

Železnice Slovenskej republiky
Železničné telekomunikácie Bratislava

Klasifikácia v zmysle ISMS: D

Smernica

**Požiadavky na ICT systémy a technológie odovzdávané do prevádzky
v datacentre ŽSR a v sieťovej infraštruktúre ŽSR**

Spracovateľský / gestorský útvar Ing. Matej Samel, SP; Ing. Jarmila Šoková, SPr; Ing. Zuzana Masaryková, SR / SKIB	Číslo 00988/2025/ŽT/SKIB 00977/2025	Označenie O-04-ŽT-2025
Účinnosť od <div style="text-align: right;">Dňom vydania</div>		
Schválil Ing. Martin Lukáčik riaditeľ Železničných telekomunikácií	Dňa 7.4.2025	

Predmet Prevádzka ŽT	Ruší
Prílohy PRÍLOHA č.1: Minimálne požiadavky na bezpečnostné opatrenia pre komponenty základných služieb	
Súvisiace interné riadiace akty Smernica prevádzková podpora ICT systémov a technológií	

SLEDOVANIE VYDANÍ A ZMIEN DOKUMENTU

Zoznam vydaní dokumentu

Vydané pod číslom	Účinnosť od - do
00988/2025/ŽT/SKIB	
00977/2025	7.4.2025 -

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. Ich znenie i znenie dokumentu so zapracovanými zmenami sú umiestnené (zverejnené) v elektronickej podobe v dokumentovom úložisku IP.

Za včasné zapracovanie zmien v texte a za vykonanie záznamu o zmenách zodpovedá držiteľ výtlačku.

Smernica R ŽT Požiadavky na ICT systémy a technológie odovzdávané v datacentre ŽSR	Strana 2 z 12	O-04-ŽT-2025
---	---------------	--------------

Obsah

1.	Konzistentnosť dát	7
2.	Bezpečnosť.....	7
3.	Správa používateľov.....	8
4.	Archivácia dát	8
5.	Prevádzkovateľnosť	8
6.	Rozhrania na iné aplikácie / zariadenia	8
7.	Servisovateľnosť	9
8.	Monitorovateľnosť.....	9
9.	Dostupnosť	10
10.	Termíny aktualizácie kmeňových dát.....	10
11.	Definovanie kompetencií po odovzdaní do prevádzky	10
12.	Technologické štandardy prevádzky IT	10
13.	Licenčné požiadavky	11
14.	SLA požiadavky.....	11
15.	Požiadavky na ochranu osobných údajov	11
16.	Prílohy	12

Rozsah znalostí

Organizačná zložka	Znalosť
Vedúci zamestnanci, projektoví manažéri, zamestnanci Sekcie prevádzky, zamestnanci SKIB	úplná
Ostatní zamestnanci	informatívna

Zoznam použitých skratiek

ICT	Informačné a telekomunikačné technológie
HW	Hardware
SW	Software
IP	Intranetový portál
OS	Operačný systém
DB	Databáza
SP	Sekcia prevádzky
SPr	Sekcia produktov
SR	Sekcia rozvoja
SKIB	Sekcia kybernetickej a informačnej bezpečnosti
CVE	Common Vulnerabilities and Exposures
Z.z.	Zbierky zákonov
VPN	Virtual private network (Virtuálna privátna sieť)
BP KIS	Bezpečnostná politika komunikačno-informačných systémov
GDPR	General Data Protection Regulation (Všeobecné nariadenie o ochrane údajov)
DC ŽSR	datacentrum ŽSR
MFA	viac faktorová autentifikácia

Úvod

Táto smernica popisuje základné požiadavky ŽSR pre odovzdávanie ICT systémov a technológií do prevádzky v datacentre ŽSR a v sieťovej infraštruktúre ŽSR.

ICT systémom v tomto dokumente sa rozumie IT a EKS aplikácie, alebo ich komplex.

Technológiou v tomto dokumente sa rozumie všetko, čo je využité v dátovom centre ŽSR a koncové technologické zariadenia (vrátane sieťových komponentov) nasadené na sieťovej infraštruktúre, ktoré sú nevyhnutné pre prevádzkovanie produktov a poskytovanie služieb ICT. Technológia môže byť reprezentovaná HW, SW (vrátane predplatenej podpory-subscription), sieťovými prvkami, ktoré sú dodávané vendorom priamo, alebo partnerom vendora.

Každý ICT systém a technológia, ktorá sa nasadzuje do produkčnej prevádzky musí spĺňať požiadavky popísané v tejto smernici.

1. Konzistentnosť dát

- ukladané dáta na disk budú konzistentné i po prípadnom výpadku systému,
- vytvorenie konzistentnej zálohy a jej uloženie v zálohovacom systéme, t.j. musí obsahovať prepojenie s externým zálohovacím systémom,
- konzistentnú obnovu dát zo zálohovacieho systému, t.j. musí obsahovať prepojenie s externým zálohovacím systémom.

2. Bezpečnosť

- dáta nesmú byť uložené v súborovom systéme v čitateľnej forme,
- do ICT systému alebo technológie nesmie byť priamy prístup z lokálneho servera, t.j. aj lokálne prihlásený užívateľ sa musí autentifikovať na úrovni aplikácie,
- ICT systém alebo technológia musí vedieť obmedziť prístup k dátam podľa rôznych typov užívateľov,
- IS alebo aplikácie dostupné z internetu musia podporovať implementáciu mechanizmov MFA autentifikácie,
- ICT systém alebo technológia a musí vedieť auditovať prístupy užívateľov k dátam,
- v prípade cloudových riešení zabezpečiť bezpečnosť na úrovni OS/DB,
- informačný systém alebo aplikácia pred nasadením do prevádzky musí prejsť testami na bezpečnosť podľa metodológie OWASP (alebo alternatívneho štandardu), tzn. dodávateľ predloží dôkaz/výstup o uskutočnení takéhoto testovania,
- v prípade implementácie do architektúry ICT systému alebo technológie treťostranných modulov (knihnice, pluginy, skripty, atď) musí ICT systém alebo technológia spĺňať bezpečnostné kritéria v každej fáze jej prevádzkovania,
- v prípade, že dodávateľ ICT systému alebo technológie zistí bezpečnostnú zraniteľnosť, bezodkladne zašle prostredníctvom styčnej osoby prevádzkovateľovi informáciu o svojich zisteniach spolu s návrhom na ich odstránenie,
- v prípade, ak objednávateľ zistí bezpečnostné zraniteľnosti ICT systému alebo technológie, dodávateľ je povinný bezodplatne poskytnúť súčinnosť pri ich analýze a vykonať nápravy na ich odstránenie,
- počas trvania realizácie diela, počas záručnej doby alebo počas doby poskytovania podpory je dodávateľ povinný pravidelne zisťovať a odstraňovať na vlastné náklady zistené bezpečnostné zraniteľnosti dodávaného ICT systému alebo technológie,
- v každej fáze prevádzkovania ICT systému alebo technológie je povinnosťou dodávateľa poskytovať informáciu objednávateľovi (resp. súčinnosť pri inštalácii) o bezpečnostných záplatách pri známych bezpečnostných zraniteľnostiach (MITRE CVE), vrátane zraniteľnosti treťostranných modulov,
- v prípade klasifikácie ICT systému alebo technológie, alebo jeho časti ako komponentu Základnej Služby v zmysle zákona 69/2018 o kybernetickej bezpečnosti musí dodávateľ zabezpečiť implementáciu bezpečnostných opatrení a odporúčaní v zmysle vyhlášky 362/2018 Z.z, minimálne však v zmysle PRÍLOHY č.1.: *Minimálne požiadavky na bezpečnostné opatrenia pre komponenty základných služieb*,
- Prevádzková dokumentácia musí obsahovať popis bezpečnostnej architektúry ICT systému, alebo technológie vrátane komunikačnej matice/mapy (popis portov a protokolov nevyhnutných pre bezchybné fungovanie systému).

3. Správa používateľov

- ICT systém alebo technológia musí poskytovať autentifikáciu voči externému prostrediu,
- prevádzková dokumentácia musí obsahovať popis zabudovaných rolí a jednotlivých oprávnení a postupy pre zabezpečenie ich životného cyklu (zriadenie, modifikácia, zrušenie),
- dodávateľ zabezpečí integráciu ICT systému alebo technológie do existujúcich systémov ŽSR používaných na správu privilegovaných účtov,
- správa používateľov musí byť odovzdaná na správu účtov ŽT.

4. Archivácia dát

- archivácia dát musí byť implementovaná, už pri spustení ICT systému alebo technológie do prevádzky,
- formát archivovaných informácií musí byť taký, aby ho vedel ICT systém alebo technológia použiť i na konci archivačného obdobia, t.j. ak je nutná archivácia na 10 rokov, aplikácia musí zabezpečiť, že archivované dáta prečíta i o 10 rokov.

5. Prevádzkovateľnosť

ICT systém alebo technológia:

- musí obsahovať jednoznačne definovaný postup na svoje spustenie a zastavenie,
- musí byť dodaná tak, aby mohla byť spúšťaná, stopovaná z externého „scheduling“ systému,
- musí byť prevádzkovateľná na PC so schváleným jednotným klientom na ŽSR,
- musí byť odovzdaná do prevádzky tak, že bude funkčná na akomkoľvek zariadení: PC/NB/MT/monitoroch od rozlíšenia FHD až po 4k,
- musí byť inštalovaná v datacentre ŽSR, musí byť prevádzkovateľná na HW a SW vybavení datacentra ŽSR,
- musia byť definované obmedzenia na patchovanie OS, DB a SW,
- je vyvíjaná na vývojovom prostredí u dodávateľa,
- vývojové prostredie dodávateľa musí byť minimálne na takých verziách ako je prevádzkové a testovacie prostredie u prevádzkovateľa.

6. Rozhrania na iné aplikácie / zariadenia

ICT systém alebo technológia:

- musí umožňovať zistiť nedostupnosť rozhrania na externé aplikácie,
- musí umožňovať zistiť nedostupnosť externých senzorov, snímačov,
- musí byť spustiteľná pri nedostupnosti externých aplikácií / zariadení.

7. Servisovateľnosť

ICT systém alebo technológia:

- musí byť možné aktualizovať, pričom musí byť jednoznačne možné identifikovať, či bol aktualizovaný úspešne, alebo neúspešne,
- musí byť schopná online aktualizácie,

iné:

- externý prístup dodávateľa do ICT systému alebo technológie definovanej v dodávateľskej zmluve bude zriadený po splnení podmienok BP KIS na požiadanie prístupom do VPN. Prístup môže byť riadený ďalšími bezpečnostnými aplikáciami, ktoré môžu zaznamenávať reláciu prihláseného používateľa. Žiadosť na udelenie výnimky zo strany dodávateľa, bude posúdená podľa platných procesov,
- v prípade, že ICT systém alebo technológia využíva ďalšie objekty, komponenty alebo aplikácie nevyhnutné k svojej prevádzke, musí byť ICT systém alebo technológia prevádzkovateľná s aktuálne podporovanými verziami objektov, komponentov alebo aplikáciami podporného SW / systémov počas platnosti zmluvy. V prípade objavenia bezpečnostnej zraniteľnosti aplikácie a súvisiacich objektov, komponentov a aplikácií musí byť po dobu platnosti zmluvy, zabezpečená možnosť ich aktualizácie na verziu bez bezpečnostných zraniteľností, so zachovaním funkcionality aplikácie,
- v každej fáze prevádzkovania musí byť ICT systém alebo technológia udržiavaná v aktualizovanom stave, vrátane implementovaných prvkov do architektúry treťostranných modulov (knihnice, pluginy, skripty, atď.) počas celej doby platnosti zmluvy,
- pri každej aktualizácii je dodávateľ povinný poskytnúť popis (Release notes) k aktualizácii, vrátane aktualizácie treťostranných modulov. Daný popis musí obsahovať minimálne zoznam aktualizovaných modulov s popisom, ktoré zraniteľnosti, alebo chyby boli odstránene,
- V prípade vývoja aplikácie na žiadosť ŽSR, je potrebné definovať vlastníka zdrojového kódu.

8. Monitorovateľnosť

ICT systém alebo technológia:

- musí umožňovať zistiť v ktoromkoľvek čase stav všetkých jej komponentov,
- musí vytvárať chybové hlásenia a minimálne ich zaznamenávať do logovacieho súboru,
- musí obsahovať popis všetkých možných chybových hlásení, ktoré môže vyprodukovať,
- musí byť schopná cez API rozhranie posilať chybové hlásenia do externého event management systému,

- musí byť schopná monitorovať svoje interné prostredia (nie operačný systém) a podľa nastavených kritérií posielat' varovné hlásenia – Early Warning System,
- musí byť schopná poskytovať interné výkonnostné parametre tak, aby bolo možné sledovať jej výkonnosť,
- musí zabezpečiť logovanie stavov,
- musí byť dodávateľom popísaný z hľadiska logovaných stavov.

9. Dostupnosť

ICT systém alebo technológia:

- musí byť škálovateľná tak, aby bola jej výkonnosť z pohľadu klienta rovnaká minimálne počas 3 ročnej prevádzky,
- pokiaľ je zaradený ako kritický, musí byť do prevádzky dodávaný v high available konfigurácii.

10. Termíny aktualizácie kmeňových dát

Ku každému odovzdávanému ICT systému alebo technológií dodať :

- zoznam tabuliek, s ktorými daná pracuje,
- kategorizáciu dát (prevádzkové/kmeňové/osobné údaje),
- popis kedy archivovať/aktualizovať,
- popis ako archivovať/aktualizovať,
- termín zapracovania dodaných podkladov do požadovaných tabuliek v DB,
- zdroj a spôsob dodania podkladov pre aktualizáciu kmeňových údajov.

11. Definovanie kompetencií po odovzdaní do prevádzky

- počas implementácie dodávateľ bude mať pre nasadenie požadované kompetencie (DB, OS atď.),
- po ukončení implementácie budú kompetencie odovzdané prevádzkovateľovi,
- kompetencie, ktoré budú ponechané dodávateľovi po odovzdaní diela budú definované po vzájomnej dohode medzi prevádzkovateľom a dodávateľom.

12. Technologické štandardy prevádzky IT

Každý ICT systém alebo technológia odovzdaná do IT prevádzky by mala byť prevádzkovaná len v rámci technologických štandardov IT prevádzky:

- Operačný systém: LINUX (RHEL), Microsoft
- Databáza: Oracle, MS SQL
- WEB server, Aplikačný server, Middleware: IIS, Tomcat
- Virtualizačná platforma: VMWare
- Zálohovanie: Veeam

- Podpora vzdialeného logovania: HTTPS, syslog

13. Licenčné požiadavky

Každý ICT systém alebo technológia musí mať preukázateľne zdokladované licenčné zabezpečenie pre datacentrum ŽSR všetkých jej implementovaných komponentov, ktoré vyžadujú licenčnú ochranu.

14. SLA požiadavky

Každý nový ICT systém alebo technológia musí byť dodávaná so Service Level Agreementom, kde sa minimálne zadefinuje:

- aké dostupnosti business oddelenie očakáva,
- ako sa budú tieto dostupnosti merať,
- ako dlho môžu trvať a ako často môžu byť plánované odstávky,
- periodicita aktualizácie nových verzií,
- predpokladaný počet používateľov, ktorí ju budú využívať.

15. Požiadavky na ochranu osobných údajov

V prípade, že sa budú v ICT systéme alebo technológii spracúvať osobné údaje musí byť zabezpečená špecificky navrhnutá a štandardná ochrana osobných údajov a ich bezpečnosť spracúvania podľa čl. 25 a 35 Nariadenia GDPR a Prílohy k vyhláske č. 158/2018 Z. z., najmä prostredníctvom týchto opatrení:

- šifrová ochrana uložených a prenášaných osobných údajov alebo ich pseudonymizácia,
- riadenie prístupov (napr. identifikácia, autentizácia a autorizácia osôb v informačnom systéme, (aplikácii)),
- minimalizácia práv oprávnených osôb na princípe zásady najnižších privilégií,
- riadenie privilegovaných prístupov,
- zaznamenávanie prístupu a aktivít poverených osôb,
- pravidelná aktualizácia operačných systémov a programového aplikačného vybavenia,
- zhromažďovanie informácií o technických zraniteľnostiach informačných systémov (aplikácii), vyhodnocovanie úrovne rizík a implementácia opatrení na potlačenie týchto rizík,
- kontrola, obmedzenie alebo zamedzenie prepojenia ICT systému alebo technológie (aplikácii), v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou,
- ICT systém alebo technológia musí umožňovať bezpečné vymazanie osobných údajov v súlade so stanovenými dobami uchovávaní alebo ich anonymizáciu,
- ICT systém alebo technológia musí umožňovať aplikovateľnosť práv dotknutej osoby.

16. Prílohy

PRÍLOHA č.1: Minimimálne požiadavky na bezpečnostné opatrenia pre komponenty základných služieb



Príloha .1
Minimimálne požiadavky

Koniec dokumentu