a pozáručného servisu.

- **Výmaz osobných údajov** - výmaz osobných údajov sa rozumie automatické odstraňovanie digitalizovaných dát ukladaných kamerovým systémom na internom záznamovom médiu, súčasťou ktorých sú aj osobné údaje bez zásahu oprávnenej osoby. Výmaz osobných údajov získaných činnosťou kamerového systému je zabezpečená automaticky, programovanou činnosťou systému, lehota likvidácie získaných údajov je 15 kalendárnych dní od ich zaznamenania. Výmazom sa rozumie nenávratná likvidácia osobných údajov, bez možnosti ich obnovenia akýmkoľvek spôsobom.

7. **Archivácia osobných údajov** - archiváciou osobných údajov sa rozumie kopírovanie digitálnych dát ukladaných kamerovým systémom na internom záznamového média na externé záznamové médium. Osobné údaje získané z kamerového systému, u ktorých je pôvodný predpoklad, že budú použité ako dôkazy v priestupkovom, správnom, prípadne trestnom konaní sa v digitalizovanej podobe archivujú na externom médiu - nosiči. Externý nosič musí byť označený príslušnou registratúrou resp. spisovou značkou udalosti alebo konania, v rámci, ktorého bol dôkaz produkovaný, menom, priezviskom a funkciou oprávnenej osoby, ktorá archiváciu vykonala, menom, priezviskom a funkciou osoby ktorá konanie vedie. Vykonanie archivácie osobného údaja na externom nosiči musí byť zapísané v protokole archivovaných záznamov kamerového systému v nasledovnom rozsahu: registratúra značka konania, právna

kvalifikácia skutku, dátum a čas archivácie, oprávnená osoba, ktorá archiváciu vykonala, dátum a doba trvania časového rozsahu archivovaného záznamu, číslo kamery, z ktorej bol záznam vyhotovený.

Čl. 2
Ochrana osobných údajov

1. Osobnými údajmi sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, teda údaje, z ktorých možno identifikovať osobu, ktorej sa týkajú. Oprávnená osoba prichádzajú do styku s osobnými údajmi v elektronickej forme spracúvanými v podmienkach prevádzkovateľa a sú teda povinní zabezpečiť náležitú ochranu spracúvaných osobných údajov.

2. Pod ochranou osobných údajov sa rozumie splnenie požiadaviek, ktoré stanovuje zákon č. 18/2018 Z.z. o ochrane osobných údajov, predovšetkým obmedzenie prístupu k zhromaždeným a spracúvaným osobným údajom len na osoby, ktoré prístup k týmto údajom oprávnenie a boli náležite poučení.

3. Oprávnené osoby sú povinné zachovávať mlčanlivosť o osobných údajoch, s ktorými prišli do styku. Povinnosť mlčanlivosti trvá aj po zániku ich funkcie .

4. Oprávnené osoby sú zodpovedné za také nastavenie prostriedkov informačných a komunikačných technológií, používaných na spracúvanie, ukladanie, alebo prenos osobných údajov v elektronickej forme ktoré zabezpečí, aby prístup k osobným údajom bol podmienený úspešnou identifikáciou a autentifikáciou oprávneného používateľa IS (zadanie správnej kombinácie mena a prístupového hesla oprávneného používateľa). Taktiež umožnia používateľom využívať na pracovných staniciach používaných pre prácu s osobnými údajmi šetrič obrazovky s heslom na ochranu prístupu do pracovnej stanice prihlásenej do systému počas krátkodobej neprítomnosti používateľa..

5. Prístupové práva pre prácu osobnými údajmi musia byť nastavené v súlade s bezpečnostným “princípom najmenších privilégií”. Za prideľovanie a prípadnú zmenu prístupových práv používateľom podľa tohto princípu zodpovedá správca systému. Za včasné informovanie správcu systému o zmenách s dopadom na prístupové práva oprávnenej osoby.

6. V záujme zabránenia prístupu neoprávnených osôb k starším kópiám osobných údajov zabezpečia zodpovedné osoby spoľahlivú likvidáciu (vymazanie) údajov zo všetkých pamäťových médií, ktoré obsahovali osobné údaje a ktoré sa vyraďujú, resp. preraďujú na iné využitie ako na spracovanie (uloženie) osobných údajov. V prípade samostatných médií u ktorých sa nepredpokladá opakované použitie, zabezpečia spoľahlivú likvidáciu médií spolu s údajmi na nich uloženými. Zariadenie na ktorom sa ukladajú zozbierané OÚ je servisnou firmou nastavené na automatický výmaz po 15 dňoch.

7. Umiestnenie, vybavenie a vyhodnocovanie získaných dát IS- Kamerový systém.

TECHNICKÉ OPATRENIA

- 1. Kamerový záznam v kvalite umožňujúcej rozlíšenie osoby má výstup na monitor nachádzajúci sa v kancelárii starostu obce. Záznam je možné sledovať na monitore pri NVR, ktoré sú uzamknuté v kancelárii starostu obce. Prenos dát s osobnými údajmi sa neuskutočňuje. Údaje sa zobrazia len na monitore pri NVR po zadaní mena a hesla. Správu hesiel zabezpečuje prevádzkovateľ – starosta obce.

- 2. Nahrávacie zariadenie NVR sa nachádza v budove s prevádzkovou miestnosťou uvedenej v bode 1. Záznam je možné zobrazovať 24 hodín. Video prenos sa nerealizuje.

-3. Kópiu záznamu je možné vyhotoviť z tohto zariadenia len po zadaní prihlasovacích údajov oprávnenej osoby, ktorá musí byť náležite poučená a preškolená. Kópiu záznamu možno vyhotoviť, len za účelom šetrenia podozrenia zo spáchania trestného činu, priestupku, alebo iného protiprávneho konania . Záznam škodovej udalosti alebo poškodenia zdravia osôb nachádzajúcich sa v monitorovacom priestore.

Kamerový systém zaznamenáva videokamerou verejné priestranstvo pred obecným úradom a čiastočne zaberá rodinné domy v okolí OÚ Bušince.

- 1 kamera sa nachádza na stĺpe pri chodníku pred budovou obecného úradu ktorá monitoruje parkovisko,

časť parku a vchod do budovy obecného úradu

- 2 kamery sa nachádzajú v zadnom dvore, ktoré monitorujú vchod zadnou bránou, časť ulice Železničná a celý areál v zadnom dvore

Monitorovaný priestor sa na viacerých miestach zreteľne označí nápisom „Priestor je monitorovaný kamerovým systémom" alebo piktogramom kamery, s popisom o prevádzkovateľovi kamerového systému a kontaktom na prevádzkovateľa.

Čl.3
Analýza bezpečnosti osobných údajov v informačných systémoch , analýza rizík

Pre poznanie informačného systému je nevyhnutné vykonať podrobnú analýzu rizík na ochranu osobných údajov. Vzhľadom na posúdenie bezpečnosti IS ako aj vypracovania PTOO bolo nevyhnutné vykonať podrobnú rizikovú analýzu IS. V rámci analýzy IS bola vykonaná analýza rozsahu IS ako aj riziková analýza aktív IS a činnosť pri spracovateľských operáciách. Analýza ,výsledky a jej vyhodnotenie je uvedené v PTOO, ktoré rieši všetky možné ohrozenia s ich vyhodnotením.

3.1. Poskytované informácie, ak osobné údaje sú získané od dotknutej osoby

(1) Ak sa od dotknutej osoby získavajú osobné údaje, ktoré sa jej týkajú, je prevádzkovateľ povinný poskytnúť dotknutej osobe pri ich získavaní

a) identifikačné údaje a kontaktné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený,

b) kontaktné údaje zodpovednej osoby,

c) účel spracúvania osobných údajov, na ktorý sú osobné údaje určené, ako aj právny základ spracúvania osobných údajov,

d) oprávnené záujmy prevádzkovateľa alebo tretej strany, ak sa osobné údaje spracúvajú podľa § 13 ods. 1 písm. f),

e) identifikáciu príjemcu alebo kategóriu príjemcu, ak existuje,

f) informáciu o tom, že prevádzkovateľ zamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii, identifikáciu tretej krajiny alebo medzinárodnej organizácie, informáciu o existencii alebo neexistencii rozhodnutia Európskej komisie (ďalej len „Komisia“) o primeranosti alebo odkaz na primerané záruky alebo vhodné záruky a prostriedky na získanie ich kópie alebo informáciu o tom, kde boli sprístupnené, ak prevádzkovateľ zamýšľa prenos podľa § 48 ods. 2, § 49 alebo § 51 ods. 1 a 2.

(2) Okrem informácií podľa odseku 1 prevádzkovateľ pri získavaní osobných údajov poskytne dotknutej osobe informácie o

a) dobe uchovávania osobných údajov; ak to nie je možné, informácie o kritériách jej určenia,

b) práve požadovať od prevádzkovateľa prístup k osobným údajom týkajúcich sa dotknutej osoby, o práve na opravu osobných údajov, o práve na vymazanie osobných údajov alebo o práve na obmedzenie spracúvania osobných údajov, o práve namietať spracúvanie osobných údajov, ako aj o práve na prenosnosť osobných údajov,

c) práve kedykoľvek svoj súhlas odvolať,

d) práve podať návrh na začatie konania podľa § 100,

e) tom, či je poskytovanie osobných údajov zákonnou požiadavkou alebo zmluvnou požiadavkou alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, a o tom, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj o možných následkoch neposkytnutia osobných údajov,

f) existencii automatizovaného individuálneho rozhodovania vrátane profilovania podľa § 28 ods. 1 a 4; v týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie o použitom postupe, ako aj o význame a predpokladaných dôsledkoch takého spracúvania osobných údajov pre dotknutú osobu.

(3) Prevádzkovateľ poskytne dotknutej osobe pred ďalším spracúvaním osobných údajov informácie o inom účele a ďalšie relevantné informácie podľa odseku 2, ak má prevádzkovateľ v úmysle ďalej spracúvať osobné údaje na iný účel ako ten, na ktorý boli získané.

3.2. Poskytované informácie, ak osobné údaje nie sú získané od dotknutej osoby

(1) Ak osobné údaje neboli získané od dotknutej osoby, prevádzkovateľ dotknutej osobe poskytne,

a) identifikačné údaje a kontaktné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený,

b) kontaktné údaje zodpovednej osoby,

c) účel spracúvania osobných údajov, na ktorý sú osobné údaje určené, ako aj právny základ spracúvania osobných údajov,

d) kategórie spracúvaných osobných údajov,

e) identifikáciu príjemcu alebo kategóriu príjemcu, ak existuje,

f) informáciu o tom, že prevádzkovateľ zamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii, identifikáciu tretej krajiny alebo medzinárodnej organizácie, informáciu o existencii alebo neexistencii rozhodnutia Komisie o primeranosti alebo odkaz na primerané záruky alebo vhodné záruky a prostriedky na získanie ich kópie alebo informáciu o tom, kde boli sprístupnené, ak prevádzkovateľ zamýšľa prenos podľa § 48 ods. 2, § 49 alebo
§ 51 ods. 1 a 2.

(2) Okrem informácií podľa odseku 1 je prevádzkovateľ poskytne dotknutej osobe informácie o

a) dobe uchovávania osobných údajov; ak to nie je možné, informáciu o kritériách jej určenia,

b) oprávnených záujmoch prevádzkovateľa alebo tretej strany, ak sa spracúvajú osobné údaje podľa § 13 ods. 1 písm. f),

c) práve požadovať od prevádzkovateľa prístup k osobným údajom týkajúcich sa dotknutej osoby o práve na opravu osobných údajov, o práve na vymazanie osobných údajov alebo o práve na obmedzenie spracúvania osobných údajov, o práve namietať spracúvanie osobných údajov, ako aj o práve na prenosnosť osobných údajov,

d) práve kedykoľvek svoj súhlas odvolať,

e) práve podať návrh na začatie konania podľa § 100,

f) zdroji, z ktorého pochádzajú osobné údaje, prípadne informácie o tom, či pochádzajú z verejne prístupných zdrojov,

g) existencii automatizovaného individuálneho rozhodovania vrátane profilovania podľa § 28 ods. 1 a 4; v týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie o použitom postupe, ako aj o význame automatizovaného individuálneho rozhodovania a predpokladaných dôsledkoch takého spracúvania osobných údajov pre dotknutú osobu.

(3) Prevádzkovateľ je povinný poskytnúť informácie podľa odsekov 1 a 2

a) najneskôr do jedného mesiaca po získaní osobných údajov, pričom zohľadní konkrétne okolnosti, za ktorých sa osobné údaje spracúvajú,

b) najneskôr v čase prvej komunikácie s touto dotknutou osobou, ak sa osobné údaje majú použiť na komunikáciu s dotknutou osobou, alebo

c) najneskôr vtedy, keď sa osobné údaje prvýkrát poskytnú, ak sa predpokladá poskytnutie osobných údajov ďalšiemu príjemcovi.

(4) Prevádzkovateľ poskytne dotknutej osobe pred ďalším spracúvaním osobných údajov informácie o inom účele a ďalšie relevantné informácie podľa odseku 2, ak má prevádzkovateľ v úmysle ďalej spracúvať osobné údaje na iný účel ako ten, na ktorý boli získané.

(5) Odseky 1 až 4 sa neuplatňujú

a) v rozsahu, v akom dotknutá osoba už dané informácie má,

b) v rozsahu, v akom sa poskytovanie týchto informácií ukáže ako nemožné alebo by si vyžadovalo neprimerané úsilie, najmä ak sa spracúvajú osobné údaje na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, na ktorý sa vzťahujú podmienky a záruky podľa § 78 ods. 8, alebo ak je pravdepodobné, že povinnosť uvedená v odseku 1 znemožní alebo závažným spôsobom sťaží dosiahnutie cieľov takého spracúvania osobných údajov; prevádzkovateľ je v takom prípade povinný prijať vhodné opatrenia na ochranu práv a oprávnených záujmov dotknutej osoby vrátane sprístupnenia daných informácií verejnosti,

c) v rozsahu, v akom sa získanie týchto informácií alebo poskytnutie týchto informácií ustanovuje v osobitnom predpise, ktorý sa na prevádzkovateľa vzťahuje a v ktorom sú ustanovené primerané opatrenia na ochranu práv a oprávnených záujmov dotknutej osoby,

3.3. Právo na prístup k osobným údajom

(1) Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú. Ak prevádzkovateľ takéto osobné údaje spracúva, dotknutá osoba má právo získať prístup k týmto osobným údajom a informácie o

a) účele spracúvania osobných údajov,

b) kategórii spracúvaných osobných údajov,

c) identifikácii príjemcu alebo o kategórii príjemcu, ktorému boli alebo majú byť osobné údaje poskytnuté, najmä o príjemcovi v tretej krajine alebo o medzinárodnej organizácii, ak je to možné,

d) dobe uchovávania osobných údajov; ak to nie je možné, informáciu o kritériách jej určenia,

e) práve požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby, ich vymazanie alebo obmedzenie ich spracúvania, alebo o práve namietať spracúvanie osobných údajov,

f) práve podať návrh na začatie konania podľa § 100,

g) zdroji osobných údajov, ak sa osobné údaje nezískali od dotknutej osoby,

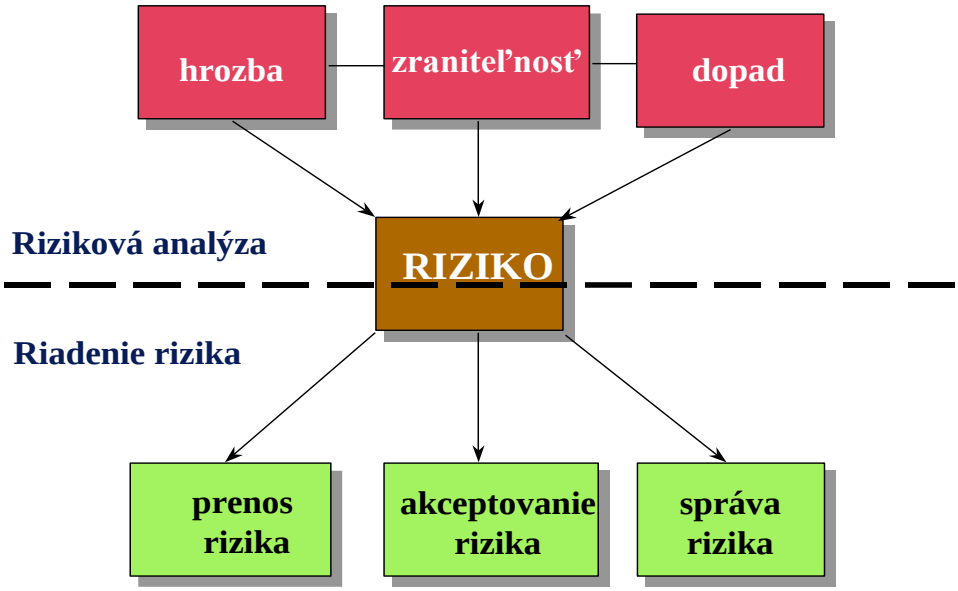
h) existencii automatizovaného individuálneho rozhodovania vrátane profilovania podľa § 28 ods. 1 a 4; v týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie najmä o použitom postupe, ako aj o význame a predpokladaných dôsledkoch takého spracúvania osobných údajov pre dotknutú osobu.

(2) Dotknutá osoba má právo byť informovaná o primeraných zárukách týkajúcich sa prenosu podľa § 48 ods. 2 až 4, ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii.

(3) Prevádzkovateľ je povinný poskytnúť dotknutej osobe jej osobné údaje, ktoré spracúva. Za opakované poskytnutie osobných údajov, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Prevádzkovateľ je povinný poskytnúť osobné údaje dotknutej osobe spôsobom podľa jej požiadavky.

(4) Právo získať osobné údaje podľa odseku 3 nesmie mať nepriaznivé dôsledky na práva iných fyzických osôb.

Riziková analýza aktív informačného systému:



Hrozby

Pre potreby tvorby analýzy je potrebné vytvoriť zoznam reálnych hrozieb voči aktívam, ktoré budú posudzované. Pre jednotlivé aktíva nemusia byť posudzované všetky hrozby, hodnotené budú len hrozby relevantné danému aktívu a časovému obdobiu.

Hrozba	Popis
Chyby a nekvalita údržby	Chybná prípadne nekvalitná údržba z dôvodov nedostatočnej odbornej pripravenosti pracovníkov, nedostatku náhradných dielov, materiálu, pohonných hmôt a pod.
Chyby prenosu	Chyby vzniknuté pri prenose dát, ktorých výsledkom môže byť modifikácia údajov.
Chyby úmyselné a neúmyselné	Činnosť OO, alebo inej osoby, ktorá nie je v súlade s internými a právnymi predpismi a jej výsledkom nie je snaha získať osobný prospech.
Neautorizovaná činnosť	Taká činnosť OO alebo externých návštevníkov, na ktorú nemajú oprávnenie a ktorou môžu spôsobiť prevádzkovateľovi škody.

Hrozba	Popis
Poruchy a chyby zariadení	Nefunkčnosť, nedostatočná alebo nesprávna funkčnosť zariadenia, chyby technických komponentov, softvéru, nedostatočnej, prípadne neodbornej údržby, nevyhovujúceho prevádzkového prostredia (vysoká teplota, vlhkosť a pod.), dosiahnutia životnosti komponentov a súčiastok.
Nedokumentované postupy	Vykonávanie činností bez odsúhlaseného metodického postupu len na základe overených alebo získaných skúseností.
Nedostatočná príprava	Nedostatočná odborná príprava OO, ktorí zabezpečujú prevádzku, správu a údržbu zariadení, systémov a aplikácii z dôvodu nedostatku školení, odbornej literatúry, jazykových znalostí oprávnených osôb.
Podvod alebo komplot	Cieľavedomá činnosť jednej alebo viacerých osôb (interných zamestnancov, externých spolupracovníkov a pod.), ktorej cieľom je nelegálne obohatenie sa na úkor prevádzkovateľa, prípadne jej partnerov. Falšovanie peňazí, cenín, podacích znakov.
Zničenie údajov a konfigurácií	Strata, zničenie údajov spracúvaných aplikáciami, potrebných pre plynulé a správne spracúvanie dát. Strata alebo zničenie konfigurácie operačných systémov, APV, databázových systémov, strata nastavení zariadení. Obnova týchto nastavení si môže vyžiadať veľké ľudské a časové kapacity.
Krádež	Odcudzenie zariadení, komponentov výpočtovej techniky, softvéru, dokumentácie, náhradných dielov, dopravných prostriedkov, Krádež hmotného majetku.
Nespokojnosť	Nespokojnosť s fungovaním , susedské problémy , zvieratá v OD,..
Nelegálne zhromažďovanie údajov	Nelegálne, neautorizované zhromažďovanie údajov. Kombináciou niektorých typov údajov, ktoré nie sú označené ako dôverné, môžu vzniknúť údaje citlivé z hľadiska prezradenia. Kombinácia niektorých skupín údajov môže byť zaujímavá pre rôzne záujmové alebo nelegálne skupiny.
Neidentifikovateľnosť vstupu	Samostatný, nekontrolovaný vstup zamestnancov do aplikácií, operačných a databázových systémov, priestorov alebo objektov bez možnosti spätne zistiť, kto a kedy sa v nich pohyboval. Nekontrolovaný pohyb zamestnancov.
Nesúlad s internou legislatívou	Nedodržiavanie, prípadne obchádzanie interných pravidiel platných v rámci prevádzkovateľa ,ktoré sú vydávané v podobe smerníc, príkazov, metodických usmernení a pod.
Nejasná alebo nesprávne interpretovaná legislatíva	Nedostatočne prepracované zákony, časté zmeny zákonov a ich pomalá alebo žiadna implementácia do legislatívneho prostredia organizácie.
Nedostatok finančných zdrojov	Nedostatok finančných zdrojov sa môže prejavovať rôznymi spôsobmi: - nedostatkom zdrojov na vnútornú správu a prevádzku organizácie, nedostatkom zdrojov na rozvoj systému, aplikácií, HW komponentov, nedostatkom zdrojov na rozvoj technológií, nedostatočným finančným ohodnotením ZO, slabým zabezpečením bezpečnostnými systémami.

Hrozba	Popis
Nedostatočná centrálna správa	Nedostatočná centrálna správa môže spôsobiť nedostatočný prehľad o fungovaní zariadení, stratu hlásení o narušení bezpečnosti, nekonsolidovaným stavom databáz a pod.
Nedostatočné kompetencie	Nedostatok kompetencií, prekrývanie kompetencií. Problémy v komunikácii medzi jednotlivými osobami.
Nejasná stratégia a koncepcia	Nedostatočné koncepčné riadenie zo strany prevádzkovateľa, nejasná stratégia rozvoja , systémov, technickej infraštruktúry, bezpečnosti, technologickej nevyrovnanosti.
Odmietnutie služby	Neposkytnutie požadovanej služby, nezískanie požadovaného výstupu zo systému z dôvodu nefunkčnosti zariadení, softvéru alebo hardvéru, preťaženia alebo nedostatočnej prenosovej kapacity liniek, nedodržanie zmluvy a pod.
Špionáž	Nekontrolovaná činnosť cudzích osôb. Jeho cieľom je získanie dôverných informácií,
Poškodenie úmyselné a neúmyselné	Poškodenie zariadení, komponentov, hardvéru, softvéru, médií, hmotného majetku a pod. neúmyselne z dôvodu chybnej manipulácie, nedostatočného zaškolenia obsluhy, chyby údržby a obsluhy alebo úmyselne (snaha poškodiť prevádzkovateľa).

Prerušenie dodávok elektrickej energie	Prerušenie dodávky elektrickej energie do objektu kritického z hľadiska prevádzky. Môže byť spôsobené prírodnými vplyvmi (búrka, blesk, prerušenie vedenia) alebo preťažením vedenia, prípadne pripojením ďalšieho odberateľa na rozvod, ktorý nie je dostatočne dimenzovaný. Neexistencia záložného napájania s dostatočnou kapacitou.

Hrozba	Popis
Únik údajov	Získanie údajov neautorizovanými aj autorizovanými osobami a ich využitie neschváleným spôsobom s cieľom obohatenia sa.
Nevhodné umiestnenie	Umiestnenie dôležitých aktív alebo ich častí na miestach s vysokým rizikom poškodenia požiarom, zatopením a pod., prípadne na miestach s častým pohybom osôb.
Výtržnosť	Náhodné narušenia objektov alebo systémov v dôsledku neplánovaných aktivít (demonštrácie v okolí, kultúrne a športové podujatia) s následným narušením priestoru, vniknutie do objektu, prerušenie normálnej práce, vandalizmus.
Ohrozenie osôb	Pomsta, vydieranie alebo psychologický nátlak s možnosťou ohrozenia zdravia alebo života OO, partnerov, návštev a iných osôb nachádzajúcich sa v priestoroch prevádzkovateľa.
Prírodné katastrofy a priemyselné nehody	Pod prírodné katastrofy a priemyselné nehody spadá zaplavenie, skrat na vedení, zanedbanie protipožiarnych opatrení, úmyselné založenie požiaru, neúmyselné založenie požiaru, havária , zosuvy pôdy a pod.
Single point of failure	Existencia jedného miesta (komponentu) v ktorom sú koncentrované kritické aktíva prevádzkovateľa bez adekvátnej náhrady.
Terorizmus	Cieľom terorizmu je násilné poškodenie organizácie, čo najväčšie narušenie jej činnosti, vznik neistoty medzi zamestnancami. Môže sa prejaviť uložením výbušniny, vydieraním, bratím rukojemníka, výhražnými telefonátmi, poštovými a listovými bombami.

Sila hrozieb je hodnotená troma stupňami:

- **(V) –** vysoká sila hrozby,
- **(S)** – stredná sila hrozby,
- **(N)** – nízka sila hrozby.

Zraniteľnosť

Zraniteľnosť je slabé miesto v systéme, ktoré môže spôsobiť realizáciu hrozby a narušenie bezpečnosti systému. Zraniteľnosť je hodnotená troma stupňami:

- **(V) –** vysoká zraniteľnosť,
- **(S)** – stredná zraniteľnosť,
- **(N)** – nízka zraniteľnosť.

Dopad

Je výsledok pôsobenia realizovanej hrozby na strategickú os. Dopad sa môže prejaviť znížením integrity, dostupnosti alebo dôvernosti hodnoteného aktíva. Veľkosť dopadu je priamoúmerná počtu zasiahnutých strategických osí a ich váham. Hodnotu dopadu bude tvoriť súčet váh strategických osí zasiahnutých hodnotenou hrozbou.

Suma dopadov	Hodnotenie
0	0
1 – 2	1
3 – 4	2
5 – 7	3
8 a viac	4

Analýza a hodnotenie rizika

Výška rizika je číselná hodnota v rozpätí 0 – 8, ktorá sa určuje podľa sily hrozby, výšky zraniteľnosti a hodnoty dopadov. Hodnotenie rizika sa v súlade s metodikou robí podľa nasledujúcej tabuľky.

Riziko - výška	Hrozba Zraniteľnosť	N			S			V		
		N	S	V	N	S	V	N	S	V
Funkčný dopad - hodnota	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Z tabuľky vyplýva, že najvyššia hodnota rizika je 8 a najnižšia je 0. Pre prijatie zodpovedajúcich opatrení a ľahšiu orientáciu môžeme zaviesť pomocné hodnotenie rizika v štyroch kategóriách.

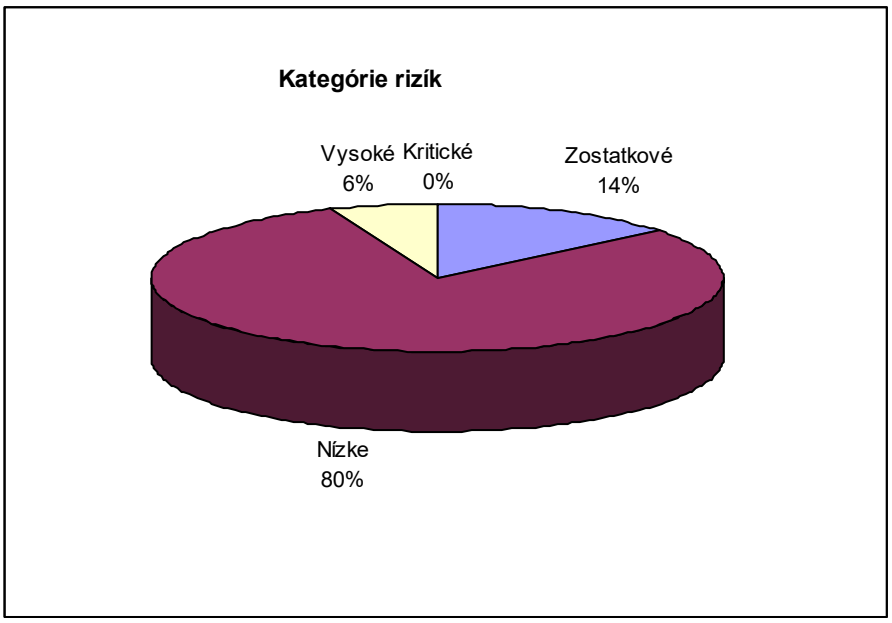
Názov	Hodnotenie podľa tabuľky 1.3	Opatrenia
Zostatkové riziko	0 až 1	Nemusia byť prijaté opatrenia. Riziko je potrebné sledovať a pravidelne vyhodnocovať.
Nízke riziko	2 až 4	Plánovať aplikáciu opatrení v období nad jeden rok.
Vážne riziko	5 až 6	Plánovať aplikáciu opatrení v blízkom období (jednotky mesiacov).
Kritické riziko	7 až 8	Prijať okamžité opatrenia proti identifikovanej hrozbe.

Popis položiek funkčných rizík
V nasledujúcej tabuľke je uvedený prehľad položiek katalógu funkčných rizík.

Položka	**Popis**
Aktívum - popis	Aktíva uvedené v tabuľke boli identifikované počas funkcionálnej analýzy rizík.
Hrozba - popis	V tomto stĺpci sú uvedené hrozby zo zoznamu hrozieb, ktoré sú relevantné pre dané aktívum. Ak je hrozba aplikovateľná na aktívum, ale spôsobuje len nízke riziko, neuvádza sa.
Hrozba – C, I, A	V týchto stĺpcoch je uvedené, ktoré z bezpečnostných potrieb – C – dôvernosť (Confidentality), I – integrita (Integrity), A – dostupnosť (Availability) – môže hrozba ovplyvniť.
Hrozba – sila	Tento stĺpec udáva silu hrozby voči aktívu za predpokladu, že nie sú implementované žiadne bezpečnostné opatrenia. Sila hrozieb je v súlade s metodikou hodnotená troma stupňami: **(V)** –vysoká, **(S)** – stredná a **(N)** – nízka sila hrozby.
Zraniteľnosť – popis	Stĺpec určuje zraniteľnosť v zmysle dôvernosti, dostupnosti a integrity. Nevzťahuje sa len na súčasnú zraniteľnosť prevádzkovateľa, ale odráža aj jej predpokladaný vývoj.
Zraniteľnosť – hodnota	Stĺpec udáva veľkosť zraniteľnosti aktív. Zraniteľnosť je hodnotená troma stupňami **(V)** – vysoká, **(S)** – stredná a **(N)** – nízka.
Dopady na strategické osi – popis	V stĺpcoch je zoznam strategických osí. U tých osí u ktorých je možné očakávať dopady v dôsledku realizácie hrozieb je vyznačená váha týchto zasiahnutých osí, u osí u ktorých sa zasiahnutie nepredpokladá je prázdne pole.
Dopady na strategické osi – hodnota	V tomto stĺpci je ohodnotená veľkosť dopadov. Spôsob určenia hodnoty dopadov je popísaný vyššie.
Riziko – hodnota	Tento stĺpec určuje úroveň rizík pre jednotlivé aktíva. Riziká sa hodnotia v súlade s metodikou v škále od 0 po 8. Po odsúhlasení bude kritériom implementácie bezpečnostných mechanizmov.
Riadenie rizika	V tomto stĺpci sa nachádza návrh konzultantov na riadenie rizika. Do úvahy prichádzajú tri možnosti **(S) –** správa, **(P)** – prenesenie, **(A) –** akceptovanie.

Výsledkom rizikovej analýzy aktív informačného systému je posúdenie a hodnotenie rizík pôsobiacich na informačný systém. Z analýzy môžeme vidieť posúdenie všetkých hodnotených aktív IS podrobne po jednotlivých hrozbách.
S pohľadu použitej metodiky môžeme riziká pôsobiace na IS rozdeliť do nasledovných kategórií:

Hodnotenie rizík		
Kategória	Počet	%
Zostatkové	18	14,1%
Nízke	102	79,7%
Vysoké	8	6,3%
Kritické	0	0,0%



Z uvedenej tabuľky je možné identifikovať, že aj keď nebolo identifikované žiadne kritické riziko bude nevyhnutné prijať opatrenia pre obmedzenie vysokých rizík. Ide najmä o tieto oblasti:

- bezpečnosť údajov, kde nie je možné vylúčiť vynesenie informácií z organizácie, resp. neautorizovanú činnosť. Tieto riziká sa týkajú všetkých skupín údajov,
- všetky úschovné objekty pre uloženie materiálov obsahujúcich osobné údaje by mali byť kovové (odolné proti požiaru) so zámkovým systémom vyššej triedy (min. trieda 2 podľa ČSN P ENV 1627),
- Ak by došlo k prenosu dát cez internet je nutné dôsledne trvať na dodržiavaní bezpečnostných pravidiel pri pripájaní sa k internetu tak, aby nebolo možné realizovať spojenie z iného, než určeného počítača,
- v zmysle platnej legislatívy nie je potrebné zaistiť podpísanie súhlasu zamestnancov so spracovaním ich osobných údajov pre potreby mzdovej a ekonomickej agendy,
- riziká vyplývajúce z možných nesprávnych rozhodnutí alebo zanedbania povinností zo strany vedenia, ktorí spracúvajú OÚ, aj ostatných zamestnancov nemožno úplne vylúčiť, ale je ich možné minimalizovať sústavným zvyšovaním kvalifikácie, preverovaním znalosti príslušných povinností a dôslednou kontrolnou činnosťou na všetkých úsekoch.

Nepokryté riziká

Časť vážnych rizík možno zaradiť do kategórie nepokrytých rizík, pretože vzhľadom na ich charakter nie je možné ich v potrebnej miere eliminovať. Sú totiž spôsobené nedokonalosťou ľudského faktora (možnosť podvodu, presadzovania osobných záujmov, nespoľahlivosti, úniku údajov, skratového konania, zámerného osobného útoku) a nedostatkami reálnej spoločenskej situácie, v ktorej organizácia pôsobí (možnosť vydierania, prinútenia k spolupráci), ak nie sú všeobecne vytvorené spoľahlivé mechanizmy zabraňujúce takýmto aktivitám.

Analýza zhody prijatých opatrení s požiadavkami štandardov

Spôsob hodnotenia zhody

V nasledujúcich tabuľkách je vykonaná analýza zhody skutkového stavu v podmienkach organizácie s požiadavkami štandardov. Na záver je celkové vyhodnotenie stavu ochrany po oblastiach a za celý systém ochrany. Celkové hodnotenie je dané podľa vzorca:

STAV OCHRANY = $\sum$ Wi x Hi kde STAV OCHRANY je celkový stav ochrany osobných údajov v organizácii

Wi váhový koeficient hodnotenej oblasti, $\sum$wi=1

Hi hodnotenie v i-tej oblasti.

Váhové koeficienty hodnotenia

Oblasť	**Hodnota váhového koeficientu**
1. Fyzické opatrenia	0,20
2. Technické opatrenia	0,20
3. Programové opatrenia	0,30
4. Režimové opatrenia	0,15
5. Personálne opatrenia	0,15
KONTROLNÁ SUMA	**1,00**

Výsledkom analýzy je nasledovné posúdenie zhody:

Oblasť	**Skóre za oblasť**	**Hodnotenie**
1. Fyzické opatrenia	36,67	Štandardná
2. Technické opatrenia	65,00	Štandardná
3. Programové opatrenia	61,14	Štandardná
4. Režimové opatrenia	45,71	Štandardná
5. Personálne opatrenia	63,33	Štandardná
CELKOVÉ HODNOTENIE	**55,03**	**Štandardná**

Je potrebné poznamenať, že nie je nevyhnutné, aby boli splnené úplne všetky požiadavky štandardu. Z tabuľky pre celkové vyhodnotenie je zrejmé, že už stav, pri ktorom sú splnené aspoň 2/3 zo všetkých požiadaviek, zodpovedá nadštandardnej úrovni ochrany údajov a splnenie požiadaviek na úrovni viac ako 1/3 zodpovedá štandardnej úrovni. Maximálne požiadavky (hodnotenie 1,00 = 100 % splnených požiadaviek) sa uplatňujú len napr. v sektore obrany, finančných inštitúciách, strategických podnikoch a pod.

Na základe vypracovanej analýzy rizík a analýzy zhody so štandardami sú odporúčané nasledovné opatrenia.

2. Postupy pri haváriách, poruchách a iných mimoriadnych situáciách

Prevádzkovateľ zosúladí dokumentáciu krízových plánov tak, aby do nich zakomponoval situácie bezprostredne súvisiace s ochranou a bezpečnosťou osobných a iných citlivých údajov. Organizácia zabezpečí účinné fungovania krízového plánu, harmonizuje všetky opatrenia, ktoré sa majú aplikovať v prípade niektorej z krízových situácií. V smernici nie sú uvedené všetky opatrenia, pretože jeho súčasťou sú aj opatrenia vyplývajúce z iných všeobecne záväzných predpisov.

Krízový plán okrem iného určuje:

a) organizačné opatrenia určujúce činnosti pri narušení objektu a priestorov, v ktorých sa spracúvajú osobné údaje, a pri pokuse o narušenie objektu,

b) organizačné opatrenia pri zistení narušenia fungovania IS,

c) organizačné opatrenia určujúce činnosti v prípade vzniku mimoriadnych udalostí,

d) spôsob výkonu kontroly opatrení krízového plánu.

3. Organizačné opatrenia určujúce činnosti pri narušení objektu a chráneného priestoru a pri pokuse o narušenie objektu a chráneného priestoru

Za narušenie objektu a chráneného priestoru a pokus o narušenie objektu a chráneného priestoru sa pre účely krízového plánu rozumie:

- krádež obyčajná;
- krádež vlámaním;

- pokus krádeže;
- teroristický útok;
- sabotáž, poškodzovanie cudzej veci, výtržnosť;
- hrozba uložením výbušného systému.

3.1 Krádeže a pokusy krádeží

Krádežou sa rozumie trestný čin krádeže alebo jeho pokusu (§ 247 trestného zákona) a to aj v prípade, že došlo ku krádeži údajov bez rozdielu ich dôležitosti. Pri krádeži v objekte a chránenom priestore spôsobenej vlastným zamestnancom, pracovníkom iných servisných dodávateľských firiem, návštevou v pracovnej dobe, sa vykonajú tieto organizačné opatrenia:

Poradie	Popis opatrenia	Kto vykoná	Spôsob
1.	Zadržanie páchateľa krádeže a pokusu o krádež – ak je to možné	zamestnanci	Znemožnením úniku z priestorov prevádzkovateľa. O zadržaní ihneď informovať nadriadeného a bezpečnostného správcu
2.	Oznámenie zistenej krádeže v objekte	občan, ktorý krádež zistil	Oznámiť skutočnosť svojmu nadriadenému a bezpečnostnému správcovi a vyčkať na ich pokyny.
		zamestnanci	Oznámiť skutočnosť orgánom činným v trestnom konaní (Policajnému zboru)
3.	Zabezpečenie miesta krádeže pred vniknutím neoprávnenej osoby a pre uchovanie dôkazného materiálu pre ďalšie vyšetrovanie	zamestnanci	Fyzickým strážením, vytvorením účinnej prekážky vstupu do priestorov v ktorých je možné predpokladať, že ku krádeži došlo

Pri teroristickom útoku na objekt, sú na objekte prijaté tieto organizačné opatrenia:

Poradie	Popis opatrenia	Kto vykoná	Spôsob
Zamestnanci a osoby zadržiavané v priestoroch organizácie a priamo ohrozované na životoch			
1.	Zabezpečenie bezpečnosti zadržiavaných osôb	Každý zadržiavaný	Primeranou spoluprácou s páchateľmi s cieľom navodiť kľud, neprovokovať k činom vedúcim k stratám na životoch
2.	Únik z ohrozeného priestoru	Každý zadržiavaný	Únik realizovať len za asistencie privolanej ozbrojenej pomoci, účinne spolupracovať s tým realizujúcim oslobodenie zadržiavaných osôb
Zamestnanci priamo neohrozovaní teroristickým útokom			
1.	Oznámenie zistenej skutočnosti	Každý občan, ktorý skutočnosť zistil	Bezodkladne informovať orgány policajného zboru, potom nadriadeného pracovníka a bezpečnostného správcu
2.	Sledovanie a stráženie ohrozeného priestoru	Do príchodu príslušníkov polície zamestnanci	Pozorovaním miesta teroristického útoku z bezpečnej vzdialenosti, sledovanie pohybu osôb a vozidiel.
3.	Zamedzenie vstupu ďalších osôb do ohrozeného priestoru	Do príchodu príslušníkov polície zamestnanci	Podaním informácie vhodným spôsobom
4.	Súčinnosť s policajným zborom	Každý občan	Podľa pokynov a požiadaviek poskytne každý pracovník policajnému zboru účinnú pomoc.
Cieľ zvládnutia každého teroristického útoku je najprv ochrana života a zdravia osôb a až následne majetku			

3.2 Poškodzovanie cudzej veci, sabotáž a výtržnosť

Za poškodzovanie cudzej veci (majetku prevádzkovateľa), sabotáž a výtržnosť sa všeobecne považujú činnosti, ktoré majú poškodiť majetok prevádzkovateľa alebo znemožniť jej ďalšie normálne fungovanie, pričom si páchateľ obvykle neprisvojuje majetok prevádzkovateľa. Za majetok sa považuje hmotný ale aj nehmotný prevádzkovateľa.
Pri zistení týchto činov sa postupuje rovnako ako pri krádežiach.

3.3 Hrozba uloženia výbušného systému

Pri hrozbe uloženia výbušného systému, sú na objekte prijaté tieto organizačné opatrenia:

Poradie	Popis opatrenia	Kto vykoná	Spôsob
1.	Evakuácia zamestnancov organizácie a osôb nachádzajúcich sa v priestoroch organizácie	Oprávnená osoba	Hlasom, telefónom, osobne. Určiť miesto kam majú byť evakuované osoby.
2.	Informovať ostatné organizácie nachádzajúce sa v budove	Oprávnená osoba	Telefonickým vyrozumením, alebo vyslaním zamestnanca.
3.	Povinnosť oznámiť uloženie výbušného systému	Oprávnená osoba	Telefonicky policajnému zboru
4.	Zabránenie vstupu osôb do priestorov organizácie	Oprávnená osoba	Po spoľahlivom zistení, že všetky osoby opustili priestory uzamknúť vstupné dvere.
5.	Spolupráca s policajným zborom	Každý občan	Podľa pokynov polície

3.4 Organizačné opatrenia pri narušení fungovania IS

Narušením fungovania informačného systému organizácie sa rozumie akákoľvek situácia, ktorá má za následok poškodenie, zničenie, modifikáciu, alebo únik údajov z NVR alebo počítačov. Narušením je takisto nežiaduce alebo nepredpokladané chovanie používaného softvéru, aj keď zdanlivo nevedie k narušeniu údajov, programových prostriedkov a operačných systémov (jedná sa hlavne o činnosť vírusov alebo obdobných infiltrácií). Za narušenie sa považuje aj porucha NVR alebo počítača, ktorá môže spôsobiť stratu údajov. Pre zvládnutie uvedených situácií sa stanovujú nasledujúce opatrenia:

Poradie	Popis opatrenia	Kto vykoná	Spôsob
1.	Zamedzenie ďalších škôd.	Oprávnená osoba	Bezodkladné bezpečné vypnutie počítača, odpojenie zdroja elektrickej energie, vrátane periférií. Odpojenie od komunikačných prostriedkov. Pri voľbe spôsobu vypnutia zvoliť malú stratu údajov (rozpracovanej práce) pred rozsiahlym poškodením zariadenia a údajov.
2.	Hlásenie narušenia.	Oprávnená osoba	Informovať bezpečnostného správcu a zamestnanca zodpovedného za chod IS
3.	Poskytnutie účinnej pomoci pri odstraňovaní škôd a vyšetrení incidentu.	Všetci občania	Podľa pokynov bezpečnostného správcu a zamestnanca zodpovedného za chod IS

3.5 Organizačné opatrenia určujúce činnosti v prípade vzniku iných mimoriadnych udalostí

Mimoriadnymi udalosťami sa pre účely krízového plánu v súvislosti s ochranou IS organizácie rozumejú najmä:

- únos občanov s cieľom ohroziť prevádzkovateľa,
- vydieranie občanov s cieľom ohroziť prevádzkovateľa, živelná pohroma, prírodná katastrofa, priemyselná a ekologická havária.

3.6 Únos

Únosom s cieľom ohroziť prevádzkovateľa sa rozumie najmä trestný čin brania rukojemníka (§ 234a trestného zákona),

ktorého cieľom je prinútiť prevádzkovateľa, aby konala proti svojim vlastným záujmom, resp. aby inak porušovala zákony SR. V prípade únosu sa vykonajú tieto opatrenia:

Poradie	Popis opatrenia	Kto vykoná	Spôsob
1.	Ohlásenie únosu policajnému zboru a nadriadenému pracovníkovi .	Občan, ktorý bol únoscami kontaktovaný, alebo sa o únose inak dozvedel.	Bezodkladne telefonicky informovať policajný zbor a riaditeľku organizácie .
2.	Spolupráca s únoscami.	Občan, ktorý je v kontakte s únoscami.	Uposlúchnuť pokyny únoscov (okrem podmienky neinformovať políciu), pokúsiť sa odložiť plnenie podmienok na prepustenie. S únoscami nevyjednávať, navodiť zdanie účinnej spolupráce.
3.	Súčinnosť s políciou.	Občan, ktorý je v kontakte s únoscami.	Postupovať podľa pokynov polície.

3.7. Vydieranie a nátlak na občana

Vydieranie a nátlak na občana sú hrozby iných osôb, alebo prevádzkovateľa smerujúce k tomu aby vydieraný na ktorého je vyvíjaný nátlak konal proti záujmom prevádzkovateľa. Pre prípad vydierania a nátlaku sa stanovujú tieto organizačné opatrenia:

Poradie	Popis opatrenia	Kto vykoná	Spôsob
1.	Ohlásenie vydierania a nátlaku.	Občan, ktorý bol únoscami kontaktovaný, alebo sa o únose inak dozvedel.	Bezodkladne telefonicky policajnému zboru a riaditeľke organizácie.
2.	Spolupráca s vydieračmi.	Vydieraný občan.	Podľa pokynov polície spolupracovať, navodiť zdanie spolupráce a poskytnúť pomoc a informácie vedúce k odhaleniu vydierača.
3.	Izolovanie vydieraného.	Oprávnená osoba	Vydieranému znemožniť konanie proti záujmom organizácie – znemožnením používania telefónu, faxu, kopírovacích zariadení a PC, prípadne aj nevpustením do priestorov. Izoláciu konzultovať s policajným zborom.

3.8. Živelná pohroma, prírodná katastrofa, priemyselná a ekologická havária

Hrozby rozsiahlych živelných pohrôm, prírodných katastrof, alebo ekologických a priemyselných havárií sú nízke. Najpravdepodobnejšou živelnou pohromou je požiar. Pri ostatných pohromách a haváriách sa postupuje obdobne ako pri požiari. Pre zvládnutie požiaru je vypracovaný plán požiarnej ochrany Plány obsahujú aj poradie evakuácie a záchrany majetku .

3.9. Opatrenia na ošetrenie rizík

Na ochranu osobných údajov budú použité primerané štandardy, ktoré sa používajú na ochranu OÚ. Na základe týchto podkladov, boli pre účely ochrany osobných údajov vypracované účelové štandardy. Pre informačné systémy s použitím automatizovaných a neautomatizovaných prostriedkov spracúvania sa použijú štandardy všetkých skupín, t.j.:

a) Fyzické opatrenia;
b) Technické opatrenia;
c) Programové opatrenia;
d) Režimové opatrenia;
e) Personálne opatrenia.
Na základe vypracovanej analýzy rizík a analýzy zhody so štandardami sú odporúčané nasledovné opatrenia.

Čl. 4
Základné zásady bezpečnej prevádzky IS

1. Opravy, úpravy a akýkoľvek zásah na všetkých komponentov IS môžu vykonávať len kvalifikované osoby, konajúce na základe platného, vopred daného poverenia. Všetky opravy a úpravy musia byť primerane zdokumentované.

2. Pri odstraňovaní porúch kľúčových komponentov IS je zodpovedné osoby oprávnené vyhlásiť technickú prestávku na nevyhnutný čas potrebný pre odstránenie poruchy.

3. Na počítačoch IS je zakázané inštalovať a prevádzkovať programové vybavenie získané nelegálnym spôsobom, resp. porušujúce platné licenčné podmienky.

4. Prevádzkovateľ je povinný zabezpečiť antivírovú ochranu IS pracoviska kvalitným antivírovým prostriedkom a zabezpečiť jeho včasnú aktualizáciu.

5. V prípade vyraďovania počítačových systémov a médií sú zodpovedné osoby povinné zabezpečiť dôkladný výmaz údajov IS na vyraďovaných zariadeniach a médiách.

6. Každá oprávnená osoby je povinná pri dlhodobom opustení miestnosti, v ktorej je uložená jemu pridelená pracovná stanica, odhlásiť sa zo systému. V prípade krátkodobého opustenia miestnosti musí aspoň aktivovať šetrič obrazovky s heslom.

Čl. 5
Zálohovanie údajov IS

1. Oprávnená osoba je povinná systematicky zálohovať údaje IS v súlade so záznamom spracovateľských činností.

2. Oprávnená osoba je oprávnená zálohovať údaje IS, na ktorých je zachytená protiprávna činnosť , a tieto údaje odovzdať príslušným orgánom na konanie v tejto veci. Odovzdanie zálohovaných údajov musí byť realizované protokolárne. Protokol je súčasťou tohto PTOO.

3. Oprávnené osoby sú povinné zálohovať aj kompletný systém nahrávacieho zariadenia tak, aby bolo možné v prípade potreby rýchlo obnoviť základné a aplikačné programové vybavenie, konfiguračné súbory, štruktúru súborového systému a všetky podstatné parametre systému potrebné pre rutinnú prevádzku.

4. Média so záložnými kópiami údajov a systému je nevyhnutné skladovať tak, aby boli chránené pred neoprávnenou manipuláciou a nepriaznivými vplyvmi prostredia a aby sa zmenšilo riziko súčasného poškodenia alebo zničenia ako originálnych, tak aj záložných kópií chránených údajov

5. Všetky média so záložnými kópiami údajov musia byť označené tak, aby označenie jednoznačne určovalo aktuálny obsah média a taktiež aby bolo možné určiť dátum vytvorenia záložnej kópie na predmetnom médiu.

6. Všetky média so záložnými kópiami údajov a programového vybavenia musia byť označené tak, aby označenie jednoznačne určovalo aktuálny obsah média a taktiež aby bolo možné určiť dátum vytvorenia záložnej kópie na predmetnom médiu.

Čl. 6
Zásady riešenia nepredvídaných udalostí s dopadom na prevádzku alebo údaje IS

1. V prípade nepredvídanej situácie ohrozujúcej prevádzku IS, alebo údaje IS sú oprávnené osoby povinné

pri riešení súvisiacich problémov zaistiť primeranú ochranu všetkých komponentov systému obsahujúcich citlivé údaje IS pred prístupom neoprávnených osôb.

2. V prípade nepredvídanej situácie je prevádzkovateľ oprávnený vyhlásiť technickú prestávku na nevyhnutný čas potrebný pre riešenie udalosti.

3. Pri odstraňovaní následkov nepredvídaných situácií je prevádzkovateľ oprávnený stanoviť prioritu poradia riešenia problémov.

Čl. 7
Zásady riešenia bezpečnostných incidentov

1. V prípade výskytu bezpečnostného incidentu oprávnená osoba bezodkladne informuje prevádzkovateľa, s ktorým tiež konzultujú postup riešenia incidentu.

2. Riešenie každého bezpečnostného incidentu musí byť primerane zdokumentované. Dokumentuje sa predovšetkým príčina vzniku incidentu (pokiaľ je známa), dôsledky, všetky opatrenia prijaté pri riešení incidentu a ich účinnosť.

3. Oprávnené osoby sa pri riešení bezpečnostného incidentu riadia nasledovnými prioritami:

    a) bezodkladné obnovenie bežnej prevádzky IS aspoň v redukovanom režime, zabezpečenie ochrany údajov IS, zachovanie dôkazového materiálu nevyhnutného na ďalšiu analýzu príčin vzniku bezpečnostného incidentu,
    b) zistenie príčin, ktoré viedli k vzniku bezpečnostného incidentu,
    c) určenie zodpovednosti za vznik bezpečnostného incidentu a vyvodenie dôsledkov,
    d) zovšeobecnenie zistených skutočností a návrh opatrení na zabránenie opakovanému výskytu bezpečnostného incidentu.

4. Prevádzkovateľ nahlási každý bezpečnostný incident Úradu na ochranu osobných údajov do 72 hodín od jeho zistenia na adrese: **statny.dozor@pdp.gov.sk**

Čl. 8
Prevencia

1. Prevádzkovateľ je povinný pravidelne každý mesiac zabezpečiť vykonanie základnej preventívnej kontroly kľúčových komponentov IS (testovanie systému, odstránenie nepotrebných súborov, posúdenie rýchlosti zapĺňania pamäťovej kapacity, množstvo a vek životnosti médií používaných na zálohovanie, previerka na výskyt nových programov v systéme, vyčistenie komponentov systému a pod.). Na tento účel je prevádzkovateľ oprávnený vyhlásiť odstávku systému na nevyhnutne potrebnú dobu. Termín odstávky stanoví tak, aby čo najmenej narušil bežnú činnosť.
2. Oprávnené osoby sú povinní pravidelne, minimálne raz za štvrťrok, vykonať základnú preventívnu kontrolu zameranú na preverenie funkčnosti komponentov nevyhnutných pre riešenie nepredvídaných situácií (zariadenie pre zálohovanie a obnovu údajov, média so záložnými kópiami údajov a programov, aktuálnosť zálohovaných prístupových hesiel a ďalších uchovávaných parametrov systému).

Čl. 9
Záverečné ustanovenia

1. Porušenie týchto pravidiel bude posudzované ako závažné porušenie pracovnej disciplíny zamestnanca v zmysle príslušných ustanovení Zákonníka práce resp. zákona NR SR č.18/2018 o ochrane osobných údajov, smernica EÚ – GDPR.

Bušince, dňa 06.marca 2024

Schválil:

Vypracoval:

Ing. Zoltán Végh, starosta obce