Železnice Slovenskej republiky, Bratislava

Generálne riaditeľstvo

Smernica

Bezpečnostná politika KIS – skrátená verzia určená pre tretie strany

(určená na zverejnenie na www.zsr.sk)

Spracovateľský / gestorský útvar	Číslo	Označenie
O210 GR ŽSR	17909/2016/O210	O-01-O210-2016
Účinnosť od Dňom vydania		
Schválil Ing. Dušan Šefčík v.r. generálny riaditeľ ŽSR	**Dňa** 22.4.2016	

SLEDOVANIE VYDANÍ A ZMIEN DOKUMENTU

Zoznam vydaní dokumentu

Vydané pod číslom	Účinnosť od - do
.....	.....

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, príp. gestorským útvarom tohto dokumentu.
Tento dokument sa vydáva len v elektronickej podobe a jeho aktuálne znenie je umiestnené (zverejnené) v dokumentovom úložisku IP ŽSR.
Držiteľ výtlačku tohto dokumentu je zodpovedný za včasné a správne vykonanie vydaných zmien a vykonanie záznamu o zmenách.

Obsah

PREHLÁSENIE VEDENIA ŽSR

k vydaniu bezpečnostnej politiky KIS

Vydaním tejto politiky bezpečnosti ŽSR prijímajú zásady na dosiahnutie potrebnej úrovne bezpečnosti KIS a zámer na stanovenie rámca riadenia bezpečnosti, na zabezpečenie chodu prevádzky všetkých KIS ŽSR v požadovanom rozsahu a kvalite; na zabezpečenie vysokej trvalej dostupnosti aplikácií kritických z hľadiska zabezpečenia základných funkcií ŽSR; na zabránenie nenávratných strát údajov uchovávaných v KIS; na zamedzenie prezradeniu údajov pri prenosoch všetkými formami a na zamedzenie úniku údajov uložených na pamäťových médiách.

Vedenie ŽSR týmto deklaruje riadenie bezpečnosti KIS za neoddeliteľnú súčasť svojej činnosti, ktoré bude uskutočňované v zhode s prijatou Bezpečnostnou politikou KIS ŽSR.

Na základe tejto Bezpečnostnej politiky KIS sa vypracovávajú ďalšie záväzné smernice ŽSR, ktoré budú komplexne pokrývať ustanovenia legislatívy a medzinárodných noriem pre oblasť informačnej bezpečnosti a zabezpečia dobré meno ŽSR. Konanie v súlade s týmito smernicami bude vyžadované od všetkých organizačných zložiek ŽSR.

ZOZNAM POUŽITÝCH SKRATIEK

HW - Zariadenia tvoriace technické vybavenie počítača komunikačných a informačných systémov
IP ŽSR - Intranetový portál Železníc Slovenskej republiky
KIS - Komunikačné a informačné systémy
DS - Dátová sieť ŽSR
IS - Informačný systém
TS - Telekomunikačný systém
IRA - Interný riadiaci akt
PC - Osobný počítač
SW - Programové vybavenie komunikačných a informačných systémov
VOJ - Vnútorná organizačná jednotka
ŽSR - Železnice Slovenskej republiky
IKT - Informačné a komunikačné technológie
OKRaO - Odbor krízového riadenia a ochrany
Z9 – Povoľovanie vstupu do obvodu dráhy v správe ŽSR
O21 - Zabezpečenie ochrany majetku podmienkach ŽSR
ÚIVP - Ústredný inštitút vzdelávania a psychológie
GR - Generálne riaditeľstvo
MDVRR – Ministerstvo dopravy, výstavby a regionálneho rozvoja
O210 - Odbor telekomunikácií, informatiky a informačnej bezpečnosti
ŽT - Železničné telekomunikácie

1. ÚVOD

Bezpečnostná politika KIS predstavuje súhrn pravidiel pre prevádzku a používanie komunikačných a informačných systémov a pre zaobchádzanie s informáciami v týchto systémoch s cieľom zachovať všetky bezpečnostné atribúty dát, predovšetkým dôvernosť, integritu a dostupnosť.

Cieľom bezpečnostnej politiky KIS je stanoviť rámec riadenia bezpečnosti, zabezpečiť chod všetkých KIS ŽSR v požadovanom rozsahu a kvalite, zabezpečiť vysokú dostupnosť aplikácií kritických z hľadiska zabezpečenia základných funkcií ŽSR, zabrániť nenávratným stratám údajov uchovávaných v KIS, zamedziť prezradeniu údajov pri prenosoch všetkými formami a zamedziť únikom údajov uložených na pamäťových médiách.

Ciele Bezpečnostnej politiky KIS možno charakterizovať ako zabezpečnie:

- Dôvernosti;
- Integrity;
- Dostupnosti informácií

Poslaním tejto Bezpečnostnej politiky KIS je spolu s ďalšími IRA a vnútornými predpismi ŽSR v oblasti informačnej bezpečnosti stanoviť stratégiu a konkrétne pravidlá bezpečného správania sa používateľov, ktorým boli zverené IKT zariadenia pre vykonávanie ich pracovných činností v rámci Železníc Slovenskej republiky.

1.1 Stanovenie rámca riadenia

Pred začatím procesu implementácie informačnej bezpečnosti musí byť jasne stanovený rámec riadenia bezpečnosti v oblasti KIS.

Kroky pre identifikovanie a dokumentovanie cieľov riadenia:

a) Definovať politiku informačnej bezpečnosti
b) Definovať rozsah systému riadenia informačnej bezpečnosti. Určiť hranice lokalizácie aktív a technológií
c) Vykonať primerané ohodnotenie rizík – z toho identifikovať hrozby pre aktíva, zraniteľnosť a dopad na organizáciu a určenie stupňa rizika
d) Na základe politiky informačnej bezpečnosti identifikovať oblasť rizík, ktoré majú byť riadené.

Tieto kroky sa v pravidelných intervaloch revidujú.

2. ZÁKLADNÉ POJMY

aktíva KIS [1]	všetko čo má pre organizáciu hodnotu (informácie; SW; fyzické aktíva; ľudia – ich kvalifikácia, zručnosti a skúsenosti; nehmotné aktíva – image organizácie ...)
vlastník aktíva KIS [1]	jednotlivec alebo entita, ktorá prijala manažérsku zodpovednosť za kontrolu výroby, vývoja, údržby, použitia a bezpečnosti aktív. Termín „vlastník“ neznamená, že daná osoba má vlastnícke právo na dané aktívum,
Informácie [2]	sú aktívum, ktoré je podobne ako iné podnikové aktíva, nevyhnutné pre aktivity organizácie a teda je potrebné, aby bolo primerane chránené. Informácie môžu existovať v mnohých formách. Môžu byť vytlačené alebo napísané na papieri, uložené elektronicky, prenášané poštou alebo použitím elektronických prostriedkov, premietnuté vo filmoch alebo vyslovené v konverzáciách. Bez ohľadu na to, akú majú informácie formu alebo akými prostriedkami sa spoločne používajú alebo ukladajú, vždy by mali byť náležite chránené,
Informačná bezpečnosť	Je ochrana, ktorá zahŕňa programové, technické, organizačné a sociálno-personálne opatrenia na minimalizáciu možných strát pri poškodení, zničení prípadne zneužití informačných systémov,
dôvernosť	bezpečnostný atribút, ktorý vyjadruje, že k obsahu informácie majú prístup iba oprávnené osoby,
integrita	bezpečnostný atribút, ktorý vyjadruje neporušenosť (celistvosť) dát v KIS,
prístupnosť (dostupnosť)	bezpečnostný atribút, ktorý vyjadruje požiadavku, aby oprávnené subjekty mali prístup k aktívam KIS vždy, keď to potrebujú,
zraniteľnosť	slabé miesto aktíva, alebo opatrenia, cez ktoré sa môže realizovať hrozba,
hrozba	je akákoľvek udalosť, ktorá môže spôsobiť narušenie dôvernosti, integrity a dostupnosti aktíva,
riziko	potenciál, že určitá hrozba využije zraniteľnosť používaného aktíva a spôsobí jeho stratu alebo poškodenie,
analýza rizík KIS	systematická kontrola všetkých zraniteľných miest KIS so stanovením pravdepodobnosti a vyčíslením následkov ich možného ohrozenia, jej výstupom je návrh bezpečnostných opatrení,
autentifikácia	jednoznačné potvrdenie identity používateľa v KIS,

autorizácia	bezpečnostný atribút, ktorý označuje potrebu zadefinovania preddefinovaných a jednoznačne vyjadrených identifikačných znakov, slúžiacich na vstup do akéhokoľvek informačného systému vyžadujúceho autorizáciu,
bezpečnostná legislatíva	súhrn predpisov, nariadení, technologických postupov, noriem, ktoré sú súčasťou realizácie bezpečnostnej politiky organizácie,
bezpečnostná politika KIS	dokument, v ktorom organizácia formálne deklaruje potrebu a ciele ochrany hmotných aj nehmotných aktív KIS,
bezpečnostný audit	kontrolná činnosť zameraná na dodržiavanie bezpečnostnej politiky a ustanovení bezpečnostnej legislatívy prevádzkovateľmi a používateľmi KIS,
bezpečnostný manažment	zamestnanci poverení tvorbou pravidiel a kontrolou dodržiavania zásad bezpečnosti na ŽSR, odbore GR, alebo vnútornej organizačnej jednotke,
fyzická bezpečnosť KIS	je systém opatrení slúžiacich na ochranu KIS 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.,
informačný systém (KIS)	ucelený systém pozostávajúci z technických prostriedkov, údajov a programových aplikácií, umožňujúcich spracovanie vstupných údajov prostriedkami výpočtovej techniky s cieľom poskytnúť informácie pre ďalšie využitie v podnikových procesoch,
používateľ KIS	každý subjekt využívajúci pri svojej práci technické a programové prostriedky niektorej z aplikácií KIS,
pravidlá bezpečnosti	zásady ochrany aktív organizácie definované pre konkrétnu činnosť príslušným metodickým útvarom a internými predpismi (prevádzkové poriadky, prevádzkové pokyny a pod.)
prevádzkovateľ KIS	Železničné telekomunikácie, iné organizačné útvary ŽSR, alebo externá organizácia, ktoré sú zodpovedné za vykonávanie informačných činností,
profil používateľa KIS	rozsah prístupových práv používateľa k dátam v aplikácii definovaný jej metodikom,
stupeň ochrany	definovaná úroveň znemožnenia neoprávneného prístupu k aktívam KIS,
škodlivý SW	Je taký SW, ktorý bol vyvinutý s úmyslom vytvoriť škodu. Tento SW zahŕňa vírusy, červy, trójske kone a ostatný škodlivý SW,
Manažérske kanály	Jednotlivé vzťahy medzi rolami vyplývajúce z kapitoly 3.1
Personálna bezpečnosť	Je systém opatrení súvisiacich s výberom, určením, školením a kontrolou osôb, ktoré môže zasahovať do KIS,
Kritické informácie	Je informácia, ktorá je neverejná, ktorou zverejnenie by sa mohlo zneužiť na činnosť smerujúcu k narušeniu alebo zničeniu prvku kritickej infraštruktúry.

Bezpečnostné incidenty	Udalosť, ktorá spôsobila narušenie bezpečnosti informačného systému. Tzn., že došlo ku strate diskrétnosti, integrity alebo dostupnosti dát. Za bezpečnostný incident treba považovať aj odhalený pokus o prekonanie bezpečnostných opatrení.
Bezpečnostné požiadavky	požiadavky kladené na informačný systém, ktoré sú odvodené zo zákonov, inštrukcií, právnych úprav, záväzných noriem a štandardov, vnútornej legislatívy organizácie; prostredia, v ktorom systém pôsobí a poslania, ktoré plní; potrebné na zaistenie dôvernosti, dostupnosti a integrity informácií, ktorá sa v systéme spracováva
Úrovne bezpečnosti	Inak povedané úroveň integrity bezpečnosti je merná jednotka kvantifikujúca omedzenie rizika. Omedzenie rizika je možné kvantifikovať na základe koncepcie úrovne integrity bezpečnosti.
Utajovaná skutočnosť	Utajovanou skutočnosťou je informácia alebo vec určená pôvodcom utajovanej skutočnosti, ktorú vzhľadom na záujem Slovenskej republiky/organizácie treba chrániť pred vyzradením, zneužitím, poškodením, neoprávneným rozmnožením, zničením, stratou alebo odcudzením
Bezpečnostné slabiny	*Možnosť existencie bezpečnostných dier, miest kde môže byť narušená integrita.*
Technologické zariadenie	Pod pojmom technologické zariadenie pre účely tohto dokumentu sa rozumie zariadenie v správe VOJ ŽT v tesnej väzbe s aktívami IKT predstavujúce riziko vo vzťahu k bezpečnostnej politike KIS (predovšetkým IT zariadenia pre prevádzku sietí, informačných systémov, nosiče dát ap.). Pre technologické zariadenia, ktoré nie sú v správe VOJ ŽT sa ustanovenia tejto smernice netýkajú. Riešenie rizík bezpečnostnej politiky vo vzťahu k takýmto zariadeniam je predmetom IRA v gescii príslušných odborov GR ŽSR. V prípade, že tretia strana pri výkone činností na technologickom zariadení, ktoré nie je v správe VOJ ŽT v zmysle platných zmlúv požaduje priamy prístup k aktívam IKT v správe VOJ ŽT (prístup k internej sieti ŽSR, prístup k informačným systémom, ap.), takéto prípady vo vymedzenom rozsahu riešia ustanovenia článku 3.2. tejto smernice.
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.
Bezpečnostné funkcie	Sú funkcie zvyšujúce bezpečnosť IS: identifikácie, autentifikácia, riadenie prístupu, dôveryhodnosť údajo, bezpečnosť prenosu údajov, presnosť a spoľahlivosť služieb.

3. ORGANIZÁCIA INFORMAČNEJ BEZPEČNOSTI

Musia sa vytvoriť vzťahy so zodpovednými kontrolnými orgánmi štátu a externými bezpečnostnými špecialistami, ktoré by pomáhali udržiavať kontakt s trendmi v rámci oboru, monitorovať štandardy a metódy hodnotenia a poskytovať styčné body pri likvidácii bezpečnostných incidentov. Musí sa podporiť multidisciplinárny prístup k informačnej bezpečnosti. Uvedené vzťahy vytvára a udržiava na ŽSR O210.

Na ŽSR štruktúra riadenia informačnej bezpečnosti vyplýva z Organizačného poriadku ŽSR a z platnej organizačnej štruktúry ŽSR. Informačná bezpečnosť je riadená vrcholovo Odborom telekomunikácií, informatiky a informačnej bezpečnosti /O210/ a prevádzkovo je riadená Železničnými telekomunikáciami, ktoré vykonávajú aj stanovené bezpečnostné pravidlá.

Bezpečnosť v oblasti KIS na ŽSR vrcholovo riadi úsek Námestníka generálneho riaditeľa pre rozvoj a informatiku, prostredníctvom Odboru telekomunikácií, informatiky a informačnej bezpečnosti GR ŽSR. Odbor telekomunikácií, informatiky a informačnej bezpečnosti na dosiahnutí bezpečnostných cieľov organizácie v oblasti KIS úzko spolupracuje so Železničnými telekomunikáciami.

4. KLASIFIKÁCIA A RIADENIE AKTÍV

Pre komplexné riešenie bezpečnosti v oblasti KIS, sa musia presne definovať všetky relevantné aktíva a významným aktívam, prideliť jednoznačné zodpovednosti. Za definovanie konkrétnych a relevantných aktív sú zodpovední vlastníci aktív.

Pridelenie zodpovedností za aktíva pomôže zaistiť udržanie primeranej ochrany, rýchlejšie reakcie na bezpečnostné incidenty, ale aj lepšie vyvodenie záverov pri navrhovaných nápravných opatreniach.

5. BEZPEČNOSŤ PRÍSTUPU TRETÍCH STRÁN

Každé udelenie prístupu tretím stranám do akéhokoľvek informačného systému ŽSR predstavuje určité riziko pre organizáciu. Uvedené udelenie prístupu môže spôsobiť rôzne bezpečnostné hrozby, ako aj ohroziť dobré meno spoločnosti a spôsobiť ekonomické škody.

I v prípade, keď neexistuje žiadny škodlivý úmysel, resp. keď sa prístup poskytuje oprávnene, musí byť prístup riadený a prísne kontrolovaný. Konfiguráciu (riadenie) prístupov tretích strán zabezpečujú Železničné telekomunikácie.

Každý prístup potenciálneho používateľa tretej strany do informačných systémov ŽSR, do technologických zariadení prevádzkovaných ŽSR a k aktívam IKT podlieha schvaľovaciemu procesu, ktorý podlieha pod kompetenciu Odboru telekomunikácií, informatiky a informačnej bezpečnosti a v ktorom sa určí či oprávnene požaduje vstup do informačných systémov a spĺňa dostatočné bezpečnostné prvky pre vstup do IKT ŽSR, prípadne technologických zariadení prevádzkovaných ŽSR. Každý z potenciálnych používateľov podlieha schvaľovaciemu procesu, ktorého výsledkom je pridelenie/odmietnutie prístupových práv do požadovaného informačného systému.

Prístupom tretích strán sa okrem uvedeného rozumie aj:

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

Udeľovanie prístupových práv pre externých používateľov vrcholovo zastrešuje Odbor telekomunikácií, informatiky a informačnej bezpečnosti, ktorý musí písomne potvrdiť na základe požiadavky pridelenie oprávnenia na prístup do definovaného IS, technologického zariadenia resp. do siete. Zasielaná požiadavka musí obsahovať pravdivé a správne vyplnené údaje, za ktoré zodpovedá osoba žiadateľa, t.j. tretia strana.

Žiadateľ vyplňuje žiadosť o pridelenie prístupu do prostredia KIS na základe definovanej prílohy Bezpečnostnej politiky KIS v spolupráci so styčnou osobou za ŽSR (Príloha č.1: Žiadosť o pridelenie prístupu tretej strane do IS ŽSR, Príloha č.2: Žiadosť o pridelenie prístupu tretej strane do siete LAN ŽSR, Príloha č.3: Žiadosť o pridelenie prístupu tretej strane do technologických zariadení, alebo Príloha č.4: Žiadosť o prístup do IS, SW apl. z dôvodu údržby).

Podmienkou schválenia žiadosti o pridelenie prístupu do prostredia KIS je podľa nižšie uvedených kritérií predloženie buď platnej Dohody o ochrane dôverných informácií a skutočností tvoriacich obchodné tajomstvo /Príloha č.6 / , ak bola uzavretá, alebo žiadateľom podpísaného Prehlásenia o ochrane dôverných informácií získaných prístupom do IKT prostredia ŽSR. /. Príloha č. 7 /.

Dohodu o ochrane dôverných informácií a skutočností tvoriacich obchodné tajomstvo / Príloha č.6 / uzatvára ŽSR s druhou stranou za účelom ochrany dôverných informácií poskytnutých druhej strane v čase pred podpisom zmluvy, ktorú ŽSR a druhá strana plánujú uzavrieť (napr. v rámci rokovaní o základných podmienkach spolupráce, produktoch ŽSR, know-how a pod.) vyplňuje žiadateľ, ktorým môže byť fyzická osoba alebo právnická osoba. Na základe uvedeného sa v Dohode o ochrane dôverných informácií vyplňujú všetky tie údaje, ktoré sa vzťahujú na vyššie uvedenú osobu. Znenie Dohody o ochrane dôverných informácií a skutočností tvoriacich obchodné tajomstvo je možné prispôsobiť konkrétnemu obchodnému prípadu.

V prípade, ak už ŽSR má s druhou 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.

Prehlásenie o ochrane dôverných informácií získaných prístupom do IKT prostredia ŽSR / Príloha č. 7/ podpisuje externý koncový užívateľ, s ktorým ŽSR nebude uzatvárať zmluvu a teda ani Dohodu o ochrane dôverných informácií a skutočností tvoriacich obchodné tajomstvo.

V zmysle Bezpečnostnej politiky KIS môže Prehlásenie o ochrane dôverných informácií podpísať splnomocnený zástupca právnickej osoby/podnikateľa. V uvedenom prípade je nutné na O210 predložiť aj podpísané splnomocnenie právnickej osoby/podnikateľa, kde za správnosť a pravdivosť vyplnených údajov zodpovedá splnomocnený zástupca.

Bezpečnostný manažér O210 zodpovedá za kontrolu kompletnosti dokumentácie všetkých predložených žiadostí VOJ ŽSR. Platnosť prístupu je maximálne do ukončenia zmluvného vzťahu so žiadateľom, v prípade, že taký neexistuje tak maximálne po dobu 6 mesiacov od dátumu schválenia projektovým manažérom O210 GR ŽSR. Po uplynutí stanovenej časovej lehoty musí žiadateľ pri novej/rozširujúcej žiadosti o prístup do KIS predložiť nové prehlásenie o ochrane dôverných informácií.

Udeľovanie prístupových práv pre externých používateľov vrcholovo zastrešuje Odbor telekomunikácií, informatiky a informačnej bezpečnosti, ktorý musí písomne potvrdiť na základe požiadavky pridelenie oprávnenia na prístup do definovaného IS, technologického zariadenia resp. do siete. a potvrdiť, kto bude znášať náklady s poskytovaním prístupu. Uvedené platí aj na prístupy už zriadené a je potrebné pre všetky opätovne doplniť súhlas O210. Pokiaľ žiadateľ nesplní požadované podmienky, O210 nariaďuje, aby ŽT takýto prístup zrušili najneskôr do 1 mesiaca po vydaní tejto Smernice. Požiadavku na pridelenie oprávnenia na prístup do definovaného IS, technologického zariadenia, resp. do siete zašle zamestnanec ŽSR, s ktorým tretia strana spolupracuje, na Odbor telekomunikácií, informatiky a informačnej bezpečnosti spoločne s vyplnenými a podpísanými prílohami, ktoré sú neoddeliteľnou súčasťou tejto smernice. Súčasťou požiadavky je aj návrh technického riešenia spôsobu pripojenia.

Potvrdenie/zamietnutie pridelenia prístupových práv musí Odbor telekomunikácií, informatiky a informačnej bezpečnosti doručiť príslušnej VOJ, ktorá prístup požaduje. V prípade negatívnej odpovede musí táto obsahovať aj zdôvodnenie zamietnutia. Prístup a nastavenie oprávnení realizujú po pridelení oprávnenia Železničné telekomunikácie. Realizácia prístupu sa vykoná v čo najskoršie možnom čase po doručení autorizácie tretej strany od Odboru telekomunikácií, informatiky a informačnej bezpečnosti.

Akékoľvek výnimky v KIS ŽSR (prístupy, používateľské účty, oprávnenia a pod.), ktoré nespĺňajú taxatívne požiadavky definované v tomto IRA a ku nemu vydaným osobitným vykonávacím dokumentom, udeľuje po zvážení gestor Bezpečnostnej politiky KIS ŽSR (Bezpečnostný manažér organizácie).

V prípade, že tretie strany nepožadujú pristupovať do internej siete ŽSR ani do žiadneho informačného systému prevádzkovaného na ŽSR, ale požadujú prístup do verejného Internetu cez WIFI prevádzkovaného ŽT z dôvodu obchodných, resp.

pracovných dôvodov, prístup nepodlieha schvaľovaciemu procesu uvedenom v tejto smernici. O uvedený spôsob pripojenia požiada tretia strana cestou styčného zamestnanca pre informatiku odboru, VOJ, ktorý pracovné jednanie s treťou stranou organizuje. Styčný zamestnanec požiada Železničné telekomunikácie o pridelenie prístupu pre tretie strany v požadovanom množstve a definovanom čase, maximálne však na 14 pracovných dní, pričom požiadavky sú nahlasované prostredníctvom ServiceDesku ŽT (Hotline – 920/2727), alebo 920/2000 voľba 3. Železničné telekomunikácie sú povinné mesačne zasielať report o zriadených WIFI prísptupoch na Odbor telekomunikácií, informatiky a informačnej bezpečnosti /bezpečnostnému manažérovi organizácie a projektovému manažérovi IKT, ktorý je zodpovedný za prístup tretích strán/.

6. ZABEZPEČENIE OCHRANY UTAJOVANÝCH SKUTOČNOSTÍ

Spracovávanie utajovaných skutočností pomocou výpočtovej techniky, využitie KIS v oblasti utajovaných skutočností si vyžaduje stanovenie a zabezpečenie adekvátnych opatrení, aby nemohlo dôjsť k ich neoprávnenej manipulácii.

Oblasť ochrany utajovaných skutočností je na ŽSR zabezpečovaná útvarmi krízového riadenia a ochrany a je vykonávaná určenými bezpečnostnými zamestnancami OKRaO v súlade s platnou legislatívou – zákonom č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a súvisiacich vyhlášok NBÚ. V podmienkach ŽSR ošetrujú IRA vydané OKRaO problematiku ochrany utajovaných skutočností, ďalej stanovujú postup pre získanie bezpečnostnej previerky na ŽSR pre požadovaný stupeň utajenia.

7. ZABEZPEČENIE OCHRANY OSOBNÝCH ÚDAJOV

Osobnými údajmi sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu. Informačným systémom (automatizovaným, neautomatizovaným) treba chápať akýkoľvek usporiadaný súbor v ktorom sa spracúvajú osobné údaje.

Železnice Slovenskej republiky ako prevádzkovateľ informačných systémov, sú povinné s účinnosťou od 1.júla 2013 spracúvať osobné údaje v súlade so zákonom 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len zákon) a prijať primerané bezpečnostné opatrenia (technické, organizačné) na plnenie tohto zákona.

Primerané bezpečnostné opatrenia sú zabezpečené prostredníctvom na to určeného bezpečnostného projektu a smerníc na ochranu osobných údajov v informačnom systéme ŽSR, ktoré sú vydané ako organizačné normy na zabezpečenie povinností vyplývajúcich z ustanovení Zákona o ochrane osobných údajov.

Zodpovednosť v rámci ochrany osobných údajov na ŽSR je vrcholovo centralizovane zabezpečovaná prostredníctvom určených zamestnancov s oprávnením zodpovedných osôb z Odboru telekomunikácií, informatiky a informačnej bezpečnosti (O 210 GR ŽSR).

8. FYZICKÁ BEZPEČNOSŤ A BEZPEČNOSŤ PROSTREDIA

Cieľ: Zabrániť neautorizovanému prístupu, poškodeniu a ohrozovaniu aktív KIS spoločnosti.

Organizácia je povinná vytvoriť také prostredie, ktoré bude jednoznačne chrániť pred neautorizovaným prístupom, poškodením a ohrozovaním priestorov a informácií spoločnosti.

Fyzická ochrana je uskutočnená vytvorením fyzických bariér okolo prostriedkov spracovávajúcich a prenášajúcich informácie. Každá bariéra vytyčuje určitý bezpečnostný okruh, každá zvyšuje celkovo zabezpečovanú ochranu nielen pred skompromitovaním údajov ale aj pred fyzickým poškodením chránených zariadení. Bezpečnostný okruh je niečo, čo vytvára bariéru, napr. stena, vstupná brána kontrolujúca vstupné preukazy, alebo recepcia so zamestnancom. Situovanie a sila každej bariéry závisí na výsledkoch ohodnotenia rizík.

Pod fyzickú bezpečnosť spadá aj ochrana pred požiarmi.

Do tohto bezpečnostného okruhu v rámci ŽSR spadajú:

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

Pre pohyb osôb v týchto priestoroch platia nasledujúce pravidlá:

a) prístupové práva k bezpečnostným oblastiam môžu mať len zamestnanci, vykonávajúci pracovné alebo kontrolné činnosti na týchto zariadeniach,

b) zamestnanci, pohybujúci sa v týchto priestoroch musia nosiť viditeľnú identifikáciu,

c) návštevníci zabezpečených oblastí musia byť sprevádzaní osobou, oprávnenou k vstupu do týchto objektov a všetky činnosti tu vykonávané môžu uskutočňovať výhradne na základe súhlasu oprávnenej osoby,

d) pre návštevníkov týchto objektov vo všeobecnosti platí, že je zakázané používať fotografické, video, audio, alebo iné záznamové zariadenia (aj mobilný telefón s fotoaparátom), ak nie je autorizovaný. Uvedené je zapracované v predpise Z9 – Povoľovanie vstupu do obvodu dráhy v správe ŽSR.

Za zabezpečenie fyzickej bezpečnosti je zodpovedné každé pracovisko spôsobom, ktorý je vypracovaný v prevádzkových poriadkoch každého osobitného pracoviska.

Metodické riadenie ochrany majetku v podmienkach ŽSR definuje predpis O21 vydaný Odborom krízového riadenia a ochrany (O520). Predmetný predpis je záväzný pre zamestnancov ŽSR v stanovenom rozsahu znalostí.

Príslušný zodpovedný vedúci pracoviska je zodpovedný za fyzickú bezpečnosť na jednotlivom pracovisku.

9. PERSONÁLNA BEZPEČNOSŤ

V rámci vstupného školenia a prideleni prístupových práv ku KIS sú všetci zamestnenci preukázateľne oboznámení s Bezpečnostneou politikou KIS ŽSR. Bezpečnostná politika je trvale dostupná na intranete organizácie. Každý zamestnanec je povinný trvalo dodržiavať svoje povinnosti. Zamestnanci sú oboznámení so skutočnosťou, že nedodržiavanie bezpečnostních zásad môže byť kvalifikované jako porušenie platných IRA ŽSR, Pracovného poriadku ŽSR prípadne příslušných ustanovení Zákonníka práce.

10. KOMUNIKAČNÝ A PREVÁDZKOVÝ MANAŽMENT

Musia byť zavedené zodpovednosti a procedúry riadenia a prevádzky prostriedkov spracujúcich informácie. Toto zahŕňa vytváranie vhodných prevádzkových inštrukcií a procedúr reakcie na incidenty.

Cieľom je dosiahnuť dostupnosť informačného systému v požadovanom rozsahu a kvalite. Za účelom dosiahnutia tohto cieľa sú všetky ťažiskové IS ŽSR prevádzkované na základe SLA, sú zavedené prevádzkové postupy s cieľom určenia zodpovednosti za prevádzku, postupy na riadenie zmien a postupy plánovania a akceptácie systémov.

V prípade spozorovaných bezpečnostných slabín a incidentov je nutné oznámiť ich určenému kontaktnému bodu Servicedesk ŽT (920-2727, servicedesk@zsr.sk) resp. priamo Bezpečnostnému manažérovi organizácie.

11. OCHRANA VOČI ŠKODLIVÉMU SOFTVÉRU NA ŽSR

Na ochranu koncových pracovných staníc /PC/ majú ŽSR zakúpené licencie antivírusového produktu. Tento softvér plne spĺňa kritériá kladené na antivírusový produkt v prostredí ŽSR. Umožňuje rezidentnú ochranu PC, ako aj kontrolu PC na požiadanie. Jeho pravidelná aktualizácia je zabezpečená sieťovými prostriedkami.

Elektronická pošta ŽSR je centrálne chránená antivírusovým programom, ktorý prehliada súbory nachádzajúce sa v prílohách posielaných správ na známe formy vírusov a ich modifikácie. Tento antivírusový program je priebežne aktualizovaný. Na serveroch elektronickej pošty je tiež aktivované blokovanie niektorých typov súborov, ktoré môžu byť potencionálnymi nositeľmi vírusov.

12. VÝVOJ A ÚDRŽBA SYSTÉMOV

Cieľom tejto oblasti je zaistiť, aby bezpečnosť bola implementovaná do informačných systémov. Bezpečnostné požiadavky na vývoj a údržbu systémov realizujú zodpovední zamestnanci zodpovední za riadenie vývoja a podpory aplikácií resp. externí dodávatelia.

Pri vývoji a údrzbe aktív informačního systému sa postupuje podľa zásad projektového riadenia, tzn. všetky požiadavky používateľov ŽSR na vývoj nových, resp. rozvoj existujúcich produktov sú predkladané na O210, ktorý zabezpečuje riešenie a manažment celého procesu od zadania požiadavky až po akceptáciu a nasadenie do prevádzky medzi dodávateľom, používateľom a prevádzkovateľom (ŽT).

13. SÚLAD SO ZÁKONOM

Cieľom je vyhnúť sa porušeniam akýchkoľvek trestných a občianskych zákonov a platných noriem v záujme ochrany KIS aktív ŽSR.

14. APLIKOVATEĽNOSŤ A PRESADENIE

Bezpečnostná politika KIS sa týka všetkých zamestnancov organizácie ŽSR, ktorí používajú jej zariadenia a informácie. Dodržiavanie politiky je v súlade s Pracovným poriadkom ŽSR.

Nedodržanie bezpečnostnej politiky môže poškodiť schopnosť ŽSR dosiahnuť svoj bezpečnostný zámer alebo poškodiť profesionálnu reputáciu spoločnosti.

ŽSR bude od tretích strán, ktoré pristupujú k zariadeniam a informáciám ŽSR požadovať povinné oboznámenie sa a dodržiavanie zásad uvedených v tomto dokumente.

Koniec základnej časti dokumentu

PRÍLOHA Č. 1 ŽIADOSŤ O PRIDELENIE PRÍSTUPU TRETEJ STRANE DO INFORMAČNÉHO SYSTÉMU ŽSR

Žiadosť o pridelenie prístupu tretej strane do informačného systému ŽSR

Vyplní zamestnanec ŽSR, prostredníctvom ktorého je prístup tretej strany žiadaný

Dátum žiadosti:

Údaje o tretej strane:

Meno a priezvisko/organizácia:

Adresa spoločnosti:

Telefónne číslo spoločnosti/zamestnanca:

E-mail zamestnanca, ktorý bude do informačného systému pristupovať:
Náklady na VPN budú účtované: (IS, názov organizácie, názov VOJ):
Požadovaný spôsob pripojenia (vzdialený / lokálny - popíše žiadateľ..):

Typ operačného systému a typ internetového prehliadača (typ klientskej aplikácie, použitej na prístup do IS):

Názov a verzia antivírusového programu na PC, z ktorého bude prístup realizovaný:

Názov informačného systému, do ktorého je prístup žiadaný:
Identifikačné údaje:
- Názov a IP adresy serverov:
- Plný prístup alebo len na konkrétne porty/priečinky:

Poznámka: V prípade *lokálneho* prístupu je zamestnanec ŽSR, prostredníctvom ktorého je prístup tretej strany žiadaný povinný vyšpecifikovať:

- **Číslo miestnosti:**
- **Podmienky sprevádzania:**
- **Čas udelený pre prístup (od – do): Povinný údaj! Nutné vyplniť!**
- **HW vybavenie (HW vybavenie externého partnera / HW vybavenie ŽSR):**

Účel (resp. dôvod) požadovaného prístupu:

Riziká pri neudelení prístupu:

Riziká pri udelení prístupu:

Dĺžka požadovaného prístupu od – do/dátum/hodina (Povinný údaj! Nutné vyplniť!): ***doplniť v prípade vzdialeného prístupu**

Údaje o zamestnancovi ŽSR, prostredníctvom ktorého je prístup žiadaný:

Meno a priezvisko:
Názov pracoviska:
Telefónne číslo:
E-mail:
Funkcia:

Zoznam HW prostriedkov poskytnutých tretej strane:

P.č.	Názov HW prostriedku poskytnutého tretej strane pre prístup do IS ŽSR

Prílohy:

Súčasťou tejto žiadosti môže byť **priloženie dohody / prehlásenia o ochrane dôverných informácií** podpísanej zmluvnou stranou resp. potenciálnym koncovým užívateľom podľa špecifikácie uvedenej v kapitole 3.

ŽSR sa zaväzujú zabezpečiť ochranu osobných údajov koncového užívateľa uvedeného v tejto žiadosti v súlade so zákonom č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov; to znamená okrem iného, že ŽSR tieto osobné údaje nezverejnia, nebudú ich ďalej šíriť, neposkytnú ich tretím stranám, zachovajú o nich mlčanlivosť a po splnení účelu ich spracovania, ktorým je zabezpečenie ochrany informačných systémov ŽSR, ich v stanovenej lehote zlikvidujú.

PRÍLOHA Č. 2 ŽIADOSŤ O PRIDELENIE PRÍSTUPU TRETEJ STRANE DO SIETE LAN ŽSR

Žiadosť o pridelenie prístupu tretej strane do siete LAN ŽSR

Vyplní zamestnanec ŽSR, prostredníctvom ktorého je prístup tretej strany žiadaný

Dátum žiadosti:

Údaje o tretej strane:

Meno a priezvisko/organizácia:

Adresa spoločnosti:

Telefónne číslo spoločnosti/zamestnanca:

E-mail zamestnanca, ktorý bude pristupovať do LAN ŽSR:
Náklady na VPN budú účtované: (IS, názov organizácie, názov VOJ):

Požadovaný spôsob pripojenia (vzdialený / lokálny - popíše žiadateľ..):

Identifikačné údaje:
- Názov LAN siete kde je prístup žiadaný resp. iné identifikačné údaje (IP adresa zariadenia v sieti a pod.)

Poznámka: V prípade lokálneho prístupu je zamestnanec ŽSR, prostredníctvom ktorého je prístup tretej strany žiadaný povinný vyšpecifikovať:

- **Číslo miestnosti:**
- **Podmienky sprevádzania:**
- **Čas udelený pre prístup (od – do): Povinný údaj! Nutné vyplniť!**
- **HW vybavenie (HW vybavenie externého partnera / HW vybavenie ŽSR):**

Účel (resp. dôvod) požadovaného prístupu:

Riziká pri neudelení prístupu:

Riziká pri udelení prístupu:

Dĺžka požadovaného prístupu od – do/dátum/hodina (Povinný údaj! Nutné vyplniť!): ***doplniť v prípade vzdialeného prístupu**

Údaje o zamestnancovi ŽSR, prostredníctvom ktorého je prístup žiadaný:

Meno a priezvisko:

Názov pracoviska:

Telefónne číslo:

E-mail:
Funkcia:

Zoznam HW prostriedkov poskytnutých tretej strane:

P.č.	Názov HW prostriedku poskytnutého tretej strane pre prístup do LAN ŽSR

Prílohy:

Súčasťou tejto žiadosti môže byť **priloženie dohody / prehlásenia o ochrane dôverných informácií** podpísanej zmluvnou stranou resp. potenciálnym koncovým užívateľom podľa špecifikácie uvedenej v kapitole 3.

ŽSR sa zaväzujú zabezpečiť ochranu osobných údajov koncového užívateľa uvedeného v tejto žiadosti v súlade so zákonom č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov; to znamená okrem iného, že ŽSR tieto osobné údaje nezverejnia, nebudú ich ďalej šíriť, neposkytnú ich tretím stranám, zachovajú o nich mlčanlivosť a po splnení účelu ich spracovania, ktorým je zabezpečenie ochrany informačných systémov ŽSR, ich v stanovenej lehote zlikvidujú.

PRÍLOHA Č. 3 ŽIADOSŤ O PRIDELENIE PRÍSTUPU TRETEJ STRANE DO TECHNOLOGICKÉHO ZARIADENIA ŽSR

Žiadosť o pridelenie prístupu tretej strane do technologického zariadenia ŽSR

Vyplní zamestnanec ŽSR, prostredníctvom ktorého je prístup tretej strany žiadaný

Dátum žiadosti:

Údaje o tretej strane:

Meno a priezvisko/organizácia:

Adresa spoločnosti:

Telefónne číslo spoločnosti/zamestnanca:

E-mail zamestnanca, ktorý bude pristupovať do technologického zariadenia ŽSR:
Náklady na VPN budú účtované: (IS, názov organizácie, názov VOJ):

Požadovaný spôsob pripojenia (vzdialený / lokálny - popíše žiadateľ..):

Identifikačné údaje:
Názov technologického zariadenia ŽSR, do ktorého je prístup žiadaný resp. iné identifikačné údaje (IP adresa zariadenia v sieti a pod.)

Poznámka: V prípade lokálneho prístupu je zamestnanec ŽSR, prostredníctvom ktorého je prístup tretej strany žiadaný povinný vyšpecifikovať:

- **Číslo miestnosti:**
- **Podmienky sprevádzania:**
- **Čas udelený pre prístup (od – do): Povinný údaj! Nutné vyplniť!**
- **HW vybavenie (HW vybavenie externého partnera / HW vybavenie ŽSR):**

Účel (resp. dôvod) požadovaného prístupu:

Riziká pri neudelení prístupu:

Riziká pri udelení prístupu:

Dĺžka požadovaného prístupu od – do/dátum/hodina (Povinný údaj! Nutné vyplniť!): ***doplniť v prípade vzdialeného prístupu**

Údaje o zamestnancovi ŽSR, prostredníctvom ktorého je prístup žiadaný:

Meno a priezvisko:

Názov pracoviska:

Telefónne číslo:

E-mail:

Funkcia:

Zoznam HW prostriedkov poskytnutých tretej strane:

P.č.	Názov HW prostriedku poskytnutého tretej strane pre prístup do technologického zariadenia ŽSR

Prílohy:

Súčasťou tejto žiadosti môže byť **priloženie dohody / prehlásenia o ochrane dôverných informácií** podpísanej zmluvnou stranou resp. potenciálnym koncovým užívateľom podľa špecifikácie uvedenej v kapitole 3.

ŽSR sa zaväzujú zabezpečiť ochranu osobných údajov koncového užívateľa uvedeného v tejto žiadosti v súlade so zákonom č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov; to znamená okrem iného, že ŽSR tieto osobné údaje nezverejnia, nebudú ich ďalej šíriť, neposkytnú ich tretím stranám, zachovajú o nich mlčanlivosť a po splnení účelu ich spracovania, ktorým je zabezpečenie ochrany informačných systémov ŽSR, ich v stanovenej lehote zlikvidujú.

PRÍLOHA Č. 4 ŽIADOSŤ O PRÍSTUP DO IS, SW, APLIKÁCIE Z DÔVODU ÚDRŽBY

Žiadosť o pridelenie prístupu dodávateľovi z dôvodu správy, údržby, opravy ním nasadeného IS/softvéru/aplikácie

Vyplní zamestnanec ŽSR, prostredníctvom ktorého je prístup tretej strany žiadaný.

Dátum žiadosti:

Údaje o tretej strane:

Meno a priezvisko/organizácia:

Adresa spoločnosti:

Telefónne číslo spoločnosti/zamestnanca:

E-mail zamestnanca, ktorý bude do IS/SW/aplikácie pristupovať:
Náklady na VPN budú účtované: (IS, názov organizácie, názov VOJ):

Požadovaný spôsob pripojenia (vzdialený / lokálny - popíše žiadateľ..):

Typ operačného systému a typ internetového prehliadača (typ klientskej aplikácie, použitej na prístup do IS) + názov a verzia antivírusového programu na PC, z ktorého bude prístup realizovaný:
Kam dodávateľ pristupuje:

☐ **Informačný systém**
Názov informačného systému, do ktorého je prístup žiadaný:
Identifikačné údaje:
- Názov a IP adresy serverov:
- Plný prístup alebo len na konkrétne porty/priečinky:

☐ **Aplikácia**
Názov aplikácie, do ktorej je prístup žiadaný:
Identifikačné údaje:
- verzia:

Poznámka: V prípade lokálneho prístupu je zamestnanec ŽSR, prostredníctvom ktorého je prístup tretej strany žiadaný povinný vyšpecifikovať:

- **Číslo miestnosti:**
- **Podmienky sprevádzania:**
- **Čas udelený pre prístup (od – do): Povinný údaj! Nutné vyplniť!**
- **HW vybavenie (HW vybavenie externého partnera / HW vybavenie ŽSR):**

Účel požadovaného prístupu:

Riziká pri neudelení prístupu:

Riziká pri udelení prístupu:

Dĺžka požadovaného prístupu od – do/dátum/hodina (Povinný údaj! Nutné vyplniť!): ***doplniť v prípade vzdialeného prístupu**

Údaje o zamestnancovi ŽSR, prostredníctvom ktorého je prístup žiadaný:

Meno a priezvisko:
Názov pracoviska:
Telefónne číslo:
E-mail:
Funkcia:

Zoznam HW prostriedkov poskytnutých tretej strane:

P.č.	Názov HW prostriedku poskytnutého tretej strane pre prístup do IS/SW/aplikácie z dôvodu správy, údržby, opravy dodávateľom nasadeného produktu

Prílohy:

Súčasťou tejto žiadosti môže byť **priloženie dohody / prehlásenia o ochrane dôverných informácií** podpísanej zmluvnou stranou resp. potenciálnym koncovým užívateľom podľa špecifikácie uvedenej v kapitole 3.2

ŽSR sa zaväzujú zabezpečiť ochranu osobných údajov koncového užívateľa uvedeného v tejto žiadosti v súlade so zákonom č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov; to znamená okrem iného, že ŽSR tieto osobné údaje nezverejnia, nebudú ich ďalej šíriť, neposkytnú ich tretím stranám, zachovajú o nich mlčanlivosť a po splnení účelu ich spracovania, ktorým je zabezpečenie ochrany informačných systémov ŽSR, ich v stanovenej lehote zlikvidujú.

PRÍLOHA Č. 5

Vzor Vyjadrenia Odboru telekomunikácií, informatiky a informačnej bezpečnosti k žiadosti o pridelenie prístupu tretej strane

Vyjadrenie Odboru telekomunikácií, informatiky a informačnej bezpečnosti k žiadosti o pridelenie prístupu tretej strane:

Odbor telekomunikácií, informatiky a informačnej bezpečnosti môže po dôkladnom prešetrení zamietnuť žiadosť o pridelenie prístupu do informačných systémov s udaním dôvodu.

Odbor telekomunikácií, informatiky a informačnej bezpečnosti žiadosť o pridelenie prístupu do definovaného KIS uvedeného v priloženej žiadosti:

Schvaľuje/Neschvaľuje **nehodiace prečiarknuť*

Odôvodnenie **v prípade negatívnej odpovede O210 GR ŽSR*

O210 GR ŽSR na základe priloženej žiadosti schvaľuje prístup tretej strany pre nasledovných používateľov zo spoločnosti XXX:

- Meno a priezvisko zamestnanca/osoby, ktorý bude do systému pristupovať

Prístup na:

Tu uviesť konkrétnu časť siete do ktorej je požadovaný prístup, konkrétne IP adresy, servery.

Pre účely:

- Tu uviesť na základe čoho sa prístup požaduje. Napr. na základe zmluvy o poskytovaní služieb č. xxx
- Náklady na zriadenie a prevádzkovanie účtovať na:

Tretia strana je povinná podpísať prílohu č. 7/Prehlásenie o odchrane dôverných informácií/, prípadne prílohu č.6 /Dohoda o ochrane dôverných informácií a skutočností tvoriacich obchodné tajomstvo č.xx/201X (NDA)/ Smernice Bezpečnostná politika KIS alebo predložiť platnú zmluvu o prístupe do siete KIS, ktorá obsahuje ustanovenia v zmysle Prílohy č. 6 prípadne Prílohy č.7

Dátum schválenia

Projektový manažér bezpečnosti

PRÍLOHA Č. 6

Dohoda o ochrane dôverných informácií

a skutočností tvoriacich obchodné tajomstvo

č. xx/201X/NDA.

uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. v platnom znení (Obchodný zákonník, ďalej len „ObZ“), na účely ochrany oprávnených záujmov v súvislosti s prípravou produktu ŽSR a plnením Zmluvy o poskytovaní služby ŽSR ak bude uzatvorená (ďalej len “Dohoda”), medzi týmito stranami

obchodné meno:	***Železnice Slovenskej republiky, Bratislava v skrátenej forme „ŽSR“***
so sídlom:	Klemensova 8, 813 61 Bratislava
štatutárny orgán :	Ing. Dušan Šefčík, generálny riaditeľ ŽSR
IČO:	31 364 501
IČ DPH:	SK2020480121
bankové spojenie:	VÚB, a.s., číslo účtu: 35-4700012/0200
IBAN:	SK1102000000350004700012
BIC:	SUBASKBX

Osoba oprávnená na podpis dohody:
iná právnická osoba zapísaná v Obchodnom registri vedenom pri Okresnom súde Bratislava I, odd. Po, vl.č. 312/B

(ďalej aj ako „ŽSR“)

a

so sídlom:
štatutárny orgán:
IČO:
IČ DPH:
DIČ:
bankové spojenie:
v zastúpení:
IBAN:
BIC:
obchodná spoločnosť zapísaná v Obchodnom registri vedenom pri Okresnom súde , odd. , vl.č.

(ďalej aj ako „*Zmluvná strana*“)

Článok I

Predmetom tejto Dohody je ochrana dôverných informácií a skutočností, ktoré tvoria obchodné tajomstvo a ktoré sa stanú známymi *Zmluvnej strane* v súvislosti s prezentáciami a rokovaniami o podmienkach produktov ŽSR (ďalej len ako „Produkt“), ako aj v súvislosti s prípravou a plnením Zmluvy o poskytovaní služby ŽSR.

Článok II

- Dôvernými informáciami sú v zmysle § 271 ObZ, podľa tejto Dohody všetky informácie, ktoré pri rokovaní o uzatvorení Zmluvy o poskytovaní služby ŽSR poskytne ŽSR, ak boli ako dôverné označené, a tiež také informácie, ktorých poskytnutie tretím osobám môže spôsobiť ŽSR majetkovú alebo nemajetkovú ujmu, pričom takéto dôsledky možno pri dodržaní primeranej starostlivosti predpokladať.
- Zmluvná strana, ktorej sa informácie podľa ods. 1 tohto článku poskytnú, je povinná s nimi nakladať s primeranou starostlivosťou, dobromyseľne, pokiaľ ide o záujmy ŽSR, nesmie také informácie prezradiť tretej osobe a ani ich použiť v rozpore s účelom na ktorý boli poskytnuté, pre svoje potreby, a to bez ohľadu na to, či dôjde k uzavretiu Zmluvy o poskytovaní služby ŽSR alebo nie.
- Obchodným tajomstvom sú v zmysle § 17 ObZ a podľa tejto Dohody všetky skutočnosti obchodnej, výrobnej alebo technickej povahy v hmotnej alebo nehmotnej forme, ktoré boli takto označené ŽSR a poskytnuté druhej strane, pričom nie sú v príslušných obchodných kruhoch bežne dostupné a ich utajenie a tomu zodpovedajúci spôsob zabezpečenia ich ochrany je v záujme ktorejkoľvek zo strán.

- Podľa tejto Dohody sú predmetom obchodného tajomstva :

(1) ceny produktov ŽSR a súvisiacich služieb, ktoré nie sú zverejnené
(2) zápisy zo stretnutí rokujúcich strán týkajúcich sa uzavretia Zmluvy o poskytovaní služby ŽSR, vrátane príloh,
(3) podklady a informácie pre prípravu Zmluvy o poskytovaní služby ŽSR s prílohami,
(4) ďalšie podklady a informácie, ktoré si rokujúce strany navzájom poskytli a ktoré sú predmetom obchodného tajomstva, ak sú takto označené.

Článok III

- Zmluvná strana, ktorej sa poskytnú informácie podľa tejto Dohody sa zaväzuje, že všetky dôverné informácie a skutočnosti tvoriace obchodné tajomstvo podľa tejto Dohody použije len na účely prípravy a plnenia Zmluvy o poskytovaní služby ŽSR, nebude ich ďalej rozširovať, reprodukovať a nesprístupní ich tretím osobám. Súčasne sa zaväzuje, že zabezpečí, aby všetky obdŕžané dokumenty, analýzy, či iné podklady obsahujúce dôverné informácie alebo skutočnosti, ktoré sú predmetom obchodného tajomstva boli riadne evidované.
- Strany Dohody zabezpečia taký obmedzený počet osôb, ktorým budú informácie chránené podľa tejto Dohody prístupné a prijmú také účinné opatrenia na zamedzenie ich úniku, aby bol zodpovedajúcim spôsobom dosiahnutý účel tejto Dohody.
- V prípade, že strane, ktorej sa poskytnú informácie, vyplynie nevyhnutnosť poskytnúť informácie a skutočnosti, ktoré sú predmetom ochrany podľa tejto Dohody tretej strane, na účely zabezpečenia činnosti, môže také informácie a skutočnosti poskytnúť len na základe predchádzajúceho písomného súhlasu ŽSR. Povinnosť predchádzajúceho písomného súhlasu sa neuplatní, ak treťou stranou je osoba, ktorá poskytuje Zmluvnej strane právnu alebo konzultantskú službu, bezprostredne súvisiacu s obsahom tejto Dohody. V takom prípade je Zmluvná strana povinná ŽSR bezodkladne písomne oznámiť identifikačné údaje takejto tretej strany. Povinnosť predchádzajúceho písomného súhlasu sa ďalej

nevyžaduje v prípade, že ide o poskytnutie informácie orgánu verejnej správy alebo inému subjektu, ak to ukladá všeobecne záväzný právny predpis alebo vykonateľné správne alebo súdne rozhodnutie.

- Povinnosť mlčanlivosti podľa tejto Dohody sa nevzťahuje na také dôverné informácie a skutočnosti tvoriace predmet obchodného tajomstva, ktoré:

(1) boli písomným súhlasom ŽSR vyňaté z režimu podľa tejto Dohody,
(2) sú alebo stali sa známymi inak než porušením tejto Dohody,
(3) sa stali ich príjemcovi známe ešte predtým, než mu ich poskytla niektorá zo strán,
(4) boli vyžiadané súdmi, orgánmi prokuratúry alebo iným vecne príslušným správnym orgánom na základe zákona.

- Poskytnutie dôverných informácií alebo skutočností tvoriacich obchodné tajomstvo nezakladá žiadne právo na licenciu, ochrannú známku, patent, právo na použitie alebo verejné rozširovanie diela, ani akékoľvek iné právo duševného alebo priemyselného vlastníctva.
- Zmluvná strana podpisom tejto dohody zároveň potvrdzuje, že sa oboznámila s obsahom dokumentu „Bezpečnostná politika KIS“, ktorý je zverejnený na webovej stránke ŽSR , súhlasí s tam uvedenými podmienkami a zaväzuje sa ich dodržiavať.

Článok IV

(1) Porušením povinností Zmluvnej strany týkajúcich sa ochrany dôverných informácií a skutočností tvoriacich obchodné tajomstvo podľa tejto Dohody, vzniká ŽSR právo požadovať zaplatenie zmluvnej pokuty a náhrady škody vzniknutej porušením povinnosti podľa tejto Dohody.
(2) Výška zmluvnej pokuty je dohodnutá na sumu 33193 € (slovom: tridsaťtritisícstodeväťdesiattri eur).
(3) Zmluvná pokuta, na ktorú vznikne ŽSR podľa tejto Dohody nárok, je druhá strana povinná uhradiť do pätnástich (15) kalendárnych dní odo dňa doručenia výzvy na jej úhradu.

Článok V

- Táto Dohoda nadobúda platnosť a účinnosť dňom jej podpísania oprávnenými zástupcami oboch strán Dohody.
- Platnosť tejto Dohody zaniká v prípade, že nedôjde k uzatvoreniu Zmluvy o poskytovaní služby ŽSR medzi ŽSR a Zmluvnou stranou uplynutím troch (3) rokov od okamihu posledného rokovania strán Dohody. V prípade, ak výsledkom vzájomných rokovaní bude uzatvorenie Zmluvy o poskytovaní služby ŽSR medzi ŽSR a Zmluvnou stranou, uplynutím troch (3) rokov od zániku Zmluvy o poskytovaní služby ŽSR.
- Záväzok chrániť dôverné informácie a skutočnosti tvoriace obchodné tajomstvo podľa tejto Dohody, ak tieto boli poskytnuté pred dňom ukončenia jej platnosti, trvá naďalej, a to po dobu troch (3) rokov odo dňa ukončenia platnosti tejto Dohody.
- Túto Dohodu možno meniť, upravovať, rozširovať a dopĺňať len na základe dohody oboch zmluvných strán vo forme písomných dodatkov.
- Táto Dohoda a právne vzťahy z nej vyplývajúce sa riadi výlučne právnym poriadkom Slovenskej republiky.
- Táto Dohoda nezakladá žiadnej zo strán povinnosť uzatvoriť Zmluvu o poskytovaní služby ŽSR.
- Táto Dohoda sa vyhotovuje v písomnej forme, v štyroch rovnopisoch, pričom každá zo strán obdrží jej dve podpísané vyhotovenia.

V Bratislave, dňa V , dňa

Za ŽSR Za *Zmluvnú stranu*

PRÍLOHA Č. 7 PREHLÁSENIE O OCHRANE DÔVERNÝCH INFORMÁCIÍ

Prehlásenie o ochrane dôverných informácií získaných prístupom do IKT prostredia ŽSR.

obchodné meno, názov PO/ FO podnikateľa:	
meno, priezvisko FO:	
Sídlo PO/miesto podnikania FO podnikateľa:	
Adresa FO:	
IČO, obchodný register/číslo zápisu podnikateľa:	
ČOP, dátum narodenia FO:	
Zástupca PO/podnikateľa oprávnený na podpis prehlásenia (meno, priezvisko, funkcia, adresa trvalého bydliska):	

(ďalej aj „koncový užívateľ“)

Zástupca PO/podnikateľa oprávnený na podpis prehlásenia svojim podpisom potvrdzuje, že zodpovedá za porušenie povinností stanovených týmto prehlásením svojimi zamestnancami, ktorí na základe jeho poverenia získali prístup do IKT prostredia ŽSR.

Koncový užívateľ sa podpisom tohto prehlásenia:

(1) zaväzuje, že v zmysle nižšie uvedených ustanovení nepoužije, nezneužije a neodovzdá tretím osobám údaje o elektronickej komunikačnej sieti, elektronických komunikačných službách a informačno - komunikačných technológiách ŽSR (ďalej „IKT prostredie“)

(2) zaväzuje, že vykoná také opatrenia, ktoré znemožnia zneužitie prístupu do IKT prostredia neoprávnenou osobou. Za dôsledky takého zneužitia zodpovedá koncový užívateľ

(3) zaväzuje využívať schválený prístup do IKT prostredia len na dohodnuté účely

(4) zaväzuje v nevyhnutnom prípade zabezpečiť taký obmedzený počet osôb, ktorým budú informácie chránené podľa tohto prehlásenia prístupné a prijať také účinné opatrenia na zamedzenie ich úniku, aby bol zodpovedajúcim spôsobom dosiahnutý účel tohto prehlásenia

(5) zaväzuje v prípade spôsobenia škody v súvislosti so vstupom a pôsobením v IKT prostredí nahradiť ŽSR všetky vzniknuté škody, ktoré vznikli hoci aj z nedbanlivosti alebo ktoré spôsobil koncový užívateľ alebo iná osoba, ktorej koncový užívateľ umožnil uskutočnenie akéhokoľvek zásahu

(6) zaväzuje držať v tajnosti obchodné tajomstvo, duševné vlastníctvo (vrátane know-how), všetky informácie získané v súvislosti s prístupom do IKT prostredia, ktoré nie sú verejne prístupné a sú pri ich poskytnutí primerane označené ako dôverné a ktoré za dohodnutým účelom získal od ŽSR. Držať dôverné informácie v tajnosti znamená zákaz odhalenia dôverných informácií tretej strane (iným ako právnym či iným poradcom a osobám pracujúcim na plnení takéhoto účelu) bez predchádzajúceho písomného súhlasu ŽSR .

Za dôverné sa považujú najmä informácie :
a) ktorých obsah ŽSR podľa svojho vyhlásenia považuje, ochraňuje a ochranu aj primeraným spôsobom zabezpečuje,
b) s charakterom obchodného tajomstva; obchodné tajomstvo tvoria všetky skutočnosti obchodnej, výrobnej a technickej povahy súvisiace so ŽSR, ktoré majú skutočnú alebo aspoň potenciálnu materiálnu alebo nemateriálnu hodnotu, nie sú v príslušných obchodných kruhoch bežne dostupné, majú byť podľa vôle ŽSR utajené a ŽSR ich utajenie zodpovedajúcim spôsobom zabezpečuje.
Ustanovenia tohto prehlásenia sa nevzťahujú na žiadne dôverné informácie, ktoré:
a) sú alebo sa stali verejnosti známe bez akéhokoľvek porušenia záväzkov koncového užívateľa
b)boli známe koncovému užívateľovi ešte pred vstupom do IKT prostredia alebo mu boli poskytnuté treťou stranou ako informácie, ktoré nie sú dôverné, pričom táto tretia strana neporušila vlastnú povinnosť mlčanlivosti; alebo
c)sú náležite sprístupnené na základe nariadenia súdu s rozhodnou právomocou alebo iného regulačného orgánu s tým, že v tomto prípade koncový užívateľ, ktorý je povinný informácie sprístupniť, bude okamžite informovať ŽSR pred sprístupnením informácií.
d)musia byť zverejnené na základe zákona.
Koncový užívateľ ďalej berie na vedomie a súhlasí, že ŽSR nenesie žiadnu zodpovednosť za škodu spôsobenú koncovému užívateľovi zariadením vo vlastníctve ŽSR, prostredníctvom ktorého je koncovému užívateľovi poskytovaná služba, za predpokladu, že škoda nebola spôsobená zavinením zo strany ŽSR.
Koncový užívateľ podpisom tohto prehlásenia vyhlasuje, že sa oboznámil s obsahom dokumentu „Bezpečnostná politika“, ktorý je zverejnený na webovej stránke ŽSR, súhlasí s tam uvedenými podmienkami a zaväzuje sa ich dodržiavať.

Koncový užívateľ alebo Splnomocnený zástupca PO/podnikateľa:
.....
(meno, priezvisko, funkcia)
ŽSR sa zaväzujú zabezpečiť ochranu osobných údajov koncového užívateľa uvedeného v tomto prehlásení v súlade so zákonom č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov; to znamená okrem iného, že ŽSR tieto osobné údaje nezverejnia, nebudú ich ďalej šíriť, neposkytnú ich tretím stranám, zachovajú o nich mlčanlivosť a po splnení účelu ich spracovania, ktorým je zabezpečenie ochrany informačných systémov ŽSR, ich v stanovenej lehote zlikvidujú.

V nasledujúcej tabuľke je uvedený prehľad ďalších právnych aktov, záväzných pre Slovenskú republiku z dôvodu členstva v Európskej únii, Organizácii pre ekonomickú spoluprácu a rozvoj, Organizácii Spojených národov a Organizácii Severoatlantickej zmluvy. Z informačno-bezpečnostného hľadiska sú príslušné nielen všetky zákonné normy, ktoré upravujú podmienky používania informačných a komunikačných technológií, ale aj tie, ktoré umožňujú spracovanie informácií v elektronickej podobe.