Železnice Slovenskej republiky
Železničné telekomunikácie

Smernica

Bezpečnostná politika KIS ŽSR – skrátená politika pre tretie strany

(určená na zverejnenie na www.zsr.sk)

Spracovateľský / gestorský útvar	**Číslo**	**Označenie**
Železničné telekomunikácie	973/ÚR/2020/2	O-05-ŽT-2020
Účinnosť od		
Dňom zverejnenia (05.01.2021)		
Schválil	**Dňa**	
Ing. Miloslav Havrila, v. r. generálny riaditeľ ŽSR	23.12.2020	

Predmet
Informatika a telekomunikácie

Súvisiace interné riadiace akty:
Bezpečnostná politika KIS ŽSR

Prílohy:
Príloha č.1: Pravidlá a formuláre pre riadenie prístupu tretích strán do IKT prostriedkov ŽSR
Príloha č.2: Bezpečnostné pravidlá pre zabezpečenie prístupu do IKT prostriedkov ŽSR
Príloha č.3: Vyhlásenie o ochrane dôverných informácií získaných prístupom do IKT prostredia ŽSR
Príloha č.4: Dohoda o ochrane dôverných informácií a skutočností tvoriacich obchodné tajomstvo

SLEDOVANIE VYDANÍ A ZMIEN DOKUMENTU

Zoznam vydaní dokumentu

Vydané pod číslom	Účinnosť od – do
973/ÚR/2020/2	Od 05.01.2021

Uvádza sa spisové číslo aktuálneho vydania a v novelizovanom dokumente (2. a ďalšie vydanie) údaj so spisovým číslom predošlého vydania s rozpätím jeho účinnosti (od – do).

Záznam o zmenách

Číslo zmeny	Popis	Účinnosť	Poznámky	Zmenu zapracoval (podpis)

Zmeny sú vydávané spracovateľským útvarom tohto dokumentu.
Tento dokument sa vydáva len v elektronickej podobe a jeho aktuálne znenie je umiestnené (zverejnené) v dokumentovom úložisku IP ŽSR, v knižnici Interné riadiace akty.
Držiteľ výtlačku tohto dokumentu je zodpovedný za včasné a správne vykonanie vydaných zmien a vykonanie záznamu o zmenách.

OBSAH

PREHLÁSENIE VEDENIA ŽSR 5

1. ÚVOD 6

1.1 RÁMEC PRE RIADENIE BEZPEČNOSTI 7
1.2 STRATEGICKÉ CIELE ŽSR V OBLASTI BEZPEČNOSTI 7
1.3 POUŽÍVANIE POLITIKY PRE TRETIE STRANY 8

2. ZÁKLADNÉ POJMY A SKRATKY 9

2.1 ZOZNAM ZÁKLADNÝCH POJMOV 9
2.2 ZOZNAM POUŽITÝCH SKRATIEK 12

3. ORGANIZÁCIA A RIADENIE BEZPEČNOSTI NA ŽSR 13

3.1 ORGANIZÁCIA BEZPEČNOSTI NA ŽSR 13
3.1.1 Úroveň stratégie a riadenia 13
Vedenie ŽSR 13
Bezpečnostný výbor ŽSR (BV ŽSR) 14
Manažér informačnej a kybernetickej bezpečnosti (MIKB) 14
Metodici bezpečnosti 14
Zodpovedná osoba za ochranu osobných údajov (DPO) 14
3.1.2 Úroveň prevádzky a realizácie 14
Bezpečnostní správcovia IS 14
Vlastníci aktív 14
Koordinátori zmluvného vzťahu 15
Pracovné skupiny pre bezpečnosť 15
Koncoví používatelia IS a ostatní zamestnanci 15
3.1.3 Úroveň kontroly a auditu 15
Audítor bezpečnosti 15
Kontrola dodržiavania bezpečnostných opatrení 15
3.2 RIADENIE BEZPEČNOSTNÝCH RIZÍK 15

4. RIADENIE OCHRANY KYBERNETICKEJ BEZPEČNOSTI 16

5. RIADENIE OCHRANY OSOBNÝCH ÚDAJOV 17

6. RIADENIE OCHRANY KRITICKEJ INFRAŠTRUKTÚRY 18

7. RIADENIE OCHRANY ÚDAJOV SPADAJÚCICH POD ZÁKON Č. 351/2011 Z. Z. O ELEKTRONICKÝCH KOMUNIKÁCIÁCH 18

8. ZÁKLADNÉ BEZPEČNOSTNÉ ZÁSADY A PRINCÍPY 19

8.1 PERSONÁLNA BEZPEČNOSŤ 19
8.1.1 Výkon činností zamestnancami tretích strán 19
8.1.2 Poskytnutie informácií zamestnancom tretích strán 20
8.2 RIADENIE PRÍSTUPU 20
8.2.1 Zásady riadenia prístupu tretím stranám 20
8.2.2 Riadenie prístupu do IS a sietí 21
8.3 BEZPEČNOSŤ PREVÁDZKY IKT PROSTRIEDKOV 22
8.3.1 Prevádzka IKT prostriedkov 22
8.3.2 Dokumentácia systémov 22
8.3.3 Ochrana pred škodlivým kódom 22
8.3.4 Údržba a správa prevádzkových problémov 22
8.3.5 Monitorovanie používania systémov a prístupov k informáciám 23
8.3.6 Riadenie technických zraniteľností a záplat 23
8.4 KOMUNIKAČNÁ BEZPEČNOSŤ 23
8.4.1 Bezpečnosť sietí 23
8.4.2 Zabezpečenie prenosu informácií 24
8.4.3 Vzdialený prístup 24
8.5 ROZVOJ A ÚDRŽBA IKT 24

8.5.1 Vývoj systémov *24*
8.5.2 Ochrana testovacích údajov *24*
8.5.3 Riadenie zmien *25*
8.6 FYZICKÁ BEZPEČNOSŤ A BEZPEČNOSŤ IKT PROSTRIEDKOV 25
8.6.1 Bezpečnosť IKT prostriedkov *25*
8.6.2 Kontrola pohybu cudzích osôb v priestoroch ŽSR *25*
8.6.3 Požiarna ochrana priestorov ŽSR *26*
8.6.4 Aplikácia pravidla čistého stola a čistej obrazovky *26*
8.7 RIADENIE KONTINUITY ČINNOSTÍ 26
8.8 VÝKON PRÁC TRETÍMI STRANAMI 26
8.9 RIADENIE BEZPEČNOSTNÝCH INCIDENTOV 27
8.10 ZABEZPEČENIE SÚLADU 28
8.10.1 Súlad s legislatívnymi a zmluvnými požiadavkami *28*
8.10.2 Ochrana autorských práv *28*
8.10.3 Kryptografické opatrenia *28*
9. PRÍLOHY 29

PREHLÁSENIE VEDENIA ŽSR

k vydaniu tohto dokumentu

Dňom nadobudnutia účinnosti tohto dokumentu, Železnice Slovenskej republiky prijali zásady na dosiahnutie potrebnej úrovne bezpečnosti informačných aktív Železníc Slovenskej republiky a zámer na:

- stanovenie rámca riadenia bezpečnosti,
- na zabezpečenie chodu prevádzky všetkých IS a sietí Železníc Slovenskej republiky v požadovanom rozsahu a kvalite;
- na zabezpečenie vysokej trvalej dostupnosti aplikácií kritických z hľadiska zabezpečenia základných funkcií a základných služieb Železníc Slovenskej republiky;
- na zabránenie nenávratných strát údajov uchovávaných v IS; na zamedzenie prezradenia údajov pri prenosoch všetkými formami a
- na zamedzenie úniku údajov uložených na pamäťových médiách.

Vedenie Železníc Slovenskej republiky si uvedomuje potrebu riadiť bezpečnosť informácií a informačných aktív a z tohto dôvodu prijalo a zaväzuje sa presadzovať a dosahovať strategické ciele a princípy definované v tomto dokumente.

Vedenie Železníc Slovenskej republiky týmto deklaruje riadenie bezpečnosti KIS za neoddeliteľnú súčasť svojej činnosti, ktoré bude uskutočňované v zhode s týmto dokumentom.

V nadväznosti na tento dokument sa v rámci ŽSR vypracovávajú ďalšie IRA a usmerňujú jednotlivé činnosti zamestnancov Železníc Slovenskej republiky, ako aj zamestnancov tretích strán pri výkone ich činností pre Železnice Slovenskej republiky. Konanie v súlade s predpismi, alebo inými IRA a usmerneniami vydanými Železnicami Slovenskej republiky je vyžadované od všetkých tretích strán a je dohodnuté zmluvne.

1. ÚVOD

Bezpečnostná politika KIS ŽSR – skrátená politika pre tretie strany (ďalej iba „politika pre tretie strany“) vychádza z Bezpečnostnej politiky KIS ŽSR a predstavuje súhrn bezpečnostných zásad a pravidiel, ktorých cieľom je rámcové usmernenie činností tretích strán za účelom zabezpečenia chodu všetkých IS a sietí ŽSR v požadovanom rozsahu a kvalite, zabezpečiť vysokú dostupnosť aplikácií kritických z hľadiska zabezpečenia základných funkcií ŽSR, zabrániť nenávratným stratám údajov, zamedziť prezradeniu údajov pri prenosoch všetkými formami a zamedziť únikom údajov.

Železnice Slovenskej republiky sú organizácia, ktorá spravuje železničnú infraštruktúru vo vlastníctve štátu a zároveň zabezpečuje prepravné a dopravné služby, ktoré zodpovedajú záujmom štátnej dopravnej politiky a požiadavkám trhu vrátane súvisiacich činností, aj s náležitým zreteľom na

- dôležitosť informačných systémov a sietí (ďalej aj „IKT“), ktoré prevádzkuje, význam informácií, ktoré sú v nich spracúvané, hodnotu majetku a technológií, ktoré používa pre svoju činnosť, povinnosť chrániť ich a povinnosť ochraňovať oprávnené záujmy štátu a svojich klientov a všetkých osôb, s ktorými prichádza do kontaktu,
- potrebu bezpečnej prevádzky IKT podporujúcich zabezpečenie prepravných a dopravných služieb ako aj činností, ktoré s uvedeným súvisia,
- potrebu zavedenia bezpečnej elektronickej komunikácie s nadradenými orgánmi, partnerskými organizáciami, partnermi, dodávateľmi a klientmi, ako aj komunikácie s verejnosťou,
- a to, že ŽSR sú:
    - prevádzkovateľom prvkov kritickej infraštruktúry v zmysle zákona č. 45/2011 Z. z. Zákon o kritickej infraštruktúre (ďalej aj „ZoKI“),
    - prevádzkovateľom základných služieb v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej aj „ZoKB“),
    - prevádzkovateľom a sprostredkovateľom v oblasti spracúvania osobných údajov v zmysle platnej legislatívy pre oblasť osobných údajov (ďalej aj „GDPR“),
    - prevádzkovateľom komunikačnej infraštruktúry v súlade s požiadavkami zákona č. 351/2011 Z. z. o elektronických komunikáciách (ďalej aj „ZoEK“).

Tretie strany a ich zamestnanci musia svojou činnosťou prispievať k naplneniu vyššie uvedených potrieb ŽSR ako aj k zabezpečeniu kontinuálnej dôvernosti (zabrániť, aby nepovolaní ľudia získali informácie), integrite (zabrániť, aby informácie boli zmenené bez oprávnenia, úmyselne alebo náhodne) a dostupnosti (zabezpečiť, aby informácie boli k dispozícii, keď to je požadované) informačných aktív ŽSR a jej klientov.

1.1 Rámec pre riadenie bezpečnosti

ŽSR chápu bezpečnosť ako komplexný proces zaistenia ochrany informácií, IKT a prevádzky základných služieb počas celého ich životného cyklu prostredníctvom zavedenia vhodných pravidiel a implementácie primeraných bezpečnostných opatrení, a to v rôznych oblastiach ako sú:

- informačná bezpečnosť,
- kybernetická bezpečnosť,
- ochrana osobných údajov,
- bezpečnosť kritickej infraštruktúry,
- bezpečnosť elektronických komunikácií,
- fyzická bezpečnosť.

1.2 Strategické ciele ŽSR v oblasti bezpečnosti

Vedenie ŽSR prijalo a zaväzuje sa presadzovať strategické ciele a princípy v oblasti bezpečnosti:

1. Riadiť bezpečnosť v súlade s požiadavkami platných právnych predpisov a právne záväzných aktov EÚ, s relevantnými regulačnými požiadavkami a s príslušnými bezpečnostnými štandardami, ako aj odporúčaniami z praxe a zabezpečiť jej trvalé zvyšovanie vo všetkých procesoch ŽSR.
2. Chrániť práva a záujmy štátu, nadriadených orgánov, partnerských organizácií, zamestnancov, klientov a dodávateľov ŽSR v oblasti bezpečnosti, implementovaním efektívnych a účinných bezpečnostných mechanizmov a opatrení.
3. Zvyšovať bezpečnostné povedomie zamestnancov a prostredníctvom vzdelávacieho programu ich systematicky viesť a motivovať k zlepšovaniu a dodržiavaniu bezpečnostných zásad pri výkone svojej práce.
4. Zabezpečiť dôvernosť, dostupnosť a integritu informácií a informačných aktív ŽSR, jeho klientov a partnerských organizácií pri ich spracúvaní.
5. Zaistiť bezpečnosť, spoľahlivosť a kvalitu prevádzkovaných prostriedkov IKT a využívaním moderných informačných technológií a ich postupným zlepšovaním a zefektívňovaním.
6. Vytvoriť podmienky na bezpečné umiestnenie jednotlivých prostriedkov IKT v závislosti na ich dôležitosti a zabezpečiť ich fyzickú ochranu a ochranu pred vplyvmi okolitého prostredia.
7. Chrániť dobré meno a dôveryhodnosť ŽSR a zabezpečiť vysokú kvalitu poskytovaných služieb.
8. Zabezpečiť realizáciu činností v oblasti hlásenia a reakcie na bezpečnostné incidenty a vykonávanie činností s dôrazom na prevenciu ich opätovného výskytu.
9. Trvale zvyšovať nároky na bezpečnostné opatrenia vo všetkých oblastiach bezpečnosti. Zdokonaľovať zavedené bezpečnostné opatrenia, trvalo zlepšovať ich efektívnosť v súlade s novými požiadavkami na poskytovanie služieb a vytvoriť organizačné podmienky na zaistenie bezpečnosti.

1.3 Používanie politiky pre tretie strany

Politika pre tretie strany definuje základnú štruktúru všetkých bezpečnostných procesov a mechanizmov, ktoré tretie strany musia dodržiavať pri výkone svojich činností pre ŽSR.

Politika pre tretie strany je platná pre všetky tretie strany a ich zamestnancov vykonávajúcich činnosti pre ŽSR. Tretie strany a ich zamestnanci sú povinní plniť všetky požiadavky tejto politiky, a to vo vzťahu k tým činnostiam, ktoré tretie strany zabezpečujú pre ŽSR.

Všetky prípadné výnimky z tejto politiky musia byť schválené Manažérom informačnej a kybernetickej bezpečnosti ŽSR, zdokumentované a tretej strane preukázateľne oznámené.

Požiadavky Bezpečnostnej politiky KIS ŽSR sú v primeranom rozsahu rozpracované prostredníctvom interných riadiacich aktov ŽSR (smernice, predpisy). Tretie strany a ich zamestnanci sú povinní dodržiavať okrem tejto politiky pre tretie strany aj všetky tie interné riadiace akty ŽSR, s ktorými bola tretia strana alebo jej zamestnanci preukázateľne oboznámení. Pokiaľ interný riadiaci akt ŽSR stanovuje bezpečnostné pravidlá a požiadavky konkrétnejšie, sú tretie strany, resp. jej zamestnanci povinní dodržiavať bezpečnostné pravidlá a požiadavky uvedené v týchto riadiacich aktoch.

2. ZÁKLADNÉ POJMY A SKRATKY

2.1 Zoznam základných pojmov

Aktívum	Aktívum je čokoľvek, čo má pre ŽSR alebo pre základnú službu, ktorú ŽSR poskytuje nejakú hodnotu. Pod aktívom rozumieme napr. hardvér, softvér, komunikačnú a technologickú infraštruktúru, budovy, používateľov systémov, údaje, know-how a pod.
Vlastník aktíva	Je spravidla vedúci útvaru alebo odboru ŽSR, ktorý zodpovedá za zverené aktívum počas jeho celého životného cyklu.
Informácia	Zmysluplný údaj – databázy a dátové súbory, zmluvy a dohody, systémová dokumentácia, informácie z výskumu, používateľské príručky, školiaci materiál, prevádzkové a podporné procedúry, plány zachovania kontinuity činnosti, záložné dohody, auditné záznamy a archivované informácie.
Informačná bezpečnosť	Zachovanie primeranej úrovne dôvernosti, dostupnosti a integrity aktíva. Informačná bezpečnosť sa dosahuje implementáciou vhodnej sady bezpečnostných opatrení.
Kybernetická bezpečnosť	Je stav, v ktorom sú siete a IS schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a IS.
Dôvernosť	Je vlastnosť, ktorá charakterizuje, že údaje alebo informácie nie sú sprístupnené alebo odhalené neoprávneným osobám alebo procesom.
Integrita	Je vlastnosť, ktorá charakterizuje bezchybnosť, úplnosť a celistvosť informácií, ktoré boli odoslané, prijaté alebo uchované. Integrita zaručuje bezchybnosť, úplnosť alebo správnosť informácií.
Prístupnosť (dostupnosť)	Je vlastnosť, ktorá charakterizuje, že informácie alebo aktíva sú autorizovaným subjektom dostupné len s nevyhnutným zdržaním. Dostupnosť zaručuje, že informácie alebo aktíva budú prístupné na správnom mieste v správnom čase alebo, že daná udalosť nastane do určenej doby.
Zraniteľnosť	Slabé miesto aktíva, alebo opatrenia, cez ktoré sa môže realizovať hrozba.
Hrozba	Hrozba je každá úmyselná alebo neúmyselná udalosť, alebo stav, ktorý môže ohroziť aktívum.

Riziko	Potenciál, že určitá hrozba využije zraniteľnosť používaného aktíva a spôsobí jeho stratu alebo poškodenie.
Analýza rizík	Systematická kontrola všetkých zraniteľných miest so stanovením pravdepodobnosti a vyčíslením následkov ich možného ohrozenia. Výstupom je návrh bezpečnostných opatrení.
Autentifikácia	Proces overenia identity. Uistenie sa, že konkrétny používateľ (proces, komponent, systém) je skutočne ten za koho sa prehlasuje.
Autorizácia	Určenie, že daný subjekt je dôveryhodný a oprávnený na vykonávanie definovanej činnosti.
Bezpečnostné opatrenie	Technický, personálny alebo administratívny prvok ochrany, ktorého účelom je udržiavať bezpečný a spoľahlivý výkon bezpečnostnej politiky. Mechanizmus, ktorý znižuje zraniteľnosť IS voči určitej hrozbe
Dopad	Je výsledok pôsobenia realizovanej hrozby. Úroveň dopadu straty dôvernosti, dostupnosti a integrity na aktíva organizácie je definovaná úrovňou požiadaviek na aktívum a hodnotou aktíva.
Bezpečnostný audit	Kontrolná činnosť zameraná na dodržiavanie bezpečnostnej politiky a ustanovení bezpečnostnej legislatívy.
Bezpečnostné požiadavky	Určujú typ a stupeň ochrany potrebnej na dosiahnutie bezpečnostnej úrovne organizácie
Fyzická bezpečnosť	Je systém opatrení slúžiacich na ochranu pred nepovolanými osobami a pred neoprávnenou manipuláciou, ale aj pred fyzickým poškodením chránených zariadení. Predstavuje mechanické alebo elektronické prostriedky zamedzujúce neautorizovanému prístupu k zariadeniam alebo dátam (zámky, mreže), požiarne zariadenia, alarmy a pod.,
Záznam	Dokument opisujúci dosiahnuté výsledky alebo poskytujúci dôkaz vykonaných činností.
Informačný systém	Funkčný celok zabezpečujúci cieľavedomé a systematické získavanie, zhromažďovanie, ukladanie, spracúvanie, poskytovanie, sprístupňovanie, prenos, archiváciu a likvidáciu údajov prostredníctvom technických a programových prostriedkov.
Škodlivý kód	Je taký kód, ktorý bol vyvinutý s úmyslom vytvoriť škodu. Tento kód zahŕňa vírusy, červy, trójske kone a ostatný škodlivý SW,

Kritická infraštruktúra	Je systém, ktorý sa člení na sektory a prvky. Sektorom kritickej infraštruktúry sa rozumie časť kritickej infraštruktúry, do ktorej sa zaraďujú prvky; sektor môže obsahovať jeden alebo viac podsektorov kritickej infraštruktúry. Prvkom kritickej infraštruktúry sa rozumie najmä inžinierska stavba, služba vo verejnom záujme a informačný systém v sektore kritickej infraštruktúry, ktorých narušenie alebo zničenie by malo podľa sektorových kritérií a prierezových kritérií závažné nepriaznivé dôsledky na uskutočňovanie hospodárskej a sociálnej funkcie štátu, a tým na kvalitu života obyvateľov z hľadiska ochrany ich života, zdravia, bezpečnosti, majetku, ako aj životného prostredia.
Personálna bezpečnosť	Je systém bezpečnostných opatrení súvisiacich s výberom, určením, školením a kontrolou osôb.
Bezpečnostné incidenty	Akýkoľvek spôsob narušenia bezpečnosti informačných systémov verejnej správy, ako aj akékoľvek porušenie bezpečnostnej politiky povinnej osoby a pravidiel súvisiacich s bezpečnosťou informačných systémov verejnej správy.
Prostriedky IKT	Všetky programové, komunikačné a iné technické prostriedky, ktoré slúžia na spracúvanie údajov (informačný systém, infraštruktúra, siete, PC, notebooky a pod.)
Plán kontinuity činností	Súbor dokumentovaných postupov zahŕňajúci všetky činnosti potrebné na zabezpečenie nepretržitej dodávky služieb a produktov na požadovanej úrovni v prípade výskytu mimoriadnej udalosti.
Tretia strana	Spoločný názov pre fyzické a právnické osoby, ktoré žiadajú/získajú prístup do IS ŽSR, resp. siete internet, nie sú zamestnancami ŽSR a nemajú uzavretú so ŽSR zmluvu, ktorá ich na takýto prístup oprávňuje. Tretia strana je povinná dodržiavať zásady bezpečnosti a ďalšie povinnosti v zmysle tejto smernice, a túto skutočnosť je povinná potvrdiť podpísaním jej príslušných príloh.
Auditný záznam	Je informácia zaznamenaná (evidovaná) systémom, obsahujúca údaje o čase a aktivite systému, programových prostriedkov alebo používateľa (použitie prístupových práv, pokusy o prístup k súborom alebo objektom a pod.).
Bezpečnosť	Pre potreby tejto bezpečnostnej politiky je bezpečnosť vnímaná ako spoločné pomenovanie pre informačnú a kybernetickú bezpečnosť, personálnu a fyzickú bezpečnosť, bezpečnosť kritickej infraštruktúry, bezpečnosť osobných údajov a bezpečnosti elektronických komunikácií.

Osobné údaje	Sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby; identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, on-line identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.
Sprostredkovateľ	Je subjekt, ktorý spracúva osobné údaje v mene ŽSR (napr. získava osobné údaje v mene ŽSR, prevádzkuje softvérový systém ŽSR obsahujúci osobné údaje).
Koordinátor zmluvného vzťahu	Koordinátor zmluvného vzťahu je osoba, ktorá zabezpečuje primárne kontakt s treťou stranou a/alebo riadi činnosť zamestnanca alebo skupiny zamestnancov tretej strany Koordinátorom zmluvného vzťahu v prípade projektov je projektový/produktový manažér príslušného IS. V ostatných prípadoch je ním spravidla vedúci toho organizačného útvaru, ktorý zodpovedá za spoluprácu s treťou stranou.

2.2 Zoznam použitých skratiek

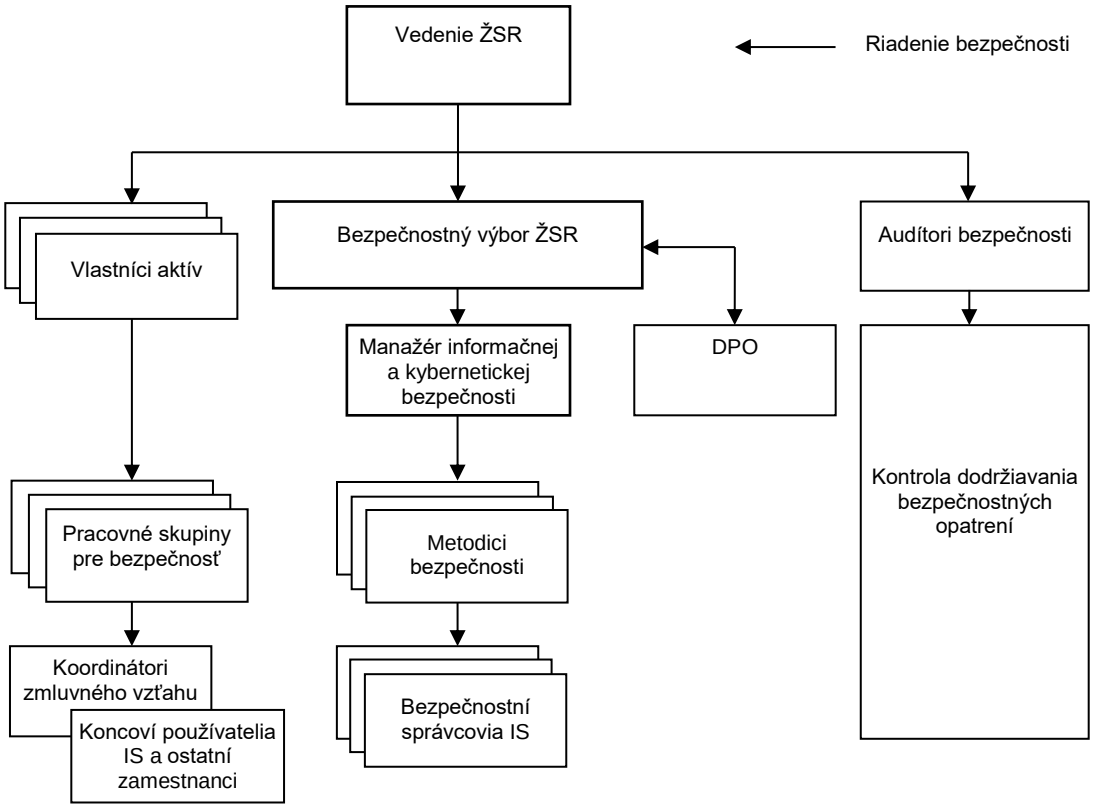
GDPR - General Data Protection Regulation – Nariadenie o ochrane osobných údajov
IS - informačný systém
SW - programové vybavenie komunikačných a informačných systémov
ŽSR - Železnice Slovenskej republiky
IKT - informačné a komunikačné technológie
EÚ - Európska únia
ŽT - železničné telekomunikácie
ZoKI - zákon č. 45/2011 Z. z. o kritickej infraštruktúre
ZoEK - zákon č. 351/2011 Z. z. o elektronických komunikáciách
ZoKB - zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.
OÚ - osobné údaje
MIKB - manažér informačnej a kybernetickej bezpečnosti
EPS - elektronická požiarna signalizácia
DPO - osoba zabezpečujúca dohľad nad spracúvaním osobných údajov
OKRaO - odbor krízového riadenia a ochrany
VOJ - vnútorná organizačná jednotka
GR - Generálne riaditeľstvo

3. ORGANIZÁCIA A RIADENIE BEZPEČNOSTI NA ŽSR

3.1 Organizácia bezpečnosti na ŽSR

Štruktúra organizácie bezpečnosti ŽSR definuje jednotlivé organizačné zložky, roly a funkcie, ktoré sú potrebné na spoľahlivé a efektívne fungovanie systému riadenia bezpečnosti a funkčné väzby medzi nimi. Organizácia bezpečnosti ŽSR je zobrazená na obrázku 3.1 uvedenom nižšie.

Tretie strany a ich zamestnanci sú povinní rešpektovať organizáciu bezpečnosti ŽSR a poskytovať súčinnosť jednotlivým organizačným zložkám, rolám a funkciám pri plnení ich povinností.



Obr. 3.1 Organizácia riadenia bezpečnosti v ŽSR

3.1.1 Úroveň stratégie a riadenia

Vedenie ŽSR

Úlohou Vedenia ŽSR v oblasti bezpečnosti je zabezpečovanie podpory bezpečnostným iniciatívam na všetkých úrovniach riadenia ŽSR a to najmä zabezpečovaním potrebných zdrojov (finančných, personálnych a materiálnych).

Bezpečnostný výbor ŽSR (BV ŽSR)

Hlavnou úlohou Bezpečnostného výboru ŽSR je podpora riadenia bezpečnosti a iniciatív v oblasti bezpečnosti na ŽSR. Bezpečnostný výbor ŽSR navrhuje a prijíma rozhodnutia týkajúce sa stratégie bezpečnosti, riadenia bezpečnostných rizík a implementácie bezpečnostných mechanizmov na ŽSR.

Manažér informačnej a kybernetickej bezpečnosti (MIKB)

Manažér informačnej a kybernetickej bezpečnosti zodpovedá za koordináciu informačnej a kybernetickej bezpečnosti na ŽSR. Spolupracuje s Bezpečnostným výborom ŽSR a je ním metodicky riadený.

Metodici bezpečnosti

Metodici bezpečnosti podporujú manažéra informačnej a kybernetickej bezpečnosti pri výkone jeho funkcií a zodpovedajú za podporu v oblasti riadenia bezpečnosti. Spolupracujú pri implementácii opatrení v oblasti riadenia bezpečnosti. Metodicky usmerňujú vlastníkov informačných aktív, koordinátorov zmluvných vzťahov a administrátorov bezpečnosti a IS pri výkone ich činností (v oblastiach súvisiacich s bezpečnosťou).

Zodpovedná osoba za ochranu osobných údajov (DPO)

Zodpovedná osoba za ochranu osobných údajov je zodpovedná osoba v zmysle platnej legislatívy v oblasti ochrany osobných údajov, ktorá zodpovedá za presadzovanie a implementáciu požiadaviek v oblasti ochrany osobných údajov na ŽSR.

3.1.2 Úroveň prevádzky a realizácie

Bezpečnostní správcovia IS

Bezpečnostní správcovia IS zabezpečujú správu a údržbu bezpečnostných mechanizmov IS, priebežné monitorovanie stavu bezpečnosti IS a podávanie správ o jej stave. Pri vzniku bezpečnostných incidentov aplikujú bezpečnostné opatrenia podľa príslušných predpisov a zabezpečujú podporu pri ich vyšetrovaní a zabezpečovaní dôkazov.

Bezpečnostní správcovia IS spolupracujú s MIKB a s metodikmi bezpečnosti a sú nimi metodicky riadení.

Vlastníci aktív

Jednotlivec alebo entita, ktorá prijala manažérsku zodpovednosť za kontrolu výroby, vývoja, údržby, použitia a bezpečnosť aktíva. Vlastníci aktív zodpovedajú za špecifikáciu bezpečnostných požiadaviek na aktíva (spravidla na ich dôvernosť, dostupnosť a integritu) a ich požadovanú úroveň v súlade s riadiacimi dokumentmi v oblasti bezpečnosti.

Koordinátori zmluvného vzťahu

Koordinátor zmluvného vzťahu je osoba, ktorá zabezpečuje primárne kontakt s treťou stranou a riadi činnosť zamestnanca alebo skupiny zamestnancov tretej strany.

Pracovné skupiny pre bezpečnosť

S cieľom koordinovať aktivity v jednotlivých oblastiach bezpečnosti a zabezpečenia súladu s požiadavkami bezpečnostných štandardov a legislatívnymi požiadavkami v jednotlivých oblastiach bezpečnosti sú vytvárané pracovné skupiny pre bezpečnosť.

Koncoví používatelia IS a ostatní zamestnanci

Koncoví používatelia IS a ostatní zamestnanci sú osoby, ktoré pristupujú alebo používajú informačné aktíva ŽSR.

3.1.3 Úroveň kontroly a auditu

Audítor bezpečnosti

Audítor bezpečnosti predstavuje kontrolnú zložku riadenia bezpečnosti na ŽSR. Audítor bezpečnosti zodpovedá za overovanie a posudzovanie implementácie a dodržiavania Bezpečnostnej politiky KIS ŽSR, platných interných riadiacich aktov v rámci všetkých organizačných útvarov, prípravu a sumarizáciu podkladov v oblasti bezpečnosti potrebných na spracovanie správy o stave bezpečnosti.

Súčasne je audítor bezpečnosti oprávnený overovať a posudzovať úroveň dodržiavania požiadaviek tejto politiky pre tretie strany tretími stranami a ich zamestnancami, ako aj dodržiavanie ostatných relevantných interných riadiacich aktov a zmluvných požiadaviek tretími stranami.

Kontrola dodržiavania bezpečnostných opatrení

Kontrolu dodržiavania zavedených bezpečnostných opatrení na úrovni prevádzky a realizácie vykonávajú v rámci svojich kompetencií všetci zamestnanci s pridelenými bezpečnostnými rolami (MIKB, metodici bezpečnosti, koordinátori zmluvného vzťahu, ...), vedúci zamestnanci a vlastníci aktív.

Za kontrolu tretích strán v oblasti dodržiavania bezpečnostných opatrení zodpovedajú príslušní koordinátori zmluvného vzťahu.

3.2 Riadenie bezpečnostných rizík

Určenie primeraných bezpečnostných opatrení vyžaduje spracovanie analýzy a ohodnotenie bezpečnostných rizík. Analýzou bezpečnostných rizík sa určuje pravdepodobnosť vzniku škodlivej udalosti, ktorá môže byť spôsobená zneužitím existujúcej zraniteľnosti aktíva potenciálnou hrozbou v spojitosti s existujúcimi bezpečnostnými opatreniami a identifikáciou dopadov pri narušení dôvernosti, integrity alebo dostupnosti aktíva.

Ohodnotenie bezpečnostných rizík musí byť vykonané vzhľadom na bezpečnostné požiadavky a definované strategické ciele ŽSR v oblasti bezpečnosti, ako aj vzhľadom na bezpečnostné požiadavky vyplývajúce z okolitého prostredia (napr. legislatíva, nadriadené orgány, partnerské organizácie, používatelia, tretie strany) s dôrazom na priority a nároky na dostupnosť, dôvernosť a integritu jednotlivých informačných aktív.

Tretie strany sú povinné prispievať k riadeniu bezpečnostných rizík, a to najmä tým, že:

- bezodkladne informujú zástupcov ŽSR (spravidla koordinátorov zmluvných vzťahov za ŽSR) o spozorovaných bezpečnostných rizikách,
- vykonávajú svoje činnosti spôsobom, ktorý predchádza vzniku bezpečnostných rizík,
- poskytujú svoje služby v súlade s touto politikou, internými riadiacimi aktami ŽSR, s požiadavkami platnej legislatívy a s bezpečnostnými štandardami,
- poskytujú vstupy pre monitorovanie, meranie a vyhodnocovanie efektivity implementovaných bezpečnostných opatrení
- poskytujú súčinnosť pri posudzovaní príčin vzniku bezpečnostných rizík a pri ich eliminovaní.

4. RIADENIE OCHRANY KYBERNETICKEJ BEZPEČNOSTI

Cieľom riadenia ochrany kybernetickej bezpečnosti je zabezpečenie kybernetickej bezpečnosti pre IS a siete podporujúce poskytovanie základných služieb ŽSR v súlade so zákonom č. 69/2018 Z.z. o kybernetickej bezpečnosti a súvisiacimi vyhláškami (ďalej aj „ZoKB“).

Oblasť kybernetickej bezpečnosti je na ŽSR zabezpečovaná VOJ Železničné telekomunikácie. V rámci ŽSR je vymenovaná osoba zodpovedná za koordináciu ochrany informačnej a kybernetickej bezpečnosti – Manažér informačnej a kybernetickej bezpečnosti (MIKB).

Tretie strany a ich zamestnanci sú povinní poskytovať MIKB podporu pri plnení jej úloh súvisiacich s ochranou IS a sietí podporujúcich základné služby ŽSR a ostatných informačných aktív ŽSR.

S tretími stranami, ktoré pre ŽSR vykonávajú činnosti, ktoré priamo súvisia s prevádzkou sietí a informačných systémov podporujúcich základné služby ŽSR je ŽSR povinné uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa ZoKB. Uvedené platí aj v prípade podnikov zabezpečujúcich poskytovanie elektronických komunikačných služieb alebo sietí v zmysle ZoEK. Tieto tretie strany sú povinné prijať bezpečnostné opatrenia definované aj v zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností.

Tretie strany a ich zamestnanci sú pri výkone svojich činností pre ŽSR povinní dodržiavať požiadavky ZoKB, požiadavky stanovené v zmluvách so ŽSR, ako aj

požiadavky uvedené v interných riadiacich aktoch ŽSR a konať tak, aby nebola narušená bezpečnosť IS a sietí, ktoré ŽSR prevádzkuje.

Každý zamestnanec tretej strany je v prípade spozorovania porušenia ochrany IS alebo siete, alebo iného informačného aktíva ŽSR, alebo v prípade spozorovania aktivít, ktoré by mohli k uvedenému smerovať, povinný o tom bezodkladne informovať určeného zamestnanca ŽSR (spravidla koordinátora zmluvného vzťahu).

5. RIADENIE OCHRANY OSOBNÝCH ÚDAJOV

Cieľom riadenia ochrany osobných údajov je zabezpečenie ochrany súkromia a údajov spracúvaných o dotknutých osobách v súlade s požiadavkami platných právnych predpisov a právne záväzných aktov EÚ.

ŽSR sa zaväzuje spracúvať osobné údaje zamestnancov tretích strán ako aj osobné údaje ostatných dotknutých osôb v súlade s požiadavkami Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej aj „GDPR“).

Na zabezpečenie naplnenia požiadaviek GDPR prijali ŽSR vhodné bezpečnostné opatrenia. Tie zabezpečujú primeranú bezpečnosť osobných údajov, a to najmä ich ochranu pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením.

Tretia strana, ktorá bude spracúvať osobné údaje v mene ŽSR a z pohľadu GDPR vystupuje v pozícií sprostredkovateľa pre spracúvanie osobných údajov, je povinná pred začatím spracovávania osobných údajov uzatvoriť so ŽSR sprostredkovateľskú zmluvu o spracúvaní osobných údajov v zmysle GDPR.

Tretie strany a ich zamestnanci sú pri vykonávaní spracúvania osobných údajov v mene ŽSR alebo pri náhodnom prístupe k osobným údajom povinní dodržiavať požiadavky GDPR, požiadavky stanovené v zmluvách s tretími stranami, ako aj požiadavky uvedené v Metodickom usmernení riaditeľa odboru 130 GR ŽSR k opatreniam na zabezpečenie ochrany osobných údajov a konať tak, aby nebola narušená bezpečnosť spracúvaných osobných údajov.

V rámci ŽSR je vymenovaná osoba zodpovedná za ochranu osobných údajov, ktorá zabezpečuje koordináciu všetkých aktivít súvisiacich s ochranou osobných údajov. Kontaktné údaje na túto osobu sú zverejnené na web stránke ŽSR.

Tretie strany a ich zamestnanci sú povinní poskytovať osobe zodpovednej za ochranu osobných údajov na ŽSR podporu pri plnení jej úloh súvisiacich s ochranou osobných údajov.

Každý zamestnanec tretej strany je v prípade spozorovania porušenia ochrany osobných údajov alebo v prípade spozorovania aktivít, ktoré by mohli k uvedenému smerovať, povinný o tom bezodkladne informovať určeného zamestnanca ŽSR (spravidla koordinátora zmluvného vzťahu).

6. RIADENIE OCHRANY KRITICKEJ INFRAŠTRUKTÚRY

Cieľom riadenia ochrany kritickej infraštruktúry je zabezpečiť ochranu všetkých prvkov kritickej infraštruktúry, ktoré ŽSR prevádzkuje.

Oblasť kritickej infraštruktúry upravuje zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov (ďalej aj „ZoKI“). Oblasť ochrany kritickej infraštruktúry je na ŽSR zabezpečovaná útvarmi krízového riadenia a ochrany a je vykonávaná určenými bezpečnostnými zamestnancami OKRaO v súlade s platnou legislatívou.

Tretie strany a ich zamestnanci musia pri výkone svojich činností dodržiavať požiadavky ZoKI, požiadavky stanovené v zmluvách s tretími stranami, ako aj požiadavky interných riadiacich aktov ŽSR a konať tak, aby nebola narušená kritická infraštruktúra, ktorú ŽSR prevádzkuje. V prípade spozorovania ohrozenia kritickej infraštruktúry alebo v prípade spozorovania aktivít, ktoré by mohli k uvedenému smerovať, sú povinní o tom bezodkladne informovať určeného zamestnanca ŽSR (spravidla koordinátora zmluvného vzťahu).

7. RIADENIE OCHRANY ÚDAJOV SPADAJÚCICH POD ZÁKON Č. 351/2011 Z. Z. O ELEKTRONICKÝCH KOMUNIKÁCIÁCH

Cieľom riadenia ochrany údajov spadajúcich pod zákon č. 351/2011 Z. z. o elektronických komunikáciách (ďalej aj „ZoEK“) je zabezpečenie ochrany komunikačných sietí a elektronických komunikačných služieb.

Oblasť elektronických komunikácií upravuje ZoEK. Oblasť ochrany elektronických komunikácií spadá pod VOJ Železničné telekomunikácie. V súlade s platnými právnymi predpismi musia byť prijaté bezpečnostné opatrenia na ochranu elektronických komunikácií a elektronických komunikačných sietí. Musia byť prijaté a dodržiavané zodpovedajúce technické, personálne a organizačné opatrenia na ochranu bezpečnosti sietí a služieb, ktoré s ohľadom na stav techniky musia zabezpečiť úroveň bezpečnosti, ktorá je primeraná existujúcemu riziku. ŽSR musí udržiavať integritu svojich sietí s cieľom zaručiť kontinuitu poskytovania služieb prostredníctvom týchto sietí. V rámci povinností a zodpovedností vyplývajúcich z uvedeného zákona musí byť poskytovaná súčinnosti relevantným orgánom v zmysle platných právnych predpisov.

Tretie strany a ich zamestnanci musia pri výkone svojich činností dodržiavať požiadavky ZoEK, požiadavky stanovené v zmluvách s tretími stranami, ako aj požiadavky interných riadiacich aktov ŽSR a konať tak, aby bola zabezpečená ochrana elektronických komunikácií, ktoré ŽSR prevádzkujú. V prípade spozorovania

ohrozenia bezpečnosti elektronických komunikácií alebo v prípade spozorovania aktivít, ktoré by mohli k uvedenému smerovať, sú povinní o tom bezodkladne informovať určeného zamestnanca ŽSR (spravidla koordinátora zmluvného vzťahu).

8. ZÁKLADNÉ BEZPEČNOSTNÉ ZÁSADY A PRINCÍPY

8.1 Personálna bezpečnosť

8.1.1 Výkon činností zamestnancami tretích strán

V oblasti personálnej bezpečnosti je nevyhnutné, aby všetci zamestnanci tretích strán dodržiavali zásady tejto politiky pre tretie strany a využívali zverené informačné aktíva výhradne iba na účely výkonu ŽSR zazmluvnených činností.

Zamestnanci tretích strán musia byť najneskôr pred začatím výkonu činností pre ŽSR preverení, či spĺňajú zmluvne definované požiadavky na svoju kvalifikáciu a odborné znalosti a či sú spôsobilí vykonávať požadovanú činnosť. Z uvedeného dôvodu je tretia strana povinná viesť dokumentované záznamy o kvalifikácii, odborných znalostiach, školeniach svojich zamestnancov a na žiadosť ŽSR je povinná uvedenú dokumentáciu predložiť k nahliadnutiu.

Tretie strany sú povinné viesť evidenciu svojich zamestnancov a v prípade ukončenia pracovného pomeru s niektorým z týchto zamestnancom alebo v prípade ukončenia výkonu činností týchto zamestnancov pre ŽSR, sú povinné bezodkladne o tom informovať koordinátora zmluvného vzťahu. Tretia strana je povinná takúto evidenciu zamestnancov doručiť ŽSR v zmysle zmluvne dohodnutých lehôt.

Všetci zamestnanci tretích strán s prístupom k citlivým informáciám musia byť preukázateľne zaviazaní mlčanlivosťou, a to ešte pred umožnením prístupu zamestnancom tretích strán k daným informáciám. Mlčanlivosť zamestnancov tretích strán zabezpečuje ochranu hmotného aj duševného vlastníctva ŽSR. Mlčanlivosť musí byť zabezpečená od vzniku zmluvného vzťahu až po jeho zánik a rovnako aj po skončení zmluvného vzťahu.

ŽSR sú oprávnené vykonávať kontrolu zamestnancov tretích strán v oblasti dodržiavania bezpečnostných politík a interných riadiacich aktov pri výkone činností pre ŽSR. Zamestnanci tretích strán sú povinní poskytnúť zamestnancom vykonávajúcim audit alebo kontrolu náležitú súčinnosť.

Zamestnancom tretích strán, ktorí končia výkon prác pre ŽSR, musia byť v dostatočnom predstihu, najneskôr ku dňu skončenia výkonu prác pre ŽSR odobraté prístupové práva k dôležitým prostriedkom IKT a k citlivým informačným aktívam a zadokumentované vrátenie všetkých zverených aktív. Z tohto dôvodu je tretia strana povinná bezodkladne v predstihu informovať ŽSR o takýchto zamestnancoch. Tretia strana je povinná najneskôr do 14 dní od skončenia trvania zmluvy vrátiť, alebo previesť na ŽSR všetky informácie a aktíva, ktoré mala na základe zmluvy.

8.1.2 Poskytnutie informácií zamestnancom tretích strán

Ak si to charakter vykonávanej činnosti bude vyžadovať, zamestnanci tretích strán musia byť informovaní o svojich povinnostiach a zodpovednostiach aj prostredníctvom ďalších interných riadiacich aktov ŽSR, ktoré usmernia ich činnosť. Tieto informácie môžu byť zamestnancom tretích strán poskytnuté:

- oboznámením s príslušným interným riadiacim aktom, alebo
- poučením zamestnanca.

Zamestnanci tretích strán sú povinní dodržiavať povinnosti a pravidlá výkonu činností stanovených zmluvou, v tejto politike ako aj v ďalších interných riadiacich aktoch, o ktorých bola tretia strana preukázateľne informovaná.

Prípad, ak zamestnanec tretej strany poruší povinnosti vyplývajúce zo zmluvy, ako aj tejto politiky alebo z internej riadiacej dokumentácie, s ktorou bol preukázateľne oboznámený, môže byť po zohľadnení všetkých objektívnych faktorov a zozbieraných dôkazov považované za porušenie zmluvného vzťahu a zamestnanec tretej strany, resp. tretia strana postihnutá sankciami definovanými zmluvou.

Každý zamestnanec tretej strany musí prejsť najneskôr pred začatím výkonu prác pre ŽSR primeraným poučením, ktorého predmetom sú okrem iného aj povinnosti a pravidlá výkonu činností stanovených zmluvou medzi ŽSR a treťou stranou, touto politikou, ako aj v ďalšími internými riadiacimi aktami, o ktorých bola tretia strana preukázateľne informovaná. Uvedené poučenie svojho zamestnanca zabezpečí tretia strana, pričom o tom vyhotoví preukázateľný záznam.

8.2 Riadenie prístupu

8.2.1 Zásady riadenia prístupu tretím stranám

Prístup zamestnancov tretích strán k dôležitým aktívam ŽSR môže byť povolený len v nevyhnutných prípadoch a len za účelom realizácie dohodnutých prác. Pri prideľovaní prístupových práv sa musia preverovať prevádzkové a bezpečnostné potreby.

Každý zamestnanec tretej strany musí mať umožnený len taký rozsah fyzického a logického prístupu k informačným aktívam ŽSR, ktorý postačuje na vykonávanie pridelených úloh a dodržanie zmluvného vzťahu ale zároveň zabráni vykonávaniu iných neautorizovaných činností (princíp minimaxu).

Tretie strany sú povinné viesť evidenciu svojich zamestnancov, ktorí majú pridelený prístup do IKT prostriedkov ŽSR a v prípade ukončenia pracovného pomeru s niektorým z týchto zamestnancom alebo v prípade ukončenia výkonu činností týchto zamestnancov pre ŽSR, sú povinné bezodkladne o tom informovať koordinátora zmluvného vzťahu.

V súčinnosti s treťou stranou musia byť navrhnuté a implementované bezpečnostné opatrenia požadované touto politikou pre tretie strany a príslušnou internou riadiacou dokumentáciou ŽSR.

8.2.2 Riadenie prístupu do IS a sietí

V prípade prístupu do IS a sietí ŽSR sa vyžaduje identifikácia a autentifikácia každého používateľa. Každý používateľ musí mať pridelený jednoznačný identifikátor, ktorý je povinný používať pri prístupe do IS a sietí ŽSR.

Prístupom tretích strán do IS a sietí ŽSR sa rozumie:

- prístup do siete LAN ŽSR na akýkoľvek účel,
- prístup do akéhokoľvek IS prevádzkovaného na ŽSR,
- prístup do technologického zariadenia prevádzkovaného na ŽSR,
- prístup tretích strán z dôvodov správy, údržby, opravy nimi nasadeného, resp. dodaného IS, softvéru, aplikácie.

Prideľovanie prístupových práv pre zamestnancov tretích strán vrcholovo zastrešujú VOJ ŽT, ktoré musia na základe požiadavky písomne potvrdiť pridelenie oprávnenia na prístup do definovaného IS/siete/technologického zariadenia/SW resp. aktíva ŽSR. Zasielaná požiadavka musí obsahovať pravdivé a správne vyplnené údaje, za ktoré zodpovedá osoba žiadateľa, t. j. tretia strana.

Prístup zamestnancom tretích strán môže byť udelený iba na základe schválenej žiadosti o prístup do siete ŽSR, ktorú podáva žiadateľ v zmysle pravidiel uvedených v prílohe č. 1 tejto politiky.

Podmienkou schválenia žiadosti o pridelenie prístupu do IS alebo siete ŽSR je predloženie buď platnej Dohody o ochrane dôverných informácií a skutočností tvoriacich obchodné tajomstvo (Príloha č. 4 tejto politiky), ak bola uzavretá; alebo žiadateľom podpísaného Vyhlásenia o ochrane dôverných informácií získaných prístupom do IKT prostredia ŽSR (Príloha č. 3 tejto politiky). V prípade, ak už ŽSR má s treťou stranou podpísanú platnú zmluvu, ktorá obsahuje aj ochranu poskytovaných dôverných informácií, nie je potrebné a vhodné uzatvárať aj Dohodu o ochrane dôverných informácií a skutočností tvoriacich obchodné tajomstvo.

Zamestnancom tretích strán môže byť prístup pridelený maximálne na dobu 6 mesiacov a maximálne do ukončenia zmluvného vzťahu s treťou stranou alebo do ukončenia zmluvného vzťahu medzi treťou stranou a jej zamestnancom. Pri každej novej žiadosti o prístup (neplatí pre žiadosti o predĺženie prístupu) musí zamestnanec tretej strany pri tejto žiadosti o prístup predložiť vyhlásenie o ochrane dôverných informácií.

Prístup do verejného Internetu cez WIFI sieť prevádzkovanú ŽSR, na výkon výhradne pracovných činností pre ŽSR, nepodlieha schvaľovaciemu procesu. Takéto pripojenie pre tretiu stranu zabezpečuje koordinátor zmluvného vzťahu za ŽSR. Takýto prístup sa prideľuje na trvanie v požadovanom čase, maximálne však na 14 pracovných dní.

Každý zamestnanec tretej strany je povinný pri prístupe do IS a sietí ŽSR dodržiavať pravidlá uvedené v prílohe č. 2 tejto politiky.

8.3 Bezpečnosť prevádzky IKT prostriedkov

8.3.1 Prevádzka IKT prostriedkov

IKT prostriedky ŽSR musia byť tretími stranami prevádzkované v súlade s pravidlami platnými v ŽSR pre prevádzku IKT prostriedkov.

Zamestnanci tretích strán majú prísne zakázané obchádzať bezpečnostné mechanizmy nastavené v rámci IS a sietí.

8.3.2 Dokumentácia systémov

Pre všetky IKT prostriedky prevádzkované v ŽSR musí byť vypracovaná dokumentácia v štandardizovanom formáte. V prípade zmien týkajúcich sa IKT prostriedkov realizovaných tretími stranami, musí byť treťou stranou zabezpečená aktualizácia dokumentácie v rozsahu vykonaných zmien.

Zamestnanci tretích strán sú povinní manipulovať s dokumentáciou tak, aby bolo zabránené jej neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii.

8.3.3 Ochrana pred škodlivým kódom

Všetky IKT prostriedky patriace tretej strane, ktorými tretie strany pristupujú do IS a sietí ŽSR, musia byť chránené adekvátnymi a účinnými bezpečnostnými opatreniami na ochranu pred škodlivým kódom a na jeho detekciu. Nástroje na ochranu pred škodlivým kódom musia byť pravidelne aktualizované. Súčasne sa musia na týchto IKT prostriedkoch nachádzať iba bezpečný a výrobcom podporovaný operačný systém a aplikácie a musia byť implementované aktuálne bezpečnostné záplaty.

Zamestnanci tretích strán majú zakázané inštalovať alebo pripájať do sietí a IS ŽSR zariadenia a pamäťové médiá, ktoré neboli schválené ŽSR. Pred ich vložením do siete alebo IS ŽSR musí byť zabezpečené ich otestovanie voči prítomnosti škodlivému kódu.

8.3.4 Údržba a správa prevádzkových problémov

Všetky prostriedky IKT musia byť udržiavané zaškolenými osobami, ich opravy a servis musia byť vykonávané len ŽSR autorizovanými osobami.

V prípade identifikácie problému, musí zamestnanec tretej strany bezodkladne informovať určeného zamestnanca ŽSR. Súčasne je tretia strana povinná pri IKT prostriedkoch, ktorých prevádzku zabezpečuje, zabezpečiť v súlade s požiadavkami ŽSR detekciu, izolovanie, opravu a dokumentáciu chýb IKT prostriedkov.

8.3.5 Monitorovanie používania systémov a prístupov k informáciám

Všetky udalosti a aktivity tretích strán súvisiace s prevádzkou a bezpečnosťou (používanie prostriedkov IKT, prístupy k dôverným alebo inak citlivým informáciám a pod.) sú nepretržite monitorované, zaznamenávané a pravidelne vyhodnocované.

Zamestnanci tretích strán majú zakázané pokúšať sa obchádzať implementované bezpečnostné mechanizmy a deaktivovať monitorovacie mechanizmy.

Prístup zamestnancov tretích strán k IKT prostriedkom, využívaným na výkon činností pre ŽSR, musí byť riadený. Všetky udalosti a aktivity na IKT prostriedkoch tretích strán, ktoré tretie strany používajú na výkon činností pre ŽSR, musia byť nepretržite monitorované, zaznamenávané a vyhodnocované. Auditné záznamy týchto udalostí a aktivít musia byť zaznamenávané a uchovávané spôsobom, ktorý umožňuje, aby tieto záznamy boli k dispozícii ako dôkaz pre prípad vyšetrovania bezpečnostných incidentov.

8.3.6 Riadenie technických zraniteľností a záplat

Musí byť zabezpečený proces riadenia technických zraniteľností a implementácie bezpečnostných záplat a opravných balíkov pre všetky IKT prostriedky tretích strán, ktoré tretie strany používajú na výkon činností podporujúcich základné služby ŽSR. Tretia strana je povinná pravidelne v ročnom intervale detegovať zraniteľnosti všetkých takýchto programových a technických prostriedkov, ako aj ich častí. Okrem toho je povinná za účelom minimalizovania vzniku zraniteľností využívať verejne dostupné alebo výrobcom vytvárané zoznamy zraniteľností prostriedkov IKT.

Tretie strany zabezpečujúce podporu IKT prostriedkov ŽSR sú povinné bezodkladne informovať ŽSR o existencii bezpečnostných záplat alebo opravných balíkov, alebo existujúcich zraniteľností pre tieto IKT prostriedky.

8.4 Komunikačná bezpečnosť

8.4.1 Bezpečnosť sietí

Vonkajšie a vnútorné sieťové prostredie tretej strany, v ktorom sú umiestnené IKT prostriedky podporujúce základné služby ŽSR, musí byť chránené firewallom. Neoprávnené spojenia zo známych adries, označených ako škodlivé alebo spôsobujúce známe hrozby, musia byť blokované. Bezpečnosť sietí musí byť nepretržite monitorovaná a vyhodnocovaná.

Siete tretej strany, v ktorých sú umiestnené IKT prostriedky podporujúce základné služby ŽSR, musia byť oddelené od ostatných IKT prostriedkov prostredníctvom vhodných technológií, resp. umiestnené vo vyhradených segmentoch siete.
Prepojenia medzi takýmito segmentami siete a ostatnými sieťami môžu byť povoľované iba v nevyhnutných prípadoch a v súlade s princípom zásady najnižších privilégií.

Prístup používateľov k sieťam a IS musí byť riadený v súlade s požiadavkami pre riadenie prístupu v kapitole 8.2 Riadenie prístupu.

8.4.2 Zabezpečenie prenosu informácií

Prenos informácií a softvéru medzi ŽSR a tretími stranami musí prebiehať na základe zmluvy o výmene informácií, prípadne inej zdokumentovanej dohody medzi ŽSR a treťou stranou, kde budú definované jednotlivé požiadavky na prenos informácií.

Ak sa prenášajú informácie v aplikačných službách verejnými sieťami, musia byť tieto informácie chránené pred podvodnými aktivitami, neoprávneným vyzradením, modifikáciou a pod. V prípade prenášania on-line informácií (on-line transakcie), musia byť informácie zabezpečené tak, aby sa zabránilo nekompletným prenosom, neoprávneným zmenám, chybnému smerovaniu, neoprávnenému vyzradeniu, neoprávneným opakovaniam a neautorizovanému duplikovaniu správ.

Pri požiadavke prepojenia internej siete ŽSR so sieťami tretích strán musia byť posúdené bezpečnostné aspekty vyplývajúce z takéhoto prepojenia.

8.4.3 Vzdialený prístup

Vzdialený prístup na IKT prostriedky ŽSR je prísne riadený. Vzdialený prístup tretích strán môže byť využívaný iba prostredníctvom bezpečných kanálov a použitím dvojfaktorovej autentizácie.

Vzdialený prístup tretím stranám je riadený v súlade s požiadavkami pre riadenie prístupu v kapitole 8.2 Riadenie prístupu. Vzdialený prístup môže byť tretím stranám umožnený len pre konkrétne osoby a len na nevyhnutne potrebný čas.

8.5 Rozvoj a údržba IKT

8.5.1 Vývoj systémov

Počas celého procesu vývoja systémov ŽSR musí byť zabezpečené oddelenie zodpovedností v oblasti vývoja, prevádzky a kontroly s cieľom obmedziť bezpečnostné riziko zneužitia systému. To znamená najmä, že osoby vykonávajúce vývoj nesmú mať prístup do produkčného prostredia / do produkčných systémov. Vývojové a testovacie prostredie musí byť oddelené od produkčného prostredia.

Systémy sa môžu nasadiť do ostrej prevádzky až po ich otestovaní a akceptácii ŽSR. Ku každému IKT prostriedku vyvíjanému treťou stranou musí byť dodaná užívateľská a administrátorská dokumentácia.

8.5.2 Ochrana testovacích údajov

Poskytnutie databáz tretím stranám za účelom testovania systémov je možné len so súhlasom vlastníka informácií.

Pri poskytnutí databáz s citlivými údajmi tretím stranám na testovacie účely, musí byť treťou stranou zabezpečená ochrana týchto údajov pred neautorizovaným prístupom k týmto údajom, pred ich únikom alebo zverejnením. Po vykonaní testovania musia byť údaje bezodkladne bezpečne zlikvidované.

8.5.3 Riadenie zmien

Zamestnanci tretích strán nesmú svojvoľne zasahovať do konfigurácie IKT prostriedkov, ktorých prevádzku zabezpečujú. Všetky zmeny vykonávané treťou stranou musia byť preukázateľne schválené ŽSR. O všetkých zmenách musia byť uchovávané záznamy.

8.6 Fyzická bezpečnosť a bezpečnosť IKT prostriedkov

8.6.1 Bezpečnosť IKT prostriedkov

Priestory tretích strán, v ktorých sú umiestnené IKT prostriedky, ktoré podporujú poskytovanie služieb ŽSR, musia byť zabezpečené primeranými bezpečnostnými opatreniami, ktoré zabezpečia ich fyzickú ochranu pred neautorizovaným prístupom, krádežou, poškodením a vplyvmi prostredia.

V okolí vyššie uvedených priestorov sa nesmú vyskytovať zariadenia, ktoré môžu ohroziť IKT prostriedky umiestnené v tomto priestore, najmä kanalizácia, vodovod, horľavé alebo iné obdobné materiály.

Tretie strany zodpovedajú za bezpečnosť zverených IKT prostriedkov. V prípade výkonu zásahov v priestoroch ŽSR, sú zamestnanci tretích strán povinní dodržiavať bezpečnostné pravidlá ŽSR platné pre jednotlivé lokality, resp. priestory ŽSR.

8.6.2 Kontrola pohybu cudzích osôb v priestoroch ŽSR

Pohyb všetkých cudzích osôb (návštev, pracovníkov tretích strán a pod.) v priestoroch ŽSR je riadený a kontrolovaný. Uvedeným osobám môžu byť sprístupnené len tie priestory, ktoré nevyhnutne potrebujú na výkon činností pre ŽSR. Zamestnanci tretích strán majú zakázané pokúšať sa vniknúť do vnútorných priestorov ŽSR bez autorizácie oprávneným zamestnancom ŽSR.

V prípade priestorov s dôležitými prostriedkami IKT môže byť prístup cudzích osôb umožnený len v sprievode zodpovedného zamestnanca ŽSR. Medzi takéto priestory patria najmä:

- objekty, kde sú ukončené fyzické vedenia – káblové závery metalických a optických káblov, ukončenie štruktúrovaných kabeláží,
- objekty, kde sú uložené zariadenia, priamo alebo nepriamo podieľajúce sa na prenose a spracovaní informácií (aj napájacie zdroje),
- objekty, v ktorých sa nachádzajú archívy dôležitých dát,
- objekty, v ktorých sa nachádzajú podporné a riadiace systémy.

Osoby vykonávajúce činnosť vo vyššie uvedených priestoroch:

- musia nosiť viditeľnú identifikáciu pokiaľ im bola takáto identifikácia pridelená,

- musia byť sprevádzaní zamestnancom ŽSR, oprávneným k vstupu do týchto priestorov,
- majú zakázané manipulovať so zariadeniam i a prinášať a vynášať zariadenia z týchto priestorov bez predchádzajúceho schválenia zodpovednou osobou ŽSR,
- nesmú používať fotografické, video, audio, alebo iné záznamové zariadenia (aj mobilný telefón s fotoaparátom) na vytváranie fotografií a záznamov; neplatí v prípade schválenia zodpovednou osobou ŽSR,
- musia udržiavať čistotu.

8.6.3 Požiarna ochrana priestorov ŽSR

Vo všetkých priestoroch, v ktorých sa nachádzajú dôležité informačné aktíva sú nainštalované systémy elektronickej požiarnej signalizácie (EPS) pripojené na centrálne kontrolné (signalizačných) pulty. Technické zariadenia, ktoré umožňujú zásah proti požiaru (technologické hasenie, hasiace prístroje a pod.) sú umiestnené všade tam, kde to vyžadujú normy, právne predpisy alebo bezpečnostné a protipožiarne požiadavky.

8.6.4 Aplikácia pravidla čistého stola a čistej obrazovky

Každý zamestnanec tretej strany musí zabezpečiť, aby pred odchodom z pracoviska uistil, aby nenechal na pracovisku na ktorom vykonával svoju činnosť voľne dostupné citlivé materiály a dokumenty, elektronické nosiče týchto informácií, autentifikačné prostriedky a pod. Po ukončení práce je povinný tieto materiály presunúť na bezpečné miesto alebo ich odovzdať zodpovednému zamestnancovi ŽSR.

Pred vzdialením sa zamestnanca tretej strany od IKT prostriedku (pracovná stanica, server, ...) musí sa zamestnanec z IKT prostriedku odhlásiť alebo IKT prostriedok zabezpečiť iným spôsobom voči neautorizovanému prístupu k tomuto prostriedku.

8.7 Riadenie kontinuity činností

Tretie strany zabezpečujúce správu a prevádzku IKT prostriedkov ŽSR patria medzi subjekty, ktoré sú povinné podporovať riadenie kontinuity činností ŽSR v relevantnom rozsahu.

Na zaistenie kontinuity kritických procesov a základných služieb ŽSR sú vypracované a udržiavané plány kontinuity činností. Tretie strany zahrnuté do plánovania obnovy IKT prostriedkov sú povinné bezodkladne informovať zodpovedné osoby ŽSR ohľadne zmien týkajúcich sa svojich zamestnancov vykonávajúcich činnosti pre ŽSR, ako aj o existujúcich alebo potenciálnych dôvodoch zníženia úrovne alebo kvality poskytovaných služieb pre IKT prostriedky.

8.8 Výkon prác tretími stranami

Ďalšie konkrétne podmienky výkonu prác tretími stranami, ako aj príslušné legislatívne a bezpečnostné požiadavky a povinnosti tretích strán pri zaisťovaní ochrany aktív, sú definované v zmluve, resp. v rámci iného písomného dokumentu

upravujúceho výkon prác tretích strán pre ŽSR a v rámci internej riadiacej dokumentácii ŽSR, s ktorou bola tretia strana, resp. jej zamestnanci preukázateľne oboznámení.

Ak tretia strana využíva na vykonávanie určených služieb ďalších dodávateľov, je povinná o tejto skutočnosti písomne informovať ŽSR. Bezpečnostné a legislatívne požiadavky kladené na tretej strany, ako aj požiadavky tejto politiky, musia byť prenesené aj na dodávateľov tretej strany.

8.9 Riadenie bezpečnostných incidentov

Systém hlásenia a reakcie na bezpečnostné incidenty (vrátane kybernetických bezpečnostných incidentov) je predpokladom pre včasné zachytenie incidentu alebo bezpečnostného problému a reakciu naň.

Všetky podozrenia alebo detegované pokusy narušenia bezpečnosti a bezpečnostné slabiny, ktoré môžu mať za následok vznik bezpečnostného incidentu a porúch IKT prostriedkov ŽSR, alebo IKT prostriedkov podporujúcich základné služby ŽSR, musia byť zamestnancom tretej strany bezodkladne ohlásené určenému kontaktnému bodu Servicedesk ŽT (920-2727, servicedesk@zsr.sk) resp. priamo príslušnému koordinátorovi zmluvného vzťahu alebo inak zmluvne dohodnutým spôsobom.

V prípadoch, kedy sú IKT prostriedky podporujúce základné služby ŽSR prevádzkované v priestoroch alebo na infraštruktúre tretích strán, sú tretie strany povinné zabezpečiť detekciu bezpečnostných incidentov prostredníctvom implementácie nástrojov na bezpečnostný a prevádzkový monitoring a na nepretržité analyzovanie a vyhodnocovanie jednotlivých udalostí, ktoré umožňujú detegovať bezpečnostné incidenty v prostredí IKT.

V prípade vzniku bezpečnostného incidentu alebo v prípade podozrenia na jeho vznik sú tretie strany, resp. jej zamestnanci zabezpečujúce správu alebo prevádzku príslušného IKT prostriedku povinní zabezpečiť dôkazy a iné informácie viažuce sa k identifikovanému incidentu napr. dátum a čas identifikácie/vzniku incidentu, lokalita, IP adresa, identifikačné údaje zariadení, mená zúčastnených osôb. Súčasne sú povinní navrhnúť opatrenia na zmiernenie alebo odvrátenie dopadu vzniknutého bezpečnostného incidentu na informačné aktíva a/alebo základné služby ŽSR.

Zamestnanci tretích strán sú povinní poskytnúť zamestnancom vyšetrujúcim vzniknuté bezpečnostné incidenty primeranú súčinnosť.

8.10 Zabezpečenie súladu

8.10.1 Súlad s legislatívnymi a zmluvnými požiadavkami

Tretie strany a ich zamestnanci sú povinné plniť všetky relevantné požiadavky právnych predpisov a právne záväzných aktov EÚ. Súčasne musia zabezpečovať ochranu informačných aktív ŽSR a aktív, ktoré podporujú poskytovanie základných služieb ŽSR v súlade s požiadavkami medzinárodne uznávaných bezpečnostných štandardov ako je napr. ISO/IEC 27001 / 27002.

8.10.2 Ochrana autorských práv

Na IKT prostriedkoch ŽSR môže byť inštalovaný len autorizovaný a legálny softvér. Používanie všetkého softvéru musí byť v súlade s autorskými právami držiteľa licencie. Neautorizovaná inštalácia softvéru a zmeny konfigurácie koncových zariadení ŽSR sú zakázané.

8.10.3 Kryptografické opatrenia

Pre informácie citlivé z hľadiska dôvernosti musí byť zabezpečené ich šifrovanie pri ich prenose a uchovávaní mimo zabezpečených priestorov ŽSR.

9. PRÍLOHY

Príloha č. 1 Pravidlá a formuláre pre riadenie prístupu tretích strán do IKT prostriedkov ŽSR

Príloha č. 1 Pravidlá
a formuláre pre riad

Príloha č. 2 Bezpečnostné pravidlá pre zabezpečenie prístupu do IKT prostriedkov ŽSR

Príloha č. 2
Bezpečnostné pravi

Príloha č. 3 Vyhlásenie o ochrane dôverných informácií získaných prístupom do IKT prostredia ŽSR

Príloha č. 3
Vyhlásenie o ochran

Príloha č. 4 Dohoda o ochrane dôverných informácií a skutočností tvoriacich obchodné tajomstvo

Príloha č. 4 Dohoda
o ochrane dôvernýc

Koniec dokumentu