

Naše zn. 65652/2026-SŽ-GŘ-025

Výzva k podání nabídky

Správa železnic, státní organizace, se sídlem Praha 1, Nové Město, Dlážďená 1003/7, PSČ 110 00, generální ředitelství, Vás při splnění podmínek uvedených v ustanovení § 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“),

vyzývá

k podání nabídky na realizaci veřejné zakázky s názvem

„Bezpečnostní testování“

Správa železnic, státní organizace, zadává tuto veřejnou zakázku jako podlimitní sektorovou veřejnou zakázku v souvislosti s výkonem relevantní činnosti dle § 151 odst. 1 ZZVZ a v souladu s § 158 odst. 1 ZZVZ nepostupuje při zadávání této veřejné zakázky podle uvedeného zákona. Řízení na zadání této veřejné zakázky se dále v textu označuje jako „výběrové řízení“.

Výše uvedená veřejná zakázka je dále v textu označována jen jako „veřejná zakázka“. Výzva k podání nabídky je v textu označována též jako „Výzva“.

Pro tuto zakázku jsou stanoveny následující podmínky:

1. Identifikační údaje zadavatele

Název: Správa železnic, státní organizace
Sídlo: Dlážďená 1003/7, Nové Město, 110 00 Praha 1
IČO: 709 94 234
DIČ: CZ70994234
Zapsán: v obchodním rejstříku vedeném Městským soudem v Praze, oddíl A, vložka 48384
Zastoupen: **Ing. Mojmiřem Nejezchlebem**, zástupcem generálního ředitele pověřeným správní radou řízením organizace a **Ing. Karlem Švejdou, MBA**, náměstkem generálního ředitele pro provozuschopnost dráhy

2. Informace o osobě, která zpracovala část Výzvy

1.1. Na zpracování Výzvy se nepodílela osoba odlišná od zadavatele.

3. Informace o předběžné tržní konzultaci:

3.1 Výzva neobsahuje informace, které by byly výsledkem předběžné tržní konzultace.

4. Komunikace mezi zadavatelem a dodavatelem

- 4.1 Veškerá komunikace mezi zadavatelem a dodavatelem ve výběrovém řízení musí být vedena pouze písemnou formou, a to elektronicky, s výjimkou případů vymezených v ustanovení § 211 odst. 5 ZZVZ. Jazyk pro komunikaci mezi zadavatelem a dodavatelem je výhradně český jazyk, není-li dále stanoveno jinak. Doručování písemností a komunikace mezi zadavatelem a dodavatelem ve výběrovém řízení bude ze strany zadavatele probíhat prostřednictvím elektronického nástroje E-ZAK (na adrese: <https://zakazky.spravazeleznic.cz/>), který splňuje podmínky vyhlášky č. 260/2016 Sb., o stanovení podrobnějších podmínek týkajících se elektronických nástrojů, elektronických úkonů při zadávání veřejných zakázek a certifikátu shody. Na komunikaci ze strany dodavatele učiněnou elektronicky, avšak nikoliv prostřednictvím elektronického nástroje E-ZAK, bude tedy zadavatel vždy odpovídat prostřednictvím elektronického nástroje.
- 4.2 Zpracování osobních údajů včetně jejich zvláštních kategorií případně poskytnutých v průběhu výběrového řízení je zadavatelem prováděno pouze za účelem zadání předmětné veřejné zakázky, přičemž zadavatel v celém procesu ochrany osobních údajů postupuje v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, obecně závaznými právními předpisy a vnitřními předpisy zadavatele, které agendu ochrany osobních údajů upravují. Podrobné informace týkající se zpracování osobních údajů, zadavatel uvedl na oficiálních webových stránkách <https://www.spravazeleznic.cz/o-nas/sdeleni-o-zpracovani-osobnich-udaju-pro-verejnost>.

5. Předmět veřejné zakázky

- 5.1 **Informace o předmětu veřejných zakázek** zadávaných na základě rámcové dohody:
- Předpokládaná hodnota: 6 000 000,- Kč bez DPH (maximální, nepřekročitelná)
- Druh veřejné zakázky: služby
- Charakteristika výběrového řízení: výběrové řízení odpovídající zadávání sektorové podlimitní zakázky dle § 131 odst. 2 Zákona zadávané dle interních předpisů zadavatele
- 5.2 Předmětem plnění je zajištění realizace bezpečnostních testů (zejm. testy zranitelností a penetrační testy). Jejich cílem je detekce zranitelností, které se vyskytují v používaných technologiích nebo vznikají nepatřičnými konfiguracemi nebo nevhodným návrhem aplikací / IS.
- 5.3 Předmětem výběrového řízení je uzavření rámcové dohody za účelem zajištění plnění dle čl. 5.2. této Výzvy. Rámcovou dohodu uzavře zadavatel s jedním dodavatelem či více dodavateli, jejichž nabídky se na základě provedeného hodnocení a posouzení podmínek účasti v tomto výběrovém řízení umístí jako 1. až 5. v pořadí. Umístí-li se na 5. místě více dodavatelů, bude rámcová dohoda uzavřena se všemi dodavateli, kteří se umístili na 5. místě. Závazný vzor rámcové dohody je přílohou č. 3 této Výzvy (dále jen „**závazný vzor RD**“). Předmět veřejných zakázek zadávaných na základě uzavřené rámcové dohody (dále jen „**dílčí zakázky**“) je specifikován v čl. 5.2. této Výzvy. Dílčí zakázky budou zadávány s obnovením soutěže.
- 5.4 Nebude-li zadavatel schopen vybrat počet dodavatelů, který uvedl podle předchozího odstavce tohoto článku Výzvy z důvodu, že nebude podán dostatečný počet nabídek nebo tyto nabídky nesplní požadavky stanovené touto Výzvou, je zadavatel oprávněn uzavřít rámcovou dohodu pouze s těmi účastníky výběrového řízení, kteří tyto požadavky splnili, tj. i s menším počtem dodavatelů, včetně i jen jediného dodavatele.
- 5.5 Bližší specifikace předmětu veřejné zakázky je přílohou č. 2 závazného vzoru RD.

6. Předpokládaná hodnota veřejných zakázek, které mohou být zadány na základě rámcové dohody uzavřené v tomto výběrovém řízení

- 6.1 Předpokládaná hodnota předmětu veřejné zakázky stanovená zadavatelem činí **6.000.000 Kč bez DPH** a je nepřekročitelná.

7. Doba a místo plnění veřejné zakázky

- 7.1 Doba účinnosti rámcové dohody: od nabytí účinnosti Rámcové dohody
- 7.2 Doba trvání rámcové dohody: 4 roky od nabytí účinnosti Rámcové dohody
- 7.3 Místo plnění: Správa železnic, Dlážďená 1003/7, Praha 1

8. Sociálně a environmentálně odpovědné zadávání, inovace

- 8.1 Zadavatel při vytváření zadávacích podmínek, včetně pravidel pro hodnocení nabídek, a výběru dodavatele, postupoval tak, aby v co nejvyšší možné míře naplnil zásady sociálně odpovědného zadávání, environmentálně odpovědného zadávání a inovací tak jak jsou definovány v § 28 odst. 1 písm. p) až r) ZZVZ (dále jen „**odpovědné zadávání**“). Vzhledem k tomu, že jednotlivé postupy odpovědného zadávání nebyly v ZZVZ ani v jiném zákoně taxativně vymezeny a současně je odpovědné zadávání stále se velmi dynamicky vyvíjejícím institutem veřejného zadávání, zadavatel při vytváření podmínek zvažoval použití zejména těch prvků odpovědného zadávání, které byly v době vytváření zadávacích podmínek jednoznačně vymezitelné a vymahatelné, a současně byla u nich vysoká míra jistoty, že zadavatel jejich aplikací neporuší ostatní zásady uvedené v § 6 ZZVZ a také principy 3E vyplývající ze zákona č. 320/2001 Sb. o finanční kontrole ve veřejné správě.

- 8.1.1. Zadavatel v rámci zásady sociálně odpovědného zadávání za účelem usnadnění přístupu k plnění veřejné zakázky, případně její části, malým a středním podnikům minimalizuje administrativní náročnost při podání nabídky možnostmi využití vzorových formulářů a čestných prohlášení, které jsou přílohami této Výzvy.

- 8.2 Použití jiných prvků odpovědného zadávání, které byly zadavateli známy při vytváření této zadávací dokumentace, není vzhledem k povaze a smyslu zakázky možné z těchto důvodů:

- 8.2.1. V oblasti environmentálního odpovědného zadávání zadavatel neshledal potřebu použití dílčích aspektů odpovědného zadávání v důsledku marginálních dopadů činností, které jsou předmětem této veřejné zakázky, na životní prostředí.

- 8.2.2. V oblasti inovací zadavatel nestanovil dílčí kritéria odpovědného zadávání s ohledem na skutečnost, že v rámci předmětu plnění veřejné zakázky neidentifikoval žádná možná inovativní řešení. Z těchto důvodů jsou inovace u daného předmětu plnění fakticky vyloučeny

- 8.2.3. V oblasti sociálně odpovědného zadávání zadavatel neshledal potřebu použití dalších dílčích aspektů odpovědného zadávání, s ohledem na specifickou službu, kdy předmětem služeb je specializované plnění. Vzhledem k těmto důvodům je nutné, aby se na plnění veřejné zakázky podílely osoby s vysokou kvalifikací. Nejedná se tedy o vhodnou příležitost k zaměstnání osob znevýhodněných na trhu práce.

9. Požadavky na prokázání splnění podmínek způsobilosti a kvalifikace dodavatele

Dodavatelé jsou povinni prokázat splnění základní a profesní způsobilosti a požadavků zadavatele obsažených v této Výzvě. V případě společné účasti dodavatelů prokazuje základní způsobilost dle čl. 9.1 této Výzvy a profesní způsobilost dle čl. 9.2.1 této Výzvy každý dodavatel samostatně. K prokázání základní a profesní způsobilosti postačí předložení dokladu ve formě prosté kopie. V případě cizojazyčných dokumentů zadavatel požaduje kopie předkládaných dokumentů s překladem do českého jazyka. Doklady ve

slovenském jazyce a doklad o vzdělání v latinském jazyce se předkládají bez překladu. Pokud se podle příslušného právního řádu požadovaný doklad nevydává, může být nahrazen čestným prohlášením. Povinnost předložit doklad může dodavatel splnit odkazem na odpovídající informace vedené v informačním systému veřejné správy nebo v obdobném systému vedeném v jiném členském státu, který umožňuje neomezený dálkový přístup. Takový odkaz musí obsahovat internetovou adresu a údaje pro přihlášení a vyhledání požadované informace, jsou-li takové údaje nezbytné.

Dodavatel prokáže splnění základní a profesní způsobilosti tak, že ke své nabídce přiloží níže uvedené doklady, jimiž doloží:

9.1 **Základní způsobilost** dodavatel v nabídce prokáže ve vztahu k České republice předložením čestného prohlášení zpracovaného v souladu s kapitolou 3 přílohy č. 1 této Výzvy:

9.1.1. Způsobilý není dodavatel, který

- a) byl v zemi svého sídla v posledních 5 letech před zahájením výběrového řízení pravomocně odsouzen pro trestný čin uvedený v příloze č. 3 ZZVZ nebo obdobný trestný čin podle právního řádu země sídla dodavatele; k zahlazeným odsouzením se nepřihlíží,
- b) má v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek,
- c) má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění,
- d) má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti,
- e) je v likvidaci, proti němuž bylo vydáno rozhodnutí o úpadku, vůči němuž byla nařízena nucená správa podle jiného právního předpisu nebo v obdobné situaci podle právního řádu země sídla dodavatele.

9.1.2. Je-li dodavatelem právnická osoba, musí podmínku podle čl. 9.1.1 písm. a) Výzvy splňovat tato právnická osoba a zároveň každý člen statutárního orgánu. Je-li členem statutárního orgánu dodavatele právnická osoba, musí podmínku podle čl. 9.1.1 písm. a) této Výzvy splňovat

- a) tato právnická osoba,
- b) každý člen statutárního orgánu této právnické osoby a
- c) osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele.

9.1.3. Účastní-li se výběrového řízení pobočka závodu

- a) zahraniční právnické osoby, musí podmínku podle čl. 9.1.1 písm. a) této Výzvy splňovat tato právnická osoba a vedoucí pobočky závodu,
- b) české právnické osoby, musí podmínku podle čl. 9.1.1 písm. a) této Výzvy splňovat osoby uvedené v čl. 9.1.2 této Výzvy a vedoucí pobočky závodu.

9.1.4. Účastník výběrového řízení může prokázat obnovení základní způsobilosti analogicky dle § 76 ZZVZ.

9.2 **Splnění profesní způsobilosti** prokáže dodavatel ve vztahu k České republice:

9.2.1. předložením výpisu z obchodního rejstříku nebo jiné obdobné evidence, pokud jiný právní předpis zápis do takové evidence vyžaduje.

9.2.2. Doklady podle čl. 9.2.1 této Výzvy dodavatel nemusí předložit, pokud právní předpisy v zemi jeho sídla obdobnou profesní způsobilost nevyžadují.

9.3 Stáří dokladů

- 9.3.1. Doklady prokazující základní způsobilost musí prokazovat splnění požadovaného kritéria způsobilosti **nejpozději v době 3 měsíců přede dnem zahájení výběrového řízení**. Den zahájení výběrového řízení je den odeslání této Výzvy prostřednictvím elektronického nástroje.

9.4 Ekonomická kvalifikace

Zadavatel nepožaduje.

9.5 Technická kvalifikace

- 9.5.1. Zadavatel požaduje, aby dodavatel ve své nabídce předložil seznam významných služeb poskytnutých dodavatelem za posledních 5 let před zahájením výběrového řízení, z něhož bude vyplývat, že v uvedeném období realizoval alespoň 5 významných služeb, jejichž předmětem bylo provádění bezpečnostních testů (tj. zejména testy zranitelnosti a penetrační testy), v minimálním finančním objemu 100.000 Kč bez DPH za jednu takovou službu, přičemž ze seznamu významných služeb musí vyplývat, že byly realizovány alespoň pro 3 různé subjekty. Splnění této části kvalifikace dodavatel prokáže formou čestného prohlášení zpracovaného v souladu s kapitolou č. 7 přílohy č. 1 této Výzvy.

Doba „za posledních 5 let před zahájením výběrového řízení“ se pro účely tohoto výběrového řízení považuje za splněnou, pokud významná zakázka byla v průběhu této doby dokončena alespoň v rozsahu odpovídajícím požadavkům zadavatele uvedeným výše (tj. řádné dokončení příslušné části významné zakázky, která naplňuje požadavky zadavatele na významné zakázky). Významná zakázka může být uznána výhradně tehdy, pokud subjekt dokládající poskytnutí příslušné referenční zakázky v jejím rámci dokončil činnosti relevantní z hlediska požadavků stanovených zadavatelem, přičemž tyto relevantní činnosti nebyly dokončeny dříve, než v posledních 5 letech před zahájením výběrového řízení veřejné zakázky. Doba „za posledních 5 let před zahájením výběrového řízení“ se považuje za splněnou i v případě, že se jedná o významné zakázky, které probíhaly i po zahájení výběrového řízení, nebo pokud stále probíhají, za předpokladu splnění výše uvedených parametrů do konce lhůty pro prokázání kvalifikace. Koncem lhůty pro prokázání kvalifikace se rozumí okamžik faktického ukončení posuzování kvalifikace zadavatelem. Z předložených údajů a dokladů vztahujících se k příslušné významné zakázce musí být zcela jednoznačně zřejmé, jaké činnosti, v jakém rozsahu a v jakém časovém období příslušný subjekt při plnění příslušné zakázky dokončil.

Pro vyloučení pochybností zadavatel uvádí, že za významnou službu se nepovažuje uzavřená rámcová dohoda, na základě které bylo v souhrnu několika dílčích smluv realizováno plnění v požadované hodnotě, nýbrž finanční objem významné zakázky musel být dosažen v rámci jedné dílčí smlouvy.

- 9.5.2. Zadavatel požaduje, aby dodavatel ve své nabídce předložil seznam osob, které se budou podílet na plnění předmětu veřejné zakázky, bez ohledu na to, zda se jedná o zaměstnance dodavatele nebo osoby v jiném vztahu k dodavateli (dále též „**realizační tým**“). Zadavatel požaduje, aby dodavatel prokázal splnění této části kvalifikace prostřednictvím níže uvedených osob s níže uvedenými požadavky. Splnění této části kvalifikace dodavatel prokáže formou čestného prohlášení zpracovaného v souladu s kapitolou č. 8 přílohy č. 1 této Výzvy, jehož přílohou budou životopisy jednotlivých členů realizačního týmu. Vzor životopisu je uveden jako příloha č. 4 této Výzvy.
- 9.5.3. Jedna osoba nemůže zastávat více níže uvedených pozic. Dodavatel musí mít k dispozici realizační tým složený nejméně z 2 osob s níže uvedenými požadavky:

Vedoucí týmu (pouze 1 osoba)

- účast na min. 3 projektech v oblasti provádění bezpečnostních testů (tj. zejména testy zranitelnosti a penetrační testy) a zároveň u minimálně 2 z těchto projektů zastával pozici vedoucího projektového týmu či obdobnou (jejímž obsahem bylo po

stránce realizační vést tým a nést odpovědnost nad prováděním bezpečnostního testování),

- praxe min. 8 let v oblasti zajišťování kybernetické bezpečnosti či vývoje a testování informačních systémů či aplikací z hlediska dodržování požadavků kybernetické bezpečnosti
- předložení alespoň jednoho certifikátu z oblasti bezpečnostních testů v oblasti IT (PECB Certified SCADA Security Manager / OSCP / CompTIA PenTest+ / obdobný či vyšší),

Penetrační tester (minimálně 1 osoba)

- účast na min. 2 projektech v oblasti provádění bezpečnostních testů (tj. zejména testy zranitelnosti a penetrační testy),
- praxe min. 5 let v oblasti zajišťování kybernetické bezpečnosti či vývoje a testování informačních systémů či aplikací z hlediska dodržování požadavků kybernetické bezpečnosti,
- předložení alespoň jednoho certifikátu z oblasti bezpečnostních testů v oblasti IT (CEH / CompTIA PenTest+/ obdobný či vyšší),

9.6 Jiný způsob prokázání základní a profesní způsobilosti

9.6.1. Předložením **Výpisu ze seznamu kvalifikovaných dodavatelů**, který je vydáván Ministerstvem pro místní rozvoj, prokáže dodavatel splnění základní způsobilosti dle čl. 9.1 této Výzvy a profesní způsobilosti dle čl. 9.2 této Výzvy v rozsahu, v jakém doklady pokrývají požadavky zadavatele pro plnění veřejné zakázky. V případě, že účastník bude prokazovat základní a profesní způsobilost prostřednictvím Výpisu ze seznamu kvalifikovaných dodavatelů, zadavatel uvádí, že je povinen přijmout výpis ze seznamu kvalifikovaných dodavatelů, pokud k poslednímu dni (viz čl. 15), ke kterému má být prokázána základní způsobilost nebo profesní způsobilost, není výpis ze seznamu kvalifikovaných dodavatelů starší než 3 měsíce. Zadavatel nemusí přijmout výpis ze seznamu kvalifikovaných dodavatelů, na kterém je vyznačeno zahájení řízení podle § 231 odst. 4 ZZVZ. Stejně jako výpisem ze seznamu kvalifikovaných dodavatelů může dodavatel prokázat kvalifikaci osvědčením, které pochází z jiného členského státu, v němž má dodavatel sídlo, a které je obdobou výpisu ze seznamu kvalifikovaných dodavatelů.

9.7 Prokázání kvalifikace prostřednictvím jiných osob

9.7.1. Dodavatel může ekonomickou kvalifikaci, technickou kvalifikaci nebo profesní způsobilost s výjimkou kritéria podle čl. 9.2 této Výzvy požadovanou zadavatelem prokázat prostřednictvím jiných osob. Dodavatel je v takovém případě povinen zadavateli předložit

- a) doklady prokazující splnění profesní způsobilosti podle čl. 9.2 této Výzvy jinou osobou,
- b) doklady prokazující splnění chybějící části kvalifikace prostřednictvím jiné osoby,
- c) doklad o splnění základní způsobilosti podle čl. 9.1 této Výzvy jinou osobou a
- d) smlouvu nebo jinou osobou podepsané potvrzení o její existenci, jejímž obsahem je závazek jiné osoby k poskytnutí plnění určeného k plnění veřejné zakázky nebo k poskytnutí věcí nebo práv, s nimiž bude dodavatel oprávněn disponovat v rámci plnění veřejné zakázky, a to alespoň v rozsahu, v jakém jiná osoba prokázala kvalifikaci za dodavatele.

9.7.2. Prokazuje-li dodavatel prostřednictvím jiné osoby kvalifikaci a předkládá doklady podle čl. 9.5 této Výzvy (v rozsahu požadavků na významné dodávky/služby nebo členy realizačního týmu) vztahující se k takové osobě, musí ze smlouvy nebo potvrzení o její existenci podle čl. 9.7.1 písm. d) této Výzvy vyplývat závazek, že jiná osoba bude vykonávat stavební práce či služby, ke kterým se prokazované kritérium kvalifikace vztahuje.

- 9.7.3. Má se za to, že požadavek podle čl. 9.7.1 písm. d) je splněn, pokud z obsahu smlouvy nebo potvrzení o její existenci podle čl. 9.7.1 písm. d) této Výzvy vyplývá závazek jiné osoby plnit veřejnou zakázku společně a nerozdílně s dodavatelem, to neplatí, pokud smlouva nebo potvrzení o její existenci podle 9.7.1 písm. d) této Výzvy musí splňovat požadavky dle čl. 9.7.2 této Výzvy.
- 9.7.4. Zadavatel požaduje, aby dodavatel a jiná osoba, jejímž prostřednictvím dodavatel prokazuje ekonomickou kvalifikaci podle čl. 9.4 této Výzvy, nesli společnou a nerozdílnou odpovědnost za plnění veřejné zakázky.
- 9.7.5. Na kvalifikaci osoby, jejímž prostřednictvím je prokazována kvalifikace, se vztahují pravidla stanovená touto Výzvou pro kvalifikaci dodavatele, za kterého je kvalifikace prokazována.
- 9.8 Dodavatel, který podal nabídku ve výběrovém řízení, nesmí být současně osobou, jejímž prostřednictvím jiný dodavatel v tomtéž výběrovém řízení prokazuje kvalifikaci.
- 9.9 Zadavatel si vyhrazuje právo postupovat analogicky k ustanovení § 48 odst. 5 ZZVZ.

10. Jiná kritéria kvalifikace stanovená analogicky k ustanovení § 167 odst. 1 ZZVZ

- 10.1 Dodavatel ke splnění kvalifikace v nabídce dále předloží:
- 10.1.1. kopii certifikátu ISO 20000, vydaného podle českých technických norem akreditovanou osobou, nebo předložením rovnocenného certifikátu vydaného podle českých technických norem akreditovanou osobou v členském státě Evropské unie, jehož prostřednictvím dodavatel prokáže, že má zaveden systém managementu kvality IT služeb.
- 10.1.2. kopii certifikátu ISO 27001, vydaného podle českých technických norem akreditovanou osobou, nebo předložením rovnocenného certifikátu vydaného podle českých technických norem akreditovanou osobou v členském státě Evropské unie, jehož prostřednictvím dodavatel prokáže, že má zaveden systém řízení bezpečnosti informací.

11. Požadavky zadavatele na zpracování nabídky

- 11.1 Účastník předloží úplnou elektronickou verzi nabídky, a to s využitím elektronického nástroje E-ZAK. Způsob správného podání nabídky v elektronické podobě na veřejnou zakázku je uveden v uživatelské příručce elektronického nástroje E-ZAK pro dodavatele, která je k dispozici na internetové stránce profilu zadavatele: <https://zakazky.spravazeleznic.cz/manual.html>
- 11.2 Pro tyto účely a v souladu se ZZVZ systém vyžaduje registraci dodavatelů a elektronický podpis založený na kvalifikovaném certifikátu. Podáním nabídky dodavatel se stanovenou formou komunikace a doručování souhlasí a zavazuje se poskytnout veškerou nezbytnou součinnost, zejména provést registraci v elektronickém nástroji E-ZAK a pravidelně kontrolovat doručené zprávy.
- 11.3 Dodavatel je oprávněn podat pouze jednu nabídku.
- 11.4 Nabídka musí obsahovat:
- identifikační údaje účastníka analogicky dle ustanovení § 28 odst. 1 písm. g) ZZVZ, kontaktní osobu účastníka pro účely této veřejné zakázky, včetně jejich kontaktních údajů (telefon, e-mail),
 - návrh rámcové dohody. Závazný vzor rámcové dohody je uveden jako příloha č. 3 této Výzvy, přičemž účastník není oprávněn vkládat do návrhu rámcové dohody a jeho obchodních podmínek jiné sankce a závazky vůči zadavateli než ty, které obsahuje příloha č. 3 této Výzvy závazný vzor rámcové dohody a jeho obchodní podmínky. Nebude-li nabídka obsahovat přílohy rámcové dohody, do kterých nebyl účastník oprávněn zasahovat, má se za to, že se zněním takových příloh souhlasí, ledaže sdělil opak.

- c) čestné prohlášení ve vztahu k zakázaným dohodám – účastník je povinen přiložit ke své nabídce čestné prohlášení o tom, že v souvislosti s výběrovým řízením na uzavření rámcové dohody a dílčími zakázkami na základě této rámcové dohody zadávanými neuzavřel a neuzavře s jinými osobami zakázanou dohodu ve smyslu zákona č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže), ve znění pozdějších předpisů. Toto bude předloženo ve formě formuláře obsaženého v kapitole č. 5 přílohy č. 1 této Výzvy.
- 11.5 Analogicky dle ustanovení § 28 odst. 2 ZZVZ platí, že nebyla-li nabídka Zadavateli doručena ve lhůtě nebo způsobem stanoveným v této Výzvě, k takové nabídce se nepřihlíží.
- 11.6 Zadavatel doporučuje a preferuje, aby nabídka byla podána za využití krycího listu uvedeného v příloze č. 1 této Výzvy.

12. Registr smluv

- 12.1 Zadavatel je povinen uveřejňovat uzavřené smlouvy v registru smluv na základě ustanovení zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (dále jen „**ZRS**“).
- 12.2 Zadavatel na základě výše uvedeného požaduje, aby účastník pro účely uveřejnění rámcové dohody v registru smluv v rámcové dohodě, která bude nedílnou součástí nabídky, označil její části, které jsou předmětem obchodního tajemství nebo ty části, ve kterých jsou obsaženy informace, které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS.
- 12.3 Pokud účastník v rámcové dohodě, která bude nedílnou součástí nabídky, označí její části nebo určité informace dle čl. 12.2 této Výzvy, je účastník povinen o tomto předložit čestné prohlášení. Vzor tohoto prohlášení je zpracován jako příloha č. 2 této Výzvy. Tímto čestným prohlášením účastník prohlašuje, že jím uvedené údaje a skutečnosti kumulativně naplňují všechny definiční znaky obchodního tajemství tak, jak je vymezeno v ustanovení § 504 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**obchodní tajemství**“) a pro případ, že by takto označené údaje a skutečnosti nenaplňovaly znaky obchodního tajemství a takto znečitelněná rámcová dohoda by byla v důsledku toho uveřejněna způsobem odporujícím ZRS, nese účastník veškerou odpovědnost.
- 12.4 Výše uvedené čestné prohlášení dle čl. 12.3 této Výzvy účastník nedokládá v případě, že neoznačí v rámcové dohodě, která bude nedílnou součástí nabídky, žádné takové části nebo informace ve smyslu čl. 12.2 této Výzvy.
- 12.5 Účastník odpovídá za správnost a pravdivost veškerých údajů a skutečností, které jím budou uvedeny ve výše uvedeném čestném prohlášení. Zadavatel nebude přezkoumávat jejich pravdivost.
- 12.6 Výjimkou z povinnosti uveřejnění rámcové dohody v registru smluv jsou důvody uvedené v ustanovení § 3 odst. 2 ZRS. Je-li účastník subjektem uvedeným v ustanovení § 3 odst. 2 písm. k) ZRS (případně je subjektem uvedeným v ustanovení § 3 odst. 2 ZRS dle jiného písmene, než je zde uvedeno), doporučuje zadavatel, aby účastník tuto skutečnost uvedl v nabídce. V případě, že tak účastník neučiní, bude zadavatel postupovat, jako by na rámcovou dohodu nedopadala výjimka uvedená v ustanovení § 3 odst. 2 písm. k) ZRS (případně jiná výjimka dle ustanovení § 3 odst. 2 ZRS dle jiného písmene, než je zde uvedeno) a zadavatel neodpovídá za škodu nebo jakoukoliv jinou újmu tímto postupem vzniklou.

13. Poddodavatel

- 13.1 Zadavatel požaduje, aby účastník výběrového řízení v nabídce:

- a) určil části veřejné zakázky, které hodlá plnit prostřednictvím poddodavatelů, a
- b) předložil seznam poddodavatelů, včetně jejich identifikačních údajů, pokud jsou účastníkovi výběrového řízení známi a uvedl, kterou část veřejné zakázky bude každý z poddodavatelů plnit.

14. Požadavky na způsob zpracování nabídkové ceny

- 14.1 Zadavatel požaduje, aby účastník uvedl cenu za 1 MD plnění předmětu této veřejné zakázky, v české měně (Koruna česká).
- 14.2 Za účelem uvedení ceny v Kč bez DPH za 1 MD bude účastníkem vyplněna příloha č. 3 závazného vzoru RD.
- 14.3 Cena za 1 MD musí být v nabídce účastníkem garantována jako cena maximální a nepřekročitelná, konečná, zahrnující veškeré náklady účastníka spojené s plněním předmětu této veřejné zakázky a v rámci jednotlivých dílčích objednávek tuto cenu nebude dodavatelem možné překročit.
- 14.4 Cena za 1 MD, uvedená účastníkem v rámci jeho nabídky, nesmí být v rámci minitenderu na zadání dílčí veřejné zakázky účastníkem překročena.

15. Lhůta a místo pro podání nabídky

- 15.1 Nabídka musí být podána elektronickými prostředky prostřednictvím elektronického nástroje E-ZAK, který je profilem zadavatele, a to v českém jazyce nebo analogicky k ustanovení § 45 odst. 3 ZZVZ. **Zadavatel nepřipouští podání nabídky v listinné podobě ani v jiné elektronické formě mimo elektronický nástroj E-ZAK.**
- 15.2 Dokumenty musí být do systému E-ZAK vkládány jako jeden soubor nebo více zkomprimovaných souborů ve formátu zip, rar nebo 7z, bez použití hesla. Zkomprimované soubory nesmí obsahovat žádný další zkomprimovaný soubor.
- 15.3 Zadavatel upozorňuje, že systém elektronického zadávání veřejných zakázek E-ZAK umožňuje pracovat se soubory o velikosti nejvýše 50 MB za jeden takový soubor, příp. zkomprimované soubory. Soubory většího rozsahu je nutno před jejich odesláním prostřednictvím E-ZAK vhodným způsobem rozdělit. Velikost samotné nabídky jako celku není nijak omezena.
- 15.4 Nabídky podávané v elektronické podobě dodavatel doručí do konce stanovené lhůty pro podání nabídek, a to prostřednictvím elektronického nástroje E-ZAK na adrese <https://zakazky.spravazeleznic.cz/>
- 15.5 Lhůta pro podání nabídek je uvedena v elektronickém nástroji E-ZAK.
- 15.6 Nabídky podané po uplynutí lhůty pro podání nabídky nebudou otevřeny. Zadavatel bezodkladně vyrozumí účastníka o tom, že jeho nabídka byla podána po uplynutí lhůty pro podání nabídky.

16. Vysvětlení Výzvy

- 16.1 Zadavatel může Výzvu vysvětlit, pokud takové vysvětlení, případně související dokumenty, uveřejní stejným způsobem, jako uveřejnil tuto Výzvu, anebo pokud je zašle všem dodavatelům, kterým zaslal Výzvu nebo kteří si ji vyzvedli, v případě, že Výzva nebyla uveřejněna.
- 16.2 Dodavatel je oprávněn po zadavateli požadovat vysvětlení Výzvy. Žádost o vysvětlení Výzvy doručí dodavatel ve stanovené lhůtě písemnou formou, a to elektronicky. Zadavatel bude na žádosti o vysvětlení Výzvy odpovídat prostřednictvím elektronického nástroje E-ZAK na adrese: <https://zakazky.spravazeleznic.cz/>. Pokud o vysvětlení Výzvy písemně požádá dodavatel, zadavatel vysvětlení uveřejní, odešle nebo předá včetně přesného znění žádosti bez identifikace tohoto dodavatele. Zadavatel není povinen

vysvětlení poskytnout, pokud není žádost o vysvětlení doručena včas, a to alespoň 3 pracovní dny před uplynutím lhůty pro podání nabídek dle bodu 15.5 této Výzvy. Zadavatel se může rozhodnout vysvětlení poskytnout i na opožděnou žádost o vysvětlení.

- 16.3 Pokud je žádost o vysvětlení Výzvy doručena včas a zadavatel neuveřejní, neodešle nebo nepředá vysvětlení do 3 pracovních dnů, prodlouží lhůtu pro podání nabídek nejméně o tolik pracovních dnů, o kolik přesáhla doba od doručení žádosti o vysvětlení Výzvy do uveřejnění, odeslání nebo předání vysvětlení 3 pracovní dny.
- 16.4 Pokud by spolu s vysvětlením Výzvy zadavatel provedl i změnu zadávacích podmínek, postupuje podle následujícího článku této Výzvy.

17. Změna Výzvy

- 17.1 Zadávací podmínky obsažené ve Výzvě může zadavatel změnit nebo doplnit před uplynutím lhůty pro podání nabídek. Změna nebo doplnění Výzvy musí být uveřejněna nebo oznámena dodavatelům stejným způsobem jako zadávací podmínka, která byla změněna nebo doplněna.
- 17.2 Pokud to povaha doplnění nebo změny Výzvy vyžaduje, zadavatel současně přiměřeně prodlouží lhůtu pro podání nabídek. V případě takové změny nebo doplnění Výzvy, která může rozšířit okruh možných účastníků výběrového řízení, prodlouží zadavatel lhůtu tak, aby od odeslání změny nebo doplnění Výzvy činila nejméně celou svou původní délku.

18. Kritérium hodnocení nabídek

- 18.1 Hodnotícím kritériem pro výběr nejvýhodnější nabídky v rámci ekonomické výhodnosti nabídek je nejnižší nabídková cena za 1 MD (zaokrouhlená maximálně na 2 desetinná místa).
- 18.2 Zadavatel vybere k uzavření rámcové dohody 5 účastníků, jejichž nabídka splňuje veškeré požadavky stanovené touto Výzvou a kteří se po provedeném hodnocení umístili na 1. až 5. místě. V případě, že se na 5. místě umístí více nabídek se shodným celkovým parametrem hodnotícího kritéria, bude rámcová dohoda uzavřena se všemi účastníky, kteří mají shodný počet bodů jako účastník, který se umístil 5. v pořadí.
- 18.3 Pokud je ve výběrovém řízení jediný účastník, může být zadavatelem vybrán bez provedení hodnocení.

19. Střet zájmů dle zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů

- 19.1 Dle § 4b zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (dále jen „**Zákon o střetu zájmů**“), se nesmí účastnit zadávacích řízení dle ZZVZ jako účastník zadávacího řízení nebo jako poddodavatel, prostřednictvím kterého účastník zadávacího řízení prokazuje kvalifikaci, obchodní společnost, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) Zákona o střetu zájmů nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti.
- 19.2 Zadavatel požaduje, aby dodavatel a jeho poddodavatel, prostřednictvím kterého prokazuje kvalifikaci, nebyli ve střetu zájmů dle § 4b Zákona o střetu zájmů. Skutečnost, že dodavatel a jeho poddodavatel, prostřednictvím kterého prokazuje část kvalifikace, nejsou ve střetu zájmů dle § 4b Zákona o střetu zájmů, prokáže dodavatel předložením čestného prohlášení, jehož vzorové znění je uvedeno v kapitole č. 4 přílohy č. 1 této Výzvy, ve své nabídce.
- 19.3 Vybraný dodavatel je povinen předložit k výzvě zadavatele analogicky dle § 122 odst. 3 písm. b) ZZVZ doklady a informace, z nichž nepochybně vyplývá, že vybraný dodavatel i všichni poddodavatelé, jimiž vybraný dodavatel prokazuje kvalifikaci, splňují podmínku neexistence střetu zájmů ve smyslu § 4b Zákona o střetu zájmů a tohoto článku. V případě vybraného dodavatele nebo jeho poddodavatele, prostřednictvím kterého

vybraný dodavatel prokazoval část kvalifikace, je-li zahraniční právnickou osobou, je vybraný dodavatel povinen předložit zejména doklady analogicky ve smyslu § 122 odst. 6 ZZVZ, a to i ve vztahu k příslušnému poddodavateli, prostřednictvím kterého vybraný dodavatel prokazoval část kvalifikace.

- 19.4 V případě postupu účastníka v rozporu s čl. 19 Výzvy bude účastník vyloučen z výběrového řízení.

20. Další zadávací podmínky v návaznosti na mezinárodní sankce, zákaz zadání veřejné zakázky

- 20.1 Zadavatel v tomto řízení postupuje analogicky v souladu s § 48a ZZVZ.

- 20.2 Zadavatel nezadá veřejnou zakázku účastníku výběrového řízení, pokud je to v rozporu s mezinárodními sankcemi podle zákona upravujícího provádění mezinárodních sankcí.

- 20.3 Pokud se mezinárodní sankce podle čl. 20.2 této Výzvy vztahuje na:

- a) účastníka výběrového řízení, může ho zadavatel vyloučit z účasti ve výběrovém řízení, nebo
- b) vybraného dodavatele, vyloučí ho zadavatel z účasti ve výběrovém řízení.

- 20.4 Pokud se mezinárodní sankce podle čl. 20.2 této Výzvy vztahuje na poddodavatele

- a) účastníka výběrového řízení, může zadavatel požadovat nahrazení poddodavatele, nebo
- b) vybraného dodavatele, musí zadavatel požadovat nahrazení poddodavatele.

- 20.5 Na základě požadavku zadavatele podle čl. 20.4 této Výzvy musí účastník výběrového řízení poddodavatele nahradit nejpozději do konce zadavatelem stanovené přiměřené lhůty. Pokud nedojde k nahrazení poddodavatele, platí, že se na účastníka výběrového vztahuje zákaz zadání veřejné zakázky.

- 20.6 Dle článku 5k nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění pozdějších předpisů¹ (dále jen „**Nařízení č. 833/2014**“) se zakazuje se zadat jakoukoli veřejnou zakázku nebo koncesní smlouvu spadající do oblasti působnosti směrnic o zadávání veřejných zakázek, jakož i čl. 10 odst. 1, 3, odst. 6 písm. a) až e), odst. 8, 9 a 10, článků 11, 12, 13 a 14 směrnice 2014/23/EU, čl. 7 písm. a) až d), článku 8 a čl. 10 písm. b) až f) a h) až j) směrnice 2014/24/EU, článku 18, čl. 21 písm. b) až e) a g) až i) a článků 29 a 30 směrnice 2014/25/EU a čl. 13 písm. a) až d), f) až h) a j) směrnice 2009/81/ES a hlavy VII nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046 následujícím osobám, subjektům nebo orgánům, nebo pokračovat v jejich plnění s následujícími osobami, subjekty a orgány:

- a) jakýkoli ruský státní příslušník, fyzická osoba s bydlištěm v Rusku nebo právnická osoba, subjekt či orgán usazené v Rusku;
- b) právnická osoba, subjekt nebo orgán, které jsou z více než 50 % přímo či nepřímo vlastněny některým ze subjektů uvedených v čl. 20.6 písm. a) této Výzvy, nebo
- c) fyzická nebo právnická osoba, subjekt nebo orgán, které jednájí jménem nebo na pokyn některého ze subjektů uvedených v čl. 20.6 písm. a) nebo b) této Výzvy,

¹ Zejm. Nařízení Rady (EU) 2022/576 ze dne 8. dubna 2022, kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině

včetně subdodavatelů, dodavatelů nebo subjektů, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, pokud představují více než 10 % hodnoty zakázky.

- 20.7 Zadavatel požaduje, aby účastník sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti ve výběrovém řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, **nebyli** osobami dle čl. 20.6 této Výzvy a Nařízení č. 833/2014.
- 20.8 Dle čl. 2 nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění pozdějších předpisů (dále jen „**Nařízení č. 269/2014**“), a dalších prováděcích předpisů k tomuto Nařízení č. 269/2014², nesmějí být žádné finanční prostředky ani hospodářské zdroje přímo ani nepřímo zpřístupněny fyzickým nebo právnickým osobám, subjektům či orgánům nebo fyzickým nebo právnickým osobám, subjektům či orgánům s nimi spojeným uvedeným v příloze I Nařízení nebo v jejich prospěch; dle čl. 2 nařízení Rady (ES) č. 765/2006 ze dne 18. května 2006 o omezujících opatřeních vzhledem k situaci v Bělorusku a k zapojení Běloruska do ruské agrese proti Ukrajině, ve znění pozdějších předpisů, nesmějí být fyzickým nebo právnickým osobám nebo subjektům uvedeným v příloze I tohoto nařízení nebo v jejich prospěch přímo ani nepřímo zpřístupněny žádné finanční prostředky ani hospodářské zdroje; dle čl. 2 nařízení Rady (EU) č. 208/2014 ze dne 5. března 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině nesmějí být žádné finanční prostředky ani hospodářské zdroje přímo ani nepřímo zpřístupněny fyzickým nebo právnickým osobám, subjektům či orgánům uvedeným v příloze I tohoto nařízení nebo v jejich prospěch (dále společně jen „**Osoby vedené na sankčních seznamech**“).
- 20.9 Zadavatel dále požaduje, aby účastník sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti ve výběrovém řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, **nebyli** Osobami vedenými na sankčních seznamech.
- 20.10 Splnění zadávacích podmínek stanovených zadavatelem dle tohoto článku prokáže účastník předložením čestného prohlášení, jehož vzorové znění je uvedeno v kapitole č. 6 přílohy č. 1 této Výzvy, ve své nabídce.
- 20.11 Zadavatel je oprávněn ověřovat si splnění zadávacích podmínek dle tohoto článku. Vybraný dodavatel je povinen předložit k výzvě zadavatele analogicky dle § 122 odst. 3 písm. b) ZZVZ doklady a informace, z nichž nepochybně vyplývá, že vybraný dodavatel i všichni poddodavatelé nebo jiné osoby, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, splňují podmínky uvedené v tomto článku Výzvy.
- 20.12 V případě postupu účastníka v rozporu s čl. 20.6 až 20.11 Výzvy bude účastník vyloučen z výběrového řízení.

21. Další požadavky zadavatele

- 21.1 Zadavatel si vyhrazuje právo výběrové řízení až do okamžiku uzavření rámcové dohody kdykoliv zrušit bez uvedení důvodu.
- 21.2 Zadavatel si vyhrazuje právo změnit, upřesnit či doplnit tuto Výzvu k podání nabídky až do skončení lhůty pro podání nabídky.

² Zejm. Prováděcí nařízení Rady (EU) 2022/581 ze dne 8. dubna 2022, kterým se provádí nařízení (EU) č. 269/2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny a prováděcí nařízení Rady (EU) 2022/658 ze dne 21. dubna 2022, kterým se provádí nařízení (EU) č. 269/2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny.

- 21.3 Zadavatel si vyhrazuje právo v průběhu výběrového řízení postupovat analogicky dle § 46 a § 113 ZZVZ.
- 21.4 Zadavatel si vyhrazuje právo vyloučit účastníka řízení analogicky dle ustanovení § 48 ZZVZ.
- 21.5 Další podmínky zadavatele pro uzavření smlouvy analogicky dle § 104 ZZVZ:
- 21.5.1. Vybraný dodavatel je povinen zadavateli na písemnou výzvu učiněnou analogicky dle § 122 odst. 3 písm. b) ZZVZ předložit doklady a informace dle čl. 19.3 a čl. 20.11 Výzvy.
- 21.5.2. Neposkytnutí součinnosti vybraným dodavatelem dle tohoto článku je důvodem pro vyloučení vybraného dodavatele.
- 21.6 Zadavatel a vybraný dodavatel jsou povinni bez zbytečného odkladu po oznámení rozhodnutí o výběru uzavřít rámcovou dohodu. Vybraného dodavatele, který nesplnil povinnost dle tohoto článku, může zadavatel z výběrového řízení vyloučit. Zadavatel si vyhrazuje právo postupovat analogicky dle § 125 odst. 1 a 2 věta první ZZVZ.
- 21.7 Zadavatel nepřipouští varianty nabídek.
- 21.8 Zadavatel upozorňuje, že preferuje uzavírání smluv v elektronické podobě prostřednictvím kvalifikovaných elektronických podpisů. V případě, že dodavatel není schopen k takovému postupu zajistit zadavateli součinnost, sdělí tuto skutečnost ve své nabídce, a to prostřednictvím krycího listu, který je č. 1 této Výzvy.

Přílohy tvořící nedílnou součást této Výzvy

- č. 1. Krycí list
- č. 2. Čestné prohlášení ve vztahu k zákonu o registru smluv
- č. 3. Závazný vzor rámcové dohody
- č. 4. Vzor životopisu člena realizačního týmu

.....
Ing. Mojmír Nejezchleb
zástupce generálního ředitele pověřený
správní radou řízením organizace

.....
Ing. Karel Švejda, MBA
náměstek generálního ředitele
pro provozuschopnost dráhy

Příloha č. 1 Výzvy k podání nabídky

Krycí list nabídky k veřejné zakázce s názvem „Bezpečnostní testování“ vedené pod č.j. 65652/2026-SŽ-GŘ-O25

Obsah

Kapitola 1. Základní údaje k nabídce	2
Kapitola 2. Ceník	3
Kapitola 3. Čestné prohlášení o splnění základní způsobilosti	4
Kapitola 4. Čestné prohlášení účastníka o střetu zájmů.....	5
Kapitola 5. Čestné prohlášení účastníka k neuzavření zakázaných dohod	6
Kapitola 6. Čestné prohlášení účastníka o splnění podmínek v souvislosti s mezinárodními sankcemi	7
Kapitola 7. Čestné prohlášení o splnění technické kvalifikace	8
Kapitola 8. Seznam osob.....	9

Kapitola 1. Základní údaje k nabídce

Zadavatel: Správa železnic, státní organizace
Praha 1 - Nové Město, Dlážděná 1003/7, PSČ 110 00
IČO 70994234, DIČ CZ70994234

Účastník: jméno osoby/název firmy
Sídlo:
IČO, DIČ

Zastoupená údaje o statutárním orgánu nebo jiné oprávněné osobě
Kontaktní osoba ve věci podání nabídky: xxxxxxxxxxxxxxxxxxxx
Email kontaktní osoby: xxxxxxxxxxxxxxxx

Účastník prohlašuje, že veškeré údaje uvedené v tomto krycím listu, který je přílohou č. 1 Výzvy k podání nabídky na veřejnou zakázku zadávanou jako podlimitní sektorovou veřejnou zakázku, jsou pravdivé, úplné a odpovídají skutečnosti. Účastník si je vědom důsledků záměrného uvedení nepravdivých údajů, které v rovině tohoto výběrového řízení mohou vést až k vyloučení Účastníka z výběrového řízení.

ÚDAJE O MOŽNOSTI ELEKTRONICKÉHO UZAVŘENÍ SMLOUVY:

Účastník disponuje platným zaručeným elektronickým podpisem ve smyslu zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce¹?

Zvolte položku:

(pokud na výše uvedenou otázku odpověděl dodavatel kladně)

Účastník je ochoten použít platný zaručený elektronický podpis pro uzavření smlouvy se zadavatelem v elektronické formě?

Zvolte položku:

¹ Takový certifikát v českém prostředí vydávají následující poskytovatelé: a) Česká pošta, s. p., b) eIdentity a.s., c) První certifikační autorita, a.s.

² Účastník vybere jednu z možností.

³ Účastník vybere jednu z možností.

Kapitola 2. Ceník

Za účelem stanovení celkové nabídkové ceny bude účastníkem vyplněna příloha č. 3 Rámcové dohody, která je přílohou č. 3 Výzvy k podání nabídky.

Kapitola 3. Čestné prohlášení o splnění základní způsobilosti

Účastník, který podává tuto nabídku, tímto čestně prohlašuje, že není účastníkem, který:

- a) byl v zemi svého sídla v posledních 5 letech před zahájením výběrového řízení pravomocně odsouzen pro trestný čin uvedený v [příloze č. 3](#) k zákonu č. 134/2016 Sb., o zadávání veřejných zakázek, nebo obdobný trestný čin podle právního řádu země sídla účastníka; k zahlazeným odsouzením se nepřihlíží,
- b) má v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek,
- c) má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění,
- d) má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti,
- e) je v likvidaci, proti němuž bylo vydáno rozhodnutí o úpadku, vůči němuž byla nařízena nucená správa podle jiného právního předpisu nebo v obdobné situaci podle právního řádu země sídla účastníka.

Výše uvedené podmínky splňuje jak Účastník (coby právnická osoba), tak každý člen jeho statutárního orgánu.

Kapitola 4. Čestné prohlášení účastníka o střetu zájmů

Účastník, který podává tuto nabídku, tímto čestně prohlašuje, že:

- a) **není** obchodní společností, ve které veřejný funkcionář uvedený v ust. § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (dále jen „**Zákon o střetu zájmů**“) nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti, a
- b) žádní poddodavatelé, jimiž prokazuje kvalifikaci ve výběrovém řízení, **nejsou** obchodní společností, ve které veřejný funkcionář uvedený v ust. § 2 odst. 1 písm. c) Zákona o střetu zájmů nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti.

Účastník dále čestně prohlašuje, že dostane-li se Účastník nebo poddodavatel, jímž prokazoval kvalifikaci ve výběrovém řízení, do střetu zájmů dle § 4b Zákona o střetu zájmů, a to kdykoliv až do okamžiku ukončení výběrového řízení, oznámí tuto skutečnost bez zbytečného odkladu zadavateli veřejné zakázky.

Účastník si je vědom všech právních důsledků, které pro něj mohou vyplývat z nepravdivosti zde uvedených údajů a skutečností.

Kapitola 5. Čestné prohlášení účastníka k neuzavření zakázaných dohod

Účastník, který podává tuto nabídku, tímto čestně prohlašuje, že:

- a) v souvislosti se zadávanou veřejnou zakázkou neuzavřel a neuzavře s jinými osobami zakázanou dohodu ve smyslu zákona č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže), ve znění pozdějších předpisů; a
- b) nepřipravoval části nabídek, které mají být hodnoceny podle kritérií hodnocení, ve vzájemné shodě s jiným účastníkem téhož výběrového řízení, s nímž je spojenou osobou podle zákona o daních z příjmů.

Účastník si je vědom všech právních důsledků, které pro něj mohou vyplývat z nepravdivosti zde uvedených údajů a skutečností.

Kapitola 6. Čestné prohlášení účastníka o splnění podmínek v souvislosti s mezinárodními sankcemi

Účastník, který podává tuto nabídku, tímto čestně prohlašuje, že:

- a) on sám jakožto dodavatel, ani jeho poddodavatelé, nejsou osobami, na něž se vztahuje zákaz zadání veřejné zakázky analogicky ve smyslu § 48a ZZVZ, tj. zejména, že
 - i. on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti ve výběrovém řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu evropských směrnic o zadávání veřejných zakázek, **nejsou** osobami dle článku 5k nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizující situaci na Ukrajině, ve znění pozdějších předpisů
 - ii. on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti ve výběrovém řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu evropských směrnic o zadávání veřejných zakázek, **nejsou** osobami dle článku 2 nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění pozdějších předpisů, a dalších prováděcích předpisů k tomuto nařízení Rady (EU) č. 269/2014, anebo osobami dle čl. 2 nařízení Rady (ES) č. 765/2006 ze dne 18. května 2006 o omezujících opatřeních vzhledem k situaci v Bělorusku a k zapojení Běloruska do ruské agrese proti Ukrajině, ve znění pozdějších předpisů anebo osobami dle čl. 2 nařízení Rady (EU) č. 208/2014 ze dne 5. března 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině, ve znění pozdějších předpisů (tzv. „**sankční seznamy**“)⁴.
- b) přestane-li on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti ve výběrovém řízení, nebo některý z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu evropských směrnic o zadávání veřejných zakázek, splňovat výše uvedené podmínky, k nimž se toto čestné prohlášení vztahuje, a to kdykoliv až do okamžiku ukončení výběrového řízení, oznámí tuto skutečnost bez zbytečného odkladu, nejpozději však **do 3 pracovních dnů** ode dne, kdy přestal splňovat výše uvedené podmínky, k nimž se toto čestné prohlášení vztahuje, zadavateli veřejné zakázky.

Účastník si je vědom všech právních důsledků, které pro něj mohou vyplývat z nepravdivosti zde uvedených údajů a skutečností.

⁴ Zejm, Prováděcí nařízení Rady (EU) 2022/581 ze dne 8. dubna 2022, kterým se provádí nařízení (EU) č. 269/2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny a prováděcí nařízení Rady (EU) 2022/658 ze dne 21. dubna 2022, kterým se provádí nařízení (EU) č. 269/2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny.

Kapitola 7. Čestné prohlášení o splnění technické kvalifikace

Účastník, který podává tuto nabídku, tímto čestně prohlašuje, že za posledních 5 let před zahájením výběrového řízení realizoval alespoň 5 významných služeb definovaných v čl. 9.5.1. Výzvy k podání nabídky v hodnotě alespoň 100.000 Kč bez DPH za každou významnou službu.

Objednatel služby IČO, sídlo, místo podnikání, kontakt k ověření realizované služby (jméno + e-mail)	Předmět plnění významné služby	Celkový finanční objem služby	Doba realizace (datum od-do, v rámci 5 kalendářních let nazpět před zahájením výběrového řízení)

Kapitola 8. Seznam osob

Účastník, který podává tuto nabídku, prohlašuje, že v případě, že se stane vybraným dodavatelem, bude plnit veřejnou zakázku v požadovaném rozsahu následujícím realizačním týmem, ledaže dojde k jeho změně v souladu se zadávacími podmínkami či uzavřenou smlouvou.

Funkce	Jméno a příjmení
Vedoucí týmu	
Penetrační tester	

Pozn. V případě, že dodavatel uvede více členů realizačního týmu, upraví dodavatel tabulku dle potřeby.

Přílohy:

Životopis Vedoucí týmu

Životopis Penetrační tester

V dne

Jméno a Příjmení

funkce osoby

—

—

Příloha č. 2 Výzvy k podání nabídky – **Účastník předloží pouze v případě postupu dle čl. 12.2. a 12.3 Výzvy.**

Čestné prohlášení

v souvislosti s ustanovením 3 odst. 1 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů, (dále jen „ZRS“)

Účastník:

Obchodní firma/jméno
Sídlo/místo podnikání
IČO
Zastoupen
.....

který podává nabídku na podlimitní sektorovou veřejnou zakázku s názvem „**Bezpečnostní testování**“, tímto čestně prohlašuje, že dále uvedené údaje a další skutečnosti uvedené či jinak řádně označené ve smlouvě na plnění předmětu veřejné zakázky/rámcové dohodě, jež je součástí jeho nabídky (dále jen „**smlouva**“), považuje účastník za obchodní tajemství ve smyslu ustanovení § 504 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**obchodní tajemství**“ a „**občanský zákoník**“), nebo se jedná o jiné informace, které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS:

Obchodní tajemství či jiné informace dle § 3 odst, 1 ZRS	Umístění ve smlouvě či jejích přílohách
Zvolte položku.	Klikněte sem a zadejte text.
	Klikněte sem a zadejte text.
	Klikněte sem a zadejte text.

Účastník tímto čestně prohlašuje, že údaje a skutečnosti uvedené ve smlouvě, která je nedílnou součástí nabídky, označené jako obchodní tajemství, naplňují současně všechny definiční znaky obchodního tajemství, tak jak je vymezeno v ustanovení § 504 občanského zákoníku, tj. obchodní tajemství tvoří konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení. Účastník dále čestně prohlašuje, že nese veškerou odpovědnost v případě, že část obsahu smlouvy, která se týká obchodního tajemství účastníka a která v důsledku toho bude pro účely uveřejnění smlouvy v registru smluv znečitelněna, pokud by smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, zda byla smlouva uveřejněna prostřednictvím registru smluv ze strany zadavatele nebo účastníka.

Účastník tímto čestně prohlašuje, že neprodleně písemně sdělí zadavateli skutečnost, že takto označené informace přestaly naplňovat znaky obchodního tajemství.

Účastník tímto čestně prohlašuje, že údaje a skutečnosti uvedené ve smlouvě, která je nedílnou součástí nabídky, jsou údaji nebo skutečnostmi (s výjimkou obchodního tajemství, uvedeného

výše), které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS. Účastník dále čestně prohlašuje, že nese veškerou odpovědnost v případě, že část obsahu smlouvy, která obsahuje informace označené účastníkem jako informace ve smyslu § 3 odst. 1 ZRS a která v důsledku toho bude pro účely uveřejnění smlouvy v registru smluv znečitelněna, pokud by smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, zda byla smlouva uveřejněna prostřednictvím registru smluv ze strany zadavatele nebo účastníka.

V dne

Příloha č. 3 Výzvy

Rámcová dohoda na „Bezpečnostní testování“

č. Objednatel: [DOPLNÍ OBJEDNATEL PŘI PODPISU RÁMCOVÉ DOHODY]

č. Zhotovitele č. 1: [DOPLNÍ ZHOTOVITEL]

č. Zhotovitele č. 2: [DOPLNÍ ZHOTOVITEL]

č. Zhotovitele č. 3: [DOPLNÍ ZHOTOVITEL]

uzavřená analogicky k ustanovení § 131 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**zákon**“), dle ustanovení § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**“)

(dále jen „**Rámcová dohoda**“ nebo „**RD**“)

mezi:

Název: Správa železnic, státní organizace

Sídlo: Dlážděná 1003/7, Nové Město, 110 00 Praha 1

IČO: 709 94 234

DIČ: CZ70994234

Zapsán: v obchodním rejstříku vedeném Městským soudem v Praze, oddíl A, vložka 48384

Zastoupen: **Ing. Mojmírem Nejezchlebem**, zástupcem generálního ředitele pověřeným správní radou řízením organizace a **Ing. Karlem Švejdu, MBA**, náměstkem generálního ředitele pro provozuschopnost dráhy

jako „**Objednatel**“ na straně jedné

a

Název: [DOPLNÍ ZHOTOVITEL]

Sídlo: [DOPLNÍ ZHOTOVITEL]

IČO: [DOPLNÍ ZHOTOVITEL]

DIČ: [DOPLNÍ ZHOTOVITEL]

Bankovní spojení: [DOPLNÍ ZHOTOVITEL]

Číslo účtu: [DOPLNÍ ZHOTOVITEL]

Zapsán: v obchodním rejstříku vedeném [DOPLNÍ ZHOTOVITEL]

Zastoupen: [DOPLNÍ ZHOTOVITEL]

jako „**Zhotovitel č. 1**“

a

Název: [DOPLNÍ ZHOTOVITEL]
Sídlo: [DOPLNÍ ZHOTOVITEL]
IČO: [DOPLNÍ ZHOTOVITEL]
DIČ: [DOPLNÍ ZHOTOVITEL]
Bankovní spojení: [DOPLNÍ ZHOTOVITEL]
Číslo účtu: [DOPLNÍ ZHOTOVITEL]
Zapsán: v obchodním rejstříku vedeném [DOPLNÍ ZHOTOVITEL]
Zastoupen: [DOPLNÍ ZHOTOVITEL]
jako „**Zhotovitel č. 2**“

a

Název: [DOPLNÍ ZHOTOVITEL]
Sídlo: [DOPLNÍ ZHOTOVITEL]
IČO: [DOPLNÍ ZHOTOVITEL]
DIČ: [DOPLNÍ ZHOTOVITEL]
Bankovní spojení: [DOPLNÍ ZHOTOVITEL]
Číslo účtu: [DOPLNÍ ZHOTOVITEL]
Zapsán: v obchodním rejstříku vedeném [DOPLNÍ ZHOTOVITEL]
Zastoupen: [DOPLNÍ ZHOTOVITEL]
jako „**Zhotovitel č. 3**“

(společně jako „**Zhotovitelé**“ a každý jednotlivě též jako „**Zhotovitel**“)

uzavřely níže uvedeného dne, měsíce a roku tuto Rámcovou dohodu

Tato Rámcová dohoda je uzavřena na základě výsledků výběrového řízení na uzavření Rámcové dohody odpovídající podlimitní sektorové veřejné zakázce s názvem Bezpečnostní testování, č.j.: 65652/2026-SŽ-GŘ-O25 (dále jen „**výběrové řízení**“). Jednotlivá ustanovení této Rámcové dohody tak budou vykládána v souladu se zadávacími podmínkami výběrového řízení na uzavření této Rámcové dohody.

I. ÚČEL A PŘEDMĚT DOHODY

1. Předmětem této Rámcové dohody je úprava rámcových podmínek týkajících se veřejných zakázek zadávaných na základě této Rámcové dohody po dobu trvání této Rámcové dohody (dále jen „**dílčí veřejné zakázky**“).
2. Předmětem dílčích veřejných zakázek bude zhotovení Díla, které je obecně specifikováno v bližší specifikaci předmětu plnění, která je přílohou č. 2 této Rámcové dohody, a bude Objednatelem konkrétně specifikováno dílčí smlouvě.

II. ZPŮSOB ZADÁVÁNÍ VEŘEJNÝCH ZAKÁZEK NA ZÁKLADĚ TÉTO RÁMCOVÉ DOHODY

1. Dílčí veřejné zakázky budou zadávány Objednatelem Zhotoviteli postupem uvedeným v této Rámcové dohodě po dobu účinnosti této Rámcové dohody a v souladu se všemi jejími podmínkami a taktéž Obchodními podmínkami uvedenými v příloze č. 1 této Rámcové dohody (dále jen „**dílčí zakázka**“). V rámci dílčí zakázky bude mezi Objednatelem a Zhotovitelem uzavřena smlouva na plnění dílčí veřejné zakázky (dále jen „**dílčí smlouva**“), na základě které Zhotovitel zhotoví pro Objednatele Dílo podle jeho konkrétních potřeb. Dílčí smlouvy budou uzavírány postupem uvedeným v tomto článku této Rámcové dohody.
2. Vznikne-li na straně Objednatele potřeba zadání dílčí zakázky, postupuje Objednatel při zadání dílčí zakázky následovně. Objednatel písemně (e-mailem) vyzve k vyjádření souhlasu s uzavřením dílčí smlouvy všechny Zhotovitele. Součástí výzvy Objednatele je vždy bližší specifikace Díla a nejzazší možný termín jeho provedení (splnění). Bližší specifikace Díla bude obsahovat minimálně přehled následujících požadavků Objednatele:
 - a. obecná specifikace požadovaného bezpečnostního testu (dle příslušné části Přílohy č. 2 této Rámcové dohody), případně jejich kombinací,
 - b. určení požadovaného přístupu k bezpečnostnímu testu (white box / black box / grey box),
 - c. obecná definice cílového prostředí (IS či aplikace – webová, tlustý / tenký klient, zařízení, OT apod.),
 - d. požadovaný termín ukončení prací (tj. nejzazší termín pro předání Zprávy o výsledku testování),
 - e. metodika, dle které má být bezpečnostní test proveden (viz příslušná část Přílohy č. 2 RD Bližší specifikace plnění),
 - f. specifické požadavky na zpracování Zprávy (jsou-li),
 - g. akceptační kritéria.
3. Na základě výzvy Objednatele dle odst. 2 tohoto článku RD jsou Zhotovitelé povinni do 5 pracovních dnů (nestanoví-li Objednatel lhůtu delší) písemně sdělit Objednateli (na e-mailovou adresu: **[DOPLNÍ OBJEDNATEL PŘI PODPISU RÁMCOVÉ DOHODY]**), zda mají zájem požadované plnění provést, a pokud ano, uvedou počet MD (případně vyjádřený v MH¹) nutných na provedení poptávaného plnění a nabídkovou cenu za 1 MD. Při stanovení ceny za 1 MD je Zhotovitel vázán cenou, kterou uvedl ve své nabídce na veřejnou zakázku, přičemž tuto cenu nesmí překročit, může však nabídnout cenu nižší.
4. Bude-li mít Zhotovitel dotaz k předmětu či rozsahu plnění, je oprávněn nejpozději 48 hodin před uplynutím lhůty dle odst. 3 tohoto článku vznést tento dotaz na e-mailovou adresu uvedenou v odst. 3 tohoto článku a Objednatel je povinen na tento dotaz odpovědět nejpozději 12 hodin před uplynutím lhůty stanovené dle odst. 3 tohoto článku. Dotaz a odpověď na něj je Objednatel povinen zaslat na vědomí i ostatním Zhotovitelům.
5. Nevyjádří-li se Zhotovitel ve lhůtě dle odst. 3 tohoto článku či vyjádří-li se s podmínkou, znamená to, že uzavření dílčí smlouvy odmítl. Zhotovitel bere na vědomí, že v rozsahu nabízeného plnění se jedná o neodvolatelnou nabídku Zhotovitele Objednateli ve smyslu § 1736 Občanského zákoníku. Zhotovitel se tak zavazuje k uzavření dílčí smlouvy s Objednatelem v rozsahu, ve kterém Objednateli učinil tuto neodvolatelnou nabídku.
6. K uzavření dílčí smlouvy bude vybrán Zhotovitel, jehož nabídková cena za předmět plnění (stanovená jako součin MD nutných pro provedení plnění a nabídnuté ceny za 1 MD) bude nejnižší. Bude-li nabídková cena za předmět plnění shodná u více Zhotovitelů, bude k uzavření

¹ 1 MD (člověkodenní) = 8 MH (člověkohodin)

dílní smlouvy vybrán ten Zhotovitel, který nabídl nejnižší počet MD nutných pro provedení plnění. Vůči vybranému Zhotoviteli bude dále postupováno dle odst. 7 tohoto článku RD. Ostatní Zhotovitelé, kteří podali nabídku na dílní veřejnou zakázku, budou seřazeni od nejlevnějšího po nejdražšího.

7. Objednatel zahájí dílní zakázku zasláním písemné výzvy k poskytnutí plnění (dále jen „**objednávka**“) vybranému Zhotoviteli. Písemná forma objednávky je splněna, i pokud Objednatel zašle Zhotoviteli objednávku e-mailovou zprávou. Smluvní strany určily následující kontaktní emailové adresy pro zasílání veškerých písemností dle tohoto článku Rámcové dohody:

Objednatel: oprávnění zaměstnanci Správy železnic, státní organizace

Zhotovitel č. 1: **[DOPLNÍ ZHOTOVITEL]**

Zhotovitel č. 2: **[DOPLNÍ ZHOTOVITEL]**

Zhotovitel č. 3: **[DOPLNÍ ZHOTOVITEL]**

8. Objednávky Objednatele dle odst. 7 tohoto článku této Rámcové dohody musí obsahovat údaje potřebné pro uzavření příslušné dílní smlouvy, tedy:
- h. označení Smluvních stran,
 - i. číslo této Rámcové dohody,
 - j. číslo objednávky,
 - k. specifikaci požadovaného Díla,
 - l. kontaktní osobu Objednatele,
 - m. cenu za plnění dílní smlouvy stanovenou postupem dle odst. 3 tohoto článku Rámcové dohody.
 - n. požadovaný termín dokončení prací a předání zhotoveného Díla (tj. nejzazší termín pro předání Zprávy o výsledku testování),
 - o. místo realizace Díla,
 - p. akceptační kritéria pro plnění dílní smlouvy,
 - q. případně další nezbytné údaje ohledně předmětu plnění dílní smlouvy.
9. V případě pochybností či nejasností ohledně údajů uvedených v objednávce je Zhotovitel povinen vyžádat si od Objednatele ve lhůtě uvedené v následujícím odstavci této dohody doplňující informace. Objednatel poskytuje doplňující informace k objednávce vždy úpravou či doplněním objednávky a zasláním takto upravené objednávky Zhotoviteli. Zasláním upravené objednávky Zhotoviteli je původní objednávka bez dalšího stornována a nemůže být již akceptována Zhotovitelem.
10. Zhotovitel je povinen na objednávku Objednatele reagovat písemně na emailovou adresu Objednatele uvedenou v odstavci 2 tohoto článku nejpozději do 3 pracovních dní od jejího doručení anebo ve lhůtě uvedené Objednatelem v objednávce. Písemnou akceptací objednávky ze strany Zhotovitele je uzavřena mezi Zhotovitelem a Objednatelem dílní smlouva na plnění dílní veřejné zakázky, která se sestává z objednávky Objednatele a její akceptace Zhotovitelem, jejíž obsah je dále tvořen dalšími ustanoveními této Rámcové dohody a jejích příloh. Odmítnutím uzavření dílní smlouvy se rozumí i nereagování na objednávku Objednatele způsobem a ve lhůtě dle tohoto odstavce Rámcové dohody; to neplatí v případě § 1743 odst. 1 občanského zákoníku. Ustanovení § 1743 odst. 2 občanského zákoníku se nepoužije.
11. Smluvní strany si postup pro uzavírání dílních smluv dle této Rámcové dohody sjednávají jako smlouvu o smlouvě budoucí dle § 1785 a násl. občanského zákoníku, přičemž předmět budoucích dílních smluv, které budou strany takto uzavírat, je ve smyslu ust. § 1785 občanského zákoníku obecným způsobem vymezen v této Rámcové dohodě a jejích přílohách.

V rámci tohoto obecného vymezení je Objednatel oprávněn vyzývat Zhotovitele opakovaně k postupnému uzavírání jednotlivých budoucích smluv postupem uvedeným v článku II. odst. 2 a 3 této dohody, přičemž výzvou k uzavření dílčí smlouvy se rozumí objednávka. Zhotovitel je povinen výzvu k uzavření dílčí smlouvy akceptovat a smlouvu uzavřít ve lhůtě uvedené v článku II. odst. 5 této dohody. Ujednanou lhůtou pro uzavírání budoucích smluv je doba trvání této Rámcové dohody. Oprávněnou smluvní stranou je Objednatel.

12. Nezahájí-li Zhotovitel, s nímž byla uzavřena dílčí smlouva, provádění předmětu plnění dílčí smlouvy v ujednaném termínu, nebo naplní jiné podmínky pro odstoupení Objednatele od dílčí smlouvy dle odst. 14.2 tohoto článku Rámcové dohody a Objednatel následně odstoupí od dílčí smlouvy, uzavře Objednatel dílčí smlouvu na totožnou dílčí veřejnou zakázku postupem dle odstavce 7 tohoto článku se Zhotovitelem, který vyjádřil souhlas s uzavřením dílčí smlouvy a jehož nabídková cena svou výší bezprostředně převyšuje nabídkovou cenu Zhotovitele, který v souladu s tímto odstavcem nezahájil plnění dílčí smlouvy. Uvedený postup se použije obdobně i na další Zhotovitele v pořadí v případě, kdy u Zhotovitele v pořadí bezprostředně předcházejícího nastane některá ze skutečností dle věty první tohoto odstavce. Postup dle tohoto odstavce lze opakovat. Výběr Zhotovitele k uzavření dílčí smlouvy Objednatel oznámí vybranému Zhotoviteli.
13. Postup podle odst. 6. a 12. tohoto článku Rámcové dohody se nepoužije v případě, že bude Rámcová dohoda uzavřena pouze s jedním Zhotovitelem.
14. Objednatel je oprávněn odstoupit
 - 14.1. od Rámcové dohody vůči Zhotoviteli:
 - a. který minimálně třikrát v průběhu doby trvání této Rámcové dohody odmítl uzavřít dílčí smlouvu k výzvě Objednatele postupem dle tohoto článku (popřípadě se k výzvě nevyjádřil), nebo
 - b. vůči kterému Objednatel třikrát odstoupil od dílčí smlouvy z důvodu dle odstavce 12 věta první tohoto článku, nebo
 - c. který minimálně třikrát v průběhu trvání této Rámcové dohody neprovedl plnění dle dílčí smlouvy řádně a včas.Odstoupení od Rámcové dohody nemá vliv na dílčí veřejné zakázky na základě Rámcové dohody již zadané.
 - 14.2. od dílčí smlouvy vůči Zhotoviteli:
 - a. který nezahájil provádění plnění dílčí smlouvy v ujednaném termínu, nebo
 - b. který přerušil provádění plnění dle dílčí smlouvy, přestože Objednatel trvá na pokračování provádění plnění.

III. DOBA, MÍSTO, ZPŮSOB A LHŮTY PLNĚNÍ

15. Tato Rámcová dohoda je uzavírána na dobu 48 měsíců od nabytí její účinnosti, anebo do doby uzavření dílčí smlouvy, na základě které dojde k objednání díla dle této Rámcové dohody (v součtu všech dílčích smluv) v částce převyšující 5.990.000 Kč bez DPH. V případě, že dojde k ukončení účinnosti této Rámcové dohody dle předchozí věty, nemá toto ukončení vliv na účinnost dílčích smluv, které byly na základě této Rámcové dohody uzavřeny. Objednatel není oprávněn na základě této Rámcové dohody učinit objednávky (v součtu všech objednávek) přesahující částku 6.000.000 Kč bez DPH.
16. Místo plnění dílčích smluv je zpravidla uvedeno v dílčí smlouvě. Dopravu do a z místa plnění zajišťuje Zhotovitel.
17. Přejímací řízení:
 - 17.1. Ustanovení čl. 8 Zvláštních obchodních podmínek, které jsou přílohou č. 7 Rámcové dohody se

pro účely této RD neužijí. Pro účely akceptace Díla se užití ustanovení části 12. Obchodních podmínek, které jsou přílohou č. 1 této RD.

- 17.2. Dodavatel je povinen předložit Objednateli Dílo (resp. Zprávu) k provedení přejímacího řízení. Okamžikem předání Díla Objednateli k provedení přejímacího řízení je přejímací řízení zahájeno.
- 17.3. Objednatel je povinen do 7 kalendářních dnů posoudit, zda Dílo bylo provedeno v souladu s požadavky ujednanými v Dílčí smlouvě. Zjistí-li Objednatel jakékoliv vady Díla, je povinen veškeré tyto vady Zhotoviteli vytknout v dostatečném detailu tak, aby mohl Zhotovitel vady odstranit. Převzít Dílo s vadami je Objednatel oprávněn pouze za předpokladu, že se jedná o drobné vady, které nemají za následek nepoužitelnost výsledků testování či jejich zjevnou nesprávnost či neurčitost.
- 17.4. Minimální výše denní smluvní pokuty za prodlení s provedením Díla dle odst. 174 přílohy č. 1 této RD je stanovena na částku 2.000 Kč.
- 17.5. Minimální výše denní smluvní pokuty za neodstranění vad dle odst. 175 přílohy č. 1 této RD je stanovena na částku 2.000 Kč.
- 17.6. Dílo se považuje za provedené až okamžikem podpisu předávacího protokolu s vyznačením „Převzato“, nebo „Převzato s výhradou“.

IV. CENA DÍLA A PLATEBNÍ PODMÍNKY

1. Cena za plnění dílčí smlouvy je uvedena v dílčí smlouvě a stanovena v souladu s postupem dle odst. 6 čl. II této RD.
2. Cena uvedená v odst. 1 tohoto článku této Rámcové dohody je cenou konečnou, zahrnující veškeré související náklady Zhotovitele, včetně případných nákladů na dopravu apod. Zhotovitel je touto cenou vázán po dobu plnění dílčí smlouvy.
3. Jednotkové ceny za provádění Díla uvedené v příloze č. 3 této Rámcové dohody jsou smluvními stranami sjednány jako ceny maximální, nepřekročitelné a představují nejvyšší možnou nabídkovou cenu příslušného Zhotovitele v rámci soutěže na dílčí veřejnou zakázku.
 - 3.1. Právo na zaplacení příslušné části ceny Zhotoviteli vzniká (okamžikem, ke kterému je Zhotovitel oprávněn vystavit fakturu) dokončením Díla či jeho příslušné části dle dílčí smlouvy a vyznačením v Předávacím protokolu „Převzato“, nebo „Převzato s výhradou“.
4. Faktura musí mít náležitosti daňového dokladu, její přílohou musí být stejnopis schváleného Předávacího protokolu s potvrzením převzetí plnění bez jakýchkoliv výhrad/vad Objednatel. V záhlaví faktury je nutno taktéž uvést číslo objednávky a této Rámcové dohody.
5. Daňové doklady (faktura), vč. všech příloh, budou zasílány pouze elektronicky do datové schránky Objednatele. V případě technických problémů s vyhotovením elektronické podoby daňového dokladu či jeho příloh (např. nečitelnost skenu) bude objednatel akceptovat daňový doklad doručený v listinné podobě.
6. Splatnost faktury se sjednává na 30 kalendářních dnů od jejího doručení Objednateli. V případě, že faktura nebude mít odpovídající náležitosti, je Objednatel oprávněn ve lhůtě splatnosti ji vrátit Zhotoviteli s vytknutím nedostatků, aniž by se dostal do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od okamžiku doručení opravené či doplněné faktury Objednateli.

V. PODDODAVATELÉ A REALIZAČNÍ TÝM

1. Na provedení Díla se budou podílet poddodavatelé uvedení v příloze č. 4 této Rámcové dohody.
2. Na provedení Díla se budou podílet členové realizačního týmu uvedení v příloze č. 5 této Rámcové dohody, a to minimálně v rozsahu, který je blíže vymezen tamtéž.

3. Zhotovitel může v průběhu provádění Díla nahradit některé osoby z osob uvedených v seznamu realizačního týmu dle přílohy č. 5 této Rámcové dohody pouze po předchozím souhlasu Objednatele na základě písemné žádosti Zhotovitele. V případě, že Zhotovitel požádá o změnu některých členů realizačního týmu uvedeného v příloze č. 5 této Rámcové dohody, musí tato osoba splňovat kvalifikaci požadovanou ve Veřejné zakázce. Změna osoby nepodléhá povinnosti uzavřít dodatek k Rámcové dohodě a proběhne na základě písemného souhlasu Objednatele s touto změnou.

VI. DALŠÍ UJEDNÁNÍ

1. Smluvní strany berou na vědomí, že tato Rámcová dohoda (následně odstavce se týkají jak této Rámcové dohody, tak dílčích smluv s hodnotou převyšující 50.000,- Kč bez DPH), podléhá uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů (dále jen „ZRS“), a současně souhlasí se zveřejněním údajů o identifikaci smluvních stran, předmětu a účelu této Rámcové dohody a dílčích smluv, její ceně či hodnotě a datu uzavření této Rámcové dohody nebo dílčí smlouvy. Osoby uzavírající tuto Rámcovou dohodu za Smluvní strany souhlasí s uveřejněním svých osobních údajů, které jsou uvedeny v této Rámcové dohodě, spolu s touto Rámcovou dohodou v registru smluv. Tento souhlas je udělen na dobu neurčitou.
2. Zaslání této Rámcové dohody a dílčích smluv správci registru smluv k uveřejnění v registru smluv zajišťuje Objednatel. Nebude-li tato Rámcová dohoda nebo dílčí smlouva zaslána k uveřejnění a/nebo uveřejněna prostřednictvím registru smluv, není žádná ze smluvních stran oprávněna požadovat po druhé Smluvní straně náhradu škody ani jiné újmy, která by jí v této souvislosti vznikla nebo vzniknout mohla.
3. Smluvní strany výslovně prohlašují, že údaje a další skutečnosti uvedené v této Rámcové dohodě a dílčích smlouvách, vyjma částí označených ve smyslu následujícího odstavce této Rámcové dohody, nepovažují za obchodní tajemství ve smyslu ustanovení § 504 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**obchodní tajemství**“), a že se nejedná ani o informace, které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS.
4. Jestliže Smluvní strana označí za své obchodní tajemství část obsahu této Rámcové dohody nebo dílčí smlouvy, která v důsledku toho bude pro účely uveřejnění této Rámcové dohody nebo dílčí smlouvy v registru smluv znečitelněna, nese tato Smluvní strana odpovědnost, pokud by tato Rámcová dohoda nebo dílčí smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, která ze Smluvních stran tuto Rámcovou dohodu nebo dílčí smlouvu v registru smluv uveřejnila. S částmi této Rámcové dohody nebo dílčí smlouvy, které druhá Smluvní strana neoznačí za své obchodní tajemství před uzavřením této Rámcové dohody nebo dílčí smlouvy, nebude Objednatel jako s obchodním tajemstvím nakládat a ani odpovídat za případnou škodu či jinou újmu takovým postupem vzniklou. Označením obchodního tajemství ve smyslu předchozí věty se rozumí Objednateli doručené písemné oznámení druhé Smluvní strany obsahující přesnou identifikaci dotčených částí této Rámcové dohody nebo dílčí smlouvy včetně odůvodnění, proč jsou za obchodní tajemství považovány. Druhá Smluvní strana je povinna výslovně uvést, že informace, které označila jako své obchodní tajemství, naplňují současně všechny definiční znaky obchodního tajemství, tak jak je vymezeno v ustanovení § 504 občanského zákoníku, a zavazuje se neprodleně písemně sdělit Objednateli skutečnost, že takto označené informace přestaly naplňovat znaky obchodního tajemství.

VII. STŘET ZÁJMŮ, POVINNOSTI ZHOTOVITELE V SOUVISLOSTI S KONFLIKTEM NA UKRAJINĚ

1. Zhotovitel prohlašuje, že není obchodní společností, ve které veřejný funkcionář uvedený v

ust. § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (dále jen „**Zákon o střetu zájmů**“) nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti, a že žádní poddodavatelé, jimiž prokazoval kvalifikaci v zadávacím řízení na zadání Veřejné zakázky, nejsou obchodní společnostmi, ve které veřejný funkcionář uvedený v ust. § 2 odst. 1 písm. c) Zákona o střetu zájmů nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti.

2. Zhotovitel prohlašuje, že:
 - a. on, ani žádný z jeho poddodavatelů, nejsou osobami, na něž se vztahuje zákaz zadání veřejné zakázky ve smyslu § 48a zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů,
 - b. on, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost byla využita ve smyslu evropských směrnic o zadávání veřejných zakázek, nejsou osobami dle článku 5k nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění pozdějších předpisů, jimž se zakazuje zadat nebo dále plnit jakoukoli veřejnou zakázku nebo koncesní smlouvu spadající do oblasti působnosti směrnic o zadávání veřejných zakázek, jakož i čl. 10 odst. 1, 3, odst. 6 písm. a) až e), odst. 8, 9 a 10, článků 11, 12, 13 a 14 směrnice 2014/23/EU, článku 7 písm. a) až d), článku 8, čl. 10 písm. b) až f) a písm. h) až j) směrnice 2014/24/EU, článku 18, čl. 21 písm. b) až e) a písm. g) až i), článků 29 a 30 směrnice 2014/25/EU a čl. 13 písm. a) až d), f) až h) a j) směrnice 2009/81/ES a hlavy VII nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046,
 - c. on, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost byla využita ve smyslu evropských směrnic o zadávání veřejných zakázek, nejsou osobami dle článku 2 nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění pozdějších předpisů, a dalších prováděcích předpisů k tomuto nařízení Rady (EU) č. 269/2014 anebo osobami dle čl. 2 nařízení uvedených v odstavci 5 této Smlouvy (dále jen „**Sankční seznamy**“).
3. Je-li Zhotovitelem sdružení více osob, platí podmínky dle odstavce 1 a 2 tohoto článku Rámcové dohody také jednotlivě pro všechny osoby v rámci Zhotovitele sdružené, a to bez ohledu na právní formu tohoto sdružení.
4. Přestane-li Zhotovitel nebo některý z jeho poddodavatelů nebo jiných osob, jejichž způsobilost byla využita ve smyslu evropských směrnic o zadávání veřejných zakázek, splňovat podmínky dle tohoto článku Rámcové dohody, oznámí tuto skutečnost bez zbytečného odkladu, nejpozději však do 3 pracovních dnů ode dne, kdy přestal splňovat výše uvedené podmínky, Objednateli.
5. Zhotovitel se dále zavazuje postupovat při plnění dílčích smluv uzavřených na základě této Rámcové dohody v souladu s nařízením Rady (ES) č. 765/2006 ze dne 18. května 2006 o omezujících opatřeních vzhledem k situaci v Bělorusku a k zapojení Běloruska do ruské agrese proti Ukrajině, ve znění pozdějších předpisů, nařízením Rady (EU) č. 208/2014 ze dne 5. března 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině, ve znění pozdějších předpisů, a dalších prováděcích předpisů k těmto nařízením.
6. Zhotovitel se dále zavazuje, že finanční prostředky ani hospodářské zdroje, které obdrží od Objednatele na základě této Smlouvy a jejich případných dodatků, nezpřístupní přímo ani nepřímým fyzickým nebo právnickým osobám, subjektům či orgánům s nimi spojeným uvedeným v Sankčních seznamech, nebo v jejich prospěch.
7. Ukáže-li se jakékoliv prohlášení Zhotovitele dle tohoto článku Rámcové dohody jako nepravdivé nebo poruší-li Zhotovitel svou oznamovací povinnost nebo některou z dalších povinností dle tohoto článku Rámcové dohody, je Objednatel oprávněn odstoupit od této

Rámcové dohody. Objednatel je vedle toho oprávněn vypovědět jednotlivé dílčí smlouvy uzavřené na základě této Rámcové dohody. Zhotovitel je dále povinen zaplatit za každé jednotlivé porušení povinností dle předchozí věty smluvní pokutu ve výši 300.000,- Kč (slovy tři sta tisíc korun českých).

VIII. COMPLIANCE

1. Smluvní strany stvrzují, že při uzavírání této smlouvy jednaly a postupovaly čestně a transparentně a zavazují se tak jednat i při plnění této smlouvy a veškerých činnostech s ní souvisejících. Každá ze smluvních stran se zavazuje jednat v souladu se zásadami, hodnotami a cíli compliance programů a etických hodnot druhé smluvní strany, pakliže těmito dokumenty dotčené smluvní strany disponují, a jsou uveřejněny na webových stránkách smluvních stran (společnosti).
2. Správa železnic, státní organizace, má výše uvedené dokumenty k dispozici na webových stránkách: <https://www.spravazeleznic.cz/o-nas/nezadouci-jednani-a-boj-s-korupci>.
3. Zhotovitel má výše uvedené dokumenty k dispozici na webových stránkách: **[doplň Zhotovitel x nemá-li Zhotovitel výše uvedené dokumenty, celý odst. 3 odstraní]**.

IX. ZÁVĚREČNÁ UJEDNÁNÍ

1. Osobami oprávněnými jednat ve vztahu k této Rámcové dohodě jsou:
na straně Objednatele: **[.....,@....., tel.: ..]**
na straně Zhotovitele: **[DOPLŇ ZHOTOVITEL]**
2. Obě Smluvní strany prohlašují, že si tuto Rámcovou dohodu před jejím podpisem přečetly, a že byla uzavřena po vzájemném projednání jako projev jejich svobodné vůle určitě, vážně a srozumitelně. Na důkaz dohody o všech článcích této Rámcové dohody připojují pověření zástupci obou Smluvních stran své podpisy.
3. Ustanovení přílohy č. 6 Platforma SŽ (včetně jejích příloh) mají přednost před ustanoveními obchodních podmínek uvedených v odst. 4. tohoto článku Rámcové dohody.
4. Rámcová dohoda se řídí Obchodními podmínkami Objednatele (příloha č. 1) a Zvláštními obchodními podmínkami Objednatele (příloha č. 7). Ustanovení Zvláštních obchodních podmínek mají přednost před ustanoveními Obchodních podmínek, pokud jsou ustanovení těchto dokumentů v rozporu, uplatní se ustanovení uvedené ve Zvláštních obchodních podmínkách.
5. Odchylná ujednání v této Smlouvě mají přednost před ustanoveními Obchodních podmínek a Zvláštních obchodních podmínek.
6. Zhotovitel prohlašuje, že se zněním obchodních podmínek před podpisem této Rámcové dohody seznámil v dostatečném rozsahu s veškerými požadavky Objednatele dle této Rámcové dohody, přičemž si není vědom žádných překážek, které by mu bránily v poskytnutí sjednaného plnění v souladu s touto Rámcovou dohodou.
7. Zhotovitel prohlašuje, že je způsobilý k řádnému a včasnému provedení Díla a že disponuje takovými kapacitami a odbornými znalostmi, které jsou třeba k řádnému provedení Díla.
8. Tato Rámcová dohoda je vyhotovena v elektronické podobě, přičemž obě Smluvní strany obdrží její elektronický originál opatřený elektronickými podpisy. V případě, že tato Rámcová dohoda z jakéhokoli důvodu nebude vyhotovena v elektronické podobě, bude sepsána ve třech vyhotoveních, ve dvou vyhotoveních pro Objednatele a jedno obdrží Zhotovitel.
9. Smluvní vztahy výslovně neupravené touto Rámcovou dohodou a Obchodními podmínkami se řídí Občanským zákoníkem a platnými obecně závaznými právními předpisy. Veškerá práva a povinnosti Smluvních stran vyplývající z této Rámcové dohody se řídí českým právním

řádem.

10. Smluvní strany se zavazují řešit případné spory vzniklé ze vzájemných obchodních smluvních vztahů především smírně – jednáním. Nedojde-li k dohodě, dohodly se Smluvní strany na tom, že k projednání sporů je příslušný obecný soud Objednatele. Rozhodným právem pro řešení sporů je právo České republiky a jednacím jazykem je český jazyk.
11. Pokud některá ustanovení Obchodních podmínek nebo jejich část nelze vzhledem k povaze Díla objektivně a zcela zřejmě použít, pak z takových ustanovení nebo jejich částí práva ani povinnosti smluvním stranám nevznikají.
12. Tato Rámcová dohoda nabývá platnosti okamžikem jejího podpisu poslední ze Smluvních stran. Účinnosti nabývá Rámcová dohoda dnem, kdy uplyne účinnost smlouvy č. j. 78281/2022-SŽ-GŘ-O8 ze dne 5. 1. 2023. Je-li tato Rámcová dohoda uveřejňována v registru smluv, nabývá účinnosti nejdříve dnem uveřejnění v registru smluv.

Přílohy tvořící nedílnou součást této Rámcové dohody:

Příloha č. 1 – Obchodní podmínky

Příloha č. 2 – Bližší specifikace plnění

Příloha č. 3 – Ceník

Příloha č. 4 – Seznam poddodavatelů

Příloha č. 5 - Realizační tým

Příloha č. 6 - Platforma SŽ

Příloha č. 7 – Zvláštní obchodní podmínky pro ICT zakázky

Za Objednatele

Za Zhotovitele:

Ing. Mojmír Nejezchleb

zástupce generálního ředitele pověřený
správní radou řízením organizace

[DOPLNÍ ZHOTOVITEL]

Ing. Karel Švejda, MBA

náměstek generálního ředitele
pro provozuschopnost dráhy

OBCHODNÍ PODMÍNKY K RÁMCOVÉ DOHODĚ

OBSAH OBCHODNÍCH PODMÍNEK

ČÁST 1 - ÚVODNÍ USTANOVENÍ.....	2
ČÁST 2 - DÍLO	3
ČÁST 3 - CENA DÍLA	3
ČÁST 4 - ZMĚNA CENY DÍLA.....	4
ČÁST 5 - PLATEBNÍ PODMÍNKY	4
ČÁST 6 - MÍSTO PLNĚNÍ.....	5
ČÁST 7 - DOBA PLNĚNÍ	5
ČÁST 8 - PROVÁDĚNÍ DÍLA	5
ČÁST 9 - ZKUŠEBNÍ PROVOZ	8
ČÁST 10 - PŘEPRAVA DÍLA.....	8
ČÁST 11 - PODDODAVATELÉ	9
ČÁST 12 - PŘEDÁNÍ A PŘEVZETÍ DÍLA	9
ČÁST 13 - VLASTNICKÉ PRÁVO A NEBEZPEČÍ ŠKODY	10
ČÁST 14 - VADY PLNĚNÍ A ZÁRUKA.....	11
ČÁST 15 - UPLATNĚNÍ PRÁV Z VADNÉHO PLNĚNÍ	11
ČÁST 16 - PODMÍNKY ODSTRANĚNÍ VAD.....	12
ČÁST 17 - POJIŠTĚNÍ	13
ČÁST 18 - DUŠEVNÍ VLASTNICTVÍ.....	13
ČÁST 19 - SANKCE	14
ČÁST 20 - OBECNÁ ODPOVĚDNOST ZHOTOVITELE	16
ČÁST 21 - Odstoupení od dílčí smlouvy a rámcové dohody	17
ČÁST 22 - OSTATNÍ UJEDNÁNÍ.....	18

ČÁST 1 - ÚVODNÍ USTANOVENÍ

1. Pro účely těchto Obchodních podmínek mají následující slova význam u nich uvedený:
 - 1.1. **Občanský zákoník** – zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
 - 1.2. **ZoDPH** – zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
 - 1.3. **ZoÚ** – zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů.
 - 1.4. **SZ** – zákon č. 283/2021 Sb., stavební zákon, ve znění pozdějších předpisů.
 - 1.5. **ZZVZ** – zákon č. 134/2016 Sb., o zadávání veřejných zakázkách, ve znění pozdějších předpisů.
 - 1.6. **Objednatel** – Správa železnic, státní organizace, IČO 70994234, se sídlem Praha 1 – Nové Město, Dlážďená 1003/7, PSČ 110 00, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. A 48384.
 - 1.7. **Zhotovitel** – osoba uvedená Rámcové dohodě jako Zhotovitel; též všechny osoby, které jsou Rámcové dohodě uvedené na straně Zhotovitele, je-li na straně Zhotovitele více než jedna osoba.
 - 1.8. **Smluvní strany** – Objednatel a Zhotovitel.
 - 1.9. **Smluvní strana** – Objednatel nebo Zhotovitel dle smyslu ujednání.
 - 1.10. **Nabídka** – souhrn dokumentů, které Zhotovitel podal jako návrh do zadávacího řízení, na jehož základě byla uzavřena Rámcová dohoda.
 - 1.11. **Rámcová dohoda** – smlouva/dohoda uzavřená mezi Smluvními stranami, která odkazuje na Obchodní podmínky.
 - 1.12. **Dílčí smlouva** – dílčí smlouva uzavřená na základě Rámcové dohody způsobem uvedeným v Rámcové dohodě.
 - 1.13. **Obchodní podmínky** – tento text obchodních podmínek.
 - 1.14. **Předmět Díla** – věc, která má být zhotovena, nebo činnost s jiným výsledkem, specifikovaná obecně v Rámcové dohodě a konkrétně v Dílčí smlouvě.
 - 1.15. **Související plnění** – další plnění (práce, dodávky, služby, činnosti a výkony), která je Zhotovitel povinen dle Rámcové dohody nebo Dílčí smlouvy poskytnout vedle samotného provedení Předmětu díla.
 - 1.16. **Rozhodnutí Objednatele** – veškerá rozhodnutí, sdělení, souhlasy, povolení či jiné výsledky úkonů orgánů státní správy, samosprávy či jiných subjektů, které pro účely Díla nebo v souvislosti s ním získal nebo do doby dokončení Díla získá Objednatel a jež Objednatel Zhotoviteli předal nebo s nimiž se Zhotovitel jinak seznámil.
 - 1.17. **Rozhodnutí Zhotovitele** – veškerá rozhodnutí, sdělení, souhlasy, povolení či jiné výsledky úkonů orgánů státní správy, samosprávy či jiných subjektů, které je Zhotovitel povinen dle Rámcové dohody nebo Dílčí smlouvy získat. Jakékoliv Rozhodnutí Zhotovitele, které není v českém jazyku, musí být do českého jazyka přeloženo a překlad musí být úředně ověřen.
 - 1.18. **Veřejnoprávní podklady** – souhrn Rozhodnutí Objednatele a Rozhodnutí Zhotovitele.
 - 1.19. **Doklady** – veškeré listiny, které se vztahují k Předmětu Díla nebo Souvisejícímu plnění a které jsou třeba k jejich převzetí a užívání; veškerá Rozhodnutí Zhotovitele; veškeré další listiny, vyjma Výzvy k úhradě, které je Zhotovitel dle Rámcové dohody nebo Dílčí smlouvy povinen předat Objednateli. Všechny Doklady musejí být v českém jazyku, nebo v původním jazyku s překladem do českého jazyka, není-li uvedeno jinak.
 - 1.20. **Dílo** – souhrn veškerých plnění, která je Zhotovitel povinen provést za účelem splnění Dílčí smlouvy; zahrnuje zejm. provedení Předmětu díla, poskytnutí či provedení Souvisejícího plnění a dodání Dokladů.
 - 1.21. **Cena Díla** – cena za Dílo uvedená v Dílčí smlouvě (částka bez DPH) anebo v případě, že v dílčí smlouvě sjednána není, je Cena Díla stanovena dle jednotkových cen sjednaných v Rámcové dohodě a množství skutečně realizovaných položek se sjednanou jednotkovou cenou v Rámcové dohodě Zhotovitelem při zhotovení Díla a odsouhlasených Objednatel na základě Zhotovitelem předloženého Akceptačního protokolu/Předávacího protokolu.

- 1.22. **Výzva k úhradě** – daňový doklad, je-li Zhotovitel povinen dle ZoDPH uhradit v souvislosti s provedením Díla nebo jeho části DPH, nebo faktura, pokud Zhotovitel v souvislosti s provedením Díla nebo jeho části není dle ZoDPH povinen uhradit DPH.
- 1.23. **Vícepráce** – práce, dodávky nebo služby nad rámec Dílčí smlouvy, na jejichž provedení se Smluvní strany dohodnou po uzavření Dílčí smlouvy.
- 1.24. **Méněpráce** – práce, dodávky nebo služby v rámci Dílčí smlouvy, na jejichž vypuštění se Smluvní strany dohodnou po uzavření Dílčí smlouvy.
- 1.25. **Obalový materiál** – palety, dřevěné desky či jiné věci, které slouží pro potřeby přepravy nebo ochrany Předmětu díla. Dle kontextu Rámcové dohody se rozumí Obalovým materiálem též jednotlivý kus palety, dřevěné desky nebo jiné věci.
- 1.26. **Přejímací řízení** – proces, při kterém Zhotovitel předává a Objednatel kontroluje a přebírá Dílo, nebo je odmítá.
- 1.27. **Předávací protokol** – listina osvědčující předání a převzetí Díla nebo jeho části, jejíž minimální náležitosti jsou uvedeny v části Předání a převzetí Díla.
- 1.28. **Záruční doba** – doba, do jejíhož uplynutí je Objednatel oprávněn uplatňovat práva z vad plnění poskytnutého Zhotovitelem na základě Rámcové dohody; Záruční doba činí 24 měsíců, není-li stanoveno v Rámcové dohodě jinak.
- 1.29. **CTD** – Centrum techniky a diagnostiky, organizační jednotka Objednatele.

ČÁST 2 - DÍLO

- 2. Zhotovitel se zavazuje provést na svůj náklad a nebezpečí pro Objednatele Dílo a Objednatel se zavazuje Dílo převzít a zaplatit Zhotoviteli Cenu díla a příslušnou DPH, bude-li Zhotovitel povinen dle ZoDPH uhradit v souvislosti s provedením Díla nebo jeho části DPH.
- 3. Zhotovitel je povinen provést Dílo v jakosti, provedení a způsobem uvedeným v Rámcové dohodě a Dílčí smlouvě a zároveň
 - 3.1. v jakosti, provedení a způsobem, jenž odpovídá vlastnostem a způsobu, které Zhotovitel popsal nebo které Objednatel očekával s ohledem na povahu Díla, a to v rozsahu, ve kterém není v rozporu s jakostí, provedením a způsobem sjednaným v Rámcové dohodě a Dílčí smlouvě,
 - 3.2. v jakosti, provedení a způsobem, jenž se hodí k účelu vyplývajícímu z Rámcové dohody a není-li v ní vyjádřen pak k účelu, ke kterému se Dílo obvykle používá, a to v rozsahu, ve kterém není v rozporu s jakostí, provedením a způsobem sjednaným v Rámcové dohodě,
 - 3.3. v souladu s Veřejnoprávními podklady,
 - 3.4. v souladu s požadavky právních předpisů, interních předpisů objednatele vztahujících se k provádění díla, Technických kvalitativních podmínek státních drah (dále též jen „TKP státních drah“) a příslušných ČSN.
- 4. Je-li jakost či provedení Předmětu díla zároveň určeno vzorkem nebo předlohou, musí Předmět díla odpovídat jakostí nebo provedením vzorku nebo předloze. Liší-li se jakost nebo provedení určené v Rámcové dohodě a vzorek nebo předloha, rozhoduje Rámcová dohoda. Určuje-li Rámcová dohoda a vzorek nebo předloha jakost nebo provedení rozdílně, nikoliv však rozporně, musí Předmět díla odpovídat Rámcové dohodě a Dílčí smlouvě i vzorku nebo předloze.
- 5. Opatřuje-li Zhotovitel věc za účelem jejího zpracování při provádění Díla, je povinen opatřit věc novou, nepoužitou a neopotřebovanou.
- 6. Je-li součástí Díla povinnost Zhotovitele zajistit jakékoliv Rozhodnutí Zhotovitele, je Zhotovitel povinen provést veškeré činnosti, kterých je k získání příslušného Rozhodnutí Zhotovitele třeba.

ČÁST 3 - CENA DÍLA

- 7. Cena díla zahrnuje veškeré náklady Zhotovitele spojené se splněním jeho povinností vyplývajících z Dílčí smlouvy, Rámcové dohody a Obchodních podmínek a zisk Zhotovitele.

8. Objednatel není povinen hradit v souvislosti s plněním Dílčí smlouvy žádné jiné finanční částky, než Cenu díla a případně příslušnou DPH, není-li uvedeno jinak (tím není dotčeno právo Zhotovitele na případnou úhradu smluvní pokuty, úroků z prodlení, či jiných sankcí, a právo na náhradu škody způsobené Objednatelem).
9. Cena díla obsahuje předpokládaný vývoj cen vstupních nákladů a předpokládané zvýšení ceny v závislosti na čase plnění, a to až do dokončení Díla.
10. Je-li Zhotovitel povinen dle ZoDPH uhradit v souvislosti s provedením Díla nebo jeho části DPH, je Objednatel povinen Zhotoviteli takovou DPH uhradit vedle Ceny díla.
11. Cenu díla lze měnit pouze za podmínek uvedených v části Změna ceny Díla (viz ČÁST 4 - Obchodních podmínek).
12. Konečné finanční částky na fakturách/daňových dokladech nesmí být zaokrouhovány na celé Kč. Objednatel nebude akceptovat zaokrouhlení a haléřové vyrovnání v případě uvedení na faktuře/daňovém dokladu nebude hradit.

ČÁST 4 - ZMĚNA CENY DÍLA

13. Změna ceny díla je možná pouze v případě
 - 13.1. víceprací nebo méněprací,
 - 13.2. zjistí-li Zhotovitel v případech, kdy je pro zhotovení Díla Objednatelem vyhotovena projektová dokumentace, kontrolou vady této dokumentace nebo její nevhodnost či neúplnost, které mají vliv na náklady Zhotovitele,
 - 13.3. v jiných případech jen pokud se na tom Smluvní strany dohodnou.
14. V případě víceprací i méněprací Zhotovitel provede ocenění jejich soupisu dle jednotkových cen sjednaných v Rámcové dohodě, jsou-li v Rámcové dohodě takové jednotkové ceny sjednány.
15. Pokud pro práce, dodávky nebo služby, které jsou předmětem víceprací, nejsou v Rámcové dohodě sjednány jednotkové ceny, užije se pro jejich ocenění Sborník prací pro údržbu a opravy železniční infrastruktury v platném znění (dále jen „Sborník“), a pokud se ceny ve Sborníku nevyskytují, použije se cena obvyklá v místě a čase.
16. V případě situace uvedené v bodu 13.2 Obchodních podmínek, postupují smluvní strany obdobně jako při oceňování víceprací nebo méněprací.
17. Změnu Ceny díla lze provést jen uzavřením dodatku k Dílčí smlouvě.

ČÁST 5 - PLATEBNÍ PODMÍNKY

18. Objednatel neposkytuje zálohy.
19. Zhotovitel vyúčtuje Objednateli Cenu díla a případnou DPH Výzvou k úhradě.
20. Cenu díla a případnou DPH je Objednatel povinen uhradit Zhotoviteli do 30 dnů ode dne doručení Výzvy k úhradě Objednateli. Výzvu k úhradě je Zhotovitel oprávněn vystavit až po převzetí Díla, případně úspěšném ukončení zkušebního provozu, nastane-li den skončení zkušebního provozu později než převzetí Díla Objednatelem.
21. Cena díla a případná DPH je uhrazena dnem jejich odepsání z bankovního účtu Objednatele.
22. Je-li Výzva k úhradě fakturou, musí obsahovat náležitosti účetního dokladu dle §11 ZoÚ a náležitosti stanovené v §435 Občanského zákoníku.
23. Je-li Výzva k úhradě daňovým dokladem, musí obsahovat náležitosti daňového dokladu dle §28 ZoDPH a náležitosti stanovené v §435 Občanského zákoníku.
24. Výzva k úhradě musí vždy obsahovat číslo Rámcové dohody, včetně uvedení uzavřených dodatků, její přílohou musí být vždy jedno vyhotovení Protokolu o převzetí potvrzeného Objednatelem a případné další dokumenty, požadované Rámcovou dohodou. Ve výzvě k úhradě musí být vždy uvedeny jako identifikace Objednatele nejméně následující údaje:
Správa železnic, státní organizace
Dlážděná 1003/7, 110 00 Praha 1 – Nové Město
IČO: 709 94 234
Obchodní rejstřík u Městského soudu v Praze, sp. zn. A 48384

25. Výzvu k úhradě je Zhotovitel povinen doručit Objednateli **ve dvou vyhotoveních**.
26. Výzvy k úhradě, vč. všech příloh, budou Objednateli zasílány následovně:
 - 26.1. v digitální podobě na e-mailovou adresu ePodatelnaCFU@spravazeleznic.cz, nebo
 - 26.2. v digitální podobě do datové schránky s identifikátorem Uccchjm, nebo
 - 26.3. v listinné podobě **ve dvou vyhotoveních** na adresu Správa železnic, státní organizace, Centrální finanční účtárna Čechy, Náměstí Jana Pernera 217, 530 02 Pardubice, nebo
 - 26.4. prostřednictvím kontaktního formuláře na webových stránkách Objednatele <https://www.spravazeleznic.cz/kontakty/podatelna>.Objednatel upřednostňuje příjem Výzev k úhradě v digitální podobě ve formátu PDF/A, ISO 19005, min. verze PDF/A-2b, na výše uvedené emailové adrese. V případě, že je Výzva k úhradě zasílána na výše uvedenou e-mailovou adresu, považuje se za doručenou po obdržení notifikace doručení, která je automaticky odesílána odesílateli.
27. Stanoví-li Výzva k úhradě splatnost delší, než je jako minimální stanovena v odstavci 20, je Objednatel oprávněn uhradit Cenu díla a případnou DPH ve lhůtě splatnosti určené ve Výzvě k úhradě.
28. Stane-li se zhotovitel nespolehlivým plátcem nebo daňový doklad zhotovitele bude obsahovat číslo bankovního účtu, na který má být plněno, aniž by bylo uvedeno ve veřejném registru spolehlivých účtů, je objednatel oprávněn z finančního plnění uhradit daň z přidané hodnoty přímo místně a věcně příslušnému správci daně zhotovitele.
29. Je-li v Rámcové dohodě nebo Dílčí smlouvě výslovně stanoveno, že Zhotovitel bude předávat Objednateli Dílo po částech, je Zhotovitel oprávněn vystavit Výzvu k úhradě předávané části Díla poté, co Objednatel převezme příslušnou část Díla. Ustanovení odstavců 20 - 28 Obchodních podmínek se užití obdobně.
30. Ustanovení §2611, §2620 - 2622 a §2624 Občanského zákoníku se neuplatní.

ČÁST 6 - MÍSTO PLNĚNÍ

31. Zhotovitel je povinen předat Objednateli Dílo v místě, jež vyplývá z Dílčí smlouvy. Nelze-li takto místo předání Díla zjistit, vyzve Zhotovitel Objednatele, aby sdělil, ve kterém místě má Zhotovitel Objednateli Dílo předat. Nesdělí-li Objednatel místo plnění do 5 pracovních dnů ode dne doručení výzvy Zhotovitele, je Zhotovitel povinen Dílo předat Objednateli v sídle Objednatele.

ČÁST 7 - DOBA PLNĚNÍ

32. Zhotovitel je povinen zahájit provádění Díla bez zbytečného odkladu po uzavření Dílčí smlouvy, není-li v Dílčí smlouvě uvedený jiný termín zahájení prací.
33. Je-li součástí povinností Zhotovitele doprava Díla po jeho zhotovení do místa plnění dle Dílčí smlouvy, je Zhotovitel povinen dopravit Dílo do místa plnění v pracovní den v době od 8 do 15 hodin, není-li v Rámcové dohodě nebo Dílčí smlouvě sjednána jiná doba. Dodá-li Zhotovitel Dílo Objednateli v jiné než uvedené době, je Objednatel oprávněn odmítnout Dílo převzít a není zároveň v prodlení s převzetím Díla. Případně-li konec sjednané doby plnění na sobotu, neděli nebo svátek, není Zhotovitel v prodlení, dodá-li Dílo nejbližší následující pracovní den v časovém rozmezí dle tohoto odstavce.
34. Není-li stanoveno jinak, je Zhotovitel povinen začít s plněním svých povinností vždy bez zbytečného odkladu.
35. Zjistí-li Zhotovitel jakékoliv skutečnosti, které by mohly mít vliv na dobu plnění, je Zhotovitel povinen bez zbytečného odkladu Objednatele o takových skutečnostech informovat.

ČÁST 8 - PROVÁDĚNÍ DÍLA

36. Zhotovitel provede Dílo s potřebnou péčí v ujednaném čase a obstará vše, co je k provedení Díla potřeba.
37. Při provádění Díla postupuje Zhotovitel samostatně, je však vázán příkazy Objednatele ohledně způsobu provádění Díla.

38. Zhotovitel se zavazuje brát v úvahu veškeré upozornění Objednatele, týkající se realizace Díla a upozorňující na možné porušování smluvních i právními předpisy stanovených povinností Zhotovitele.
39. Zhotovitel je povinen upozornit Objednatele bez zbytečného odkladu na nevhodnou povahu věci převzatých od Objednatele nebo příkazů daných mu Objednatelem k provedení Díla, jestliže Zhotovitel mohl tuto nevhodnost zjistit při vynaložení odborné péče.
40. Překáží-li nevhodná věc nebo příkaz v řádném provádění Díla, Zhotovitel je v nezbytném rozsahu přerušit až do výměny věci nebo změny příkazu; trvá-li Objednatel na provádění Díla s použitím předané věci nebo podle daného příkazu, má Zhotovitel právo požadovat, aby tak Objednatel učinil v písemné formě.
41. Doba stanovená pro dokončení Díla se prodlužuje o dobu vyvolanou přerušením dle předchozího odstavce.
42. Trvá-li Objednatel na provádění Díla s použitím předané věci nebo podle daného příkazu a zachová-li se Zhotovitel podle toho, nemá Objednatel práva z vady Díla vzniklé pro nevhodnost věci nebo příkazu.

Harmonogram

43. Je-li dle Rámcové dohody vyžadován Harmonogram provádění Díla, je Zhotovitel povinen jej předložit Objednateli bez zbytečného odkladu po uzavření Dílčí smlouvy, nejpozději však ke dni zahájení prací na provádění Díla.
44. Zhotovitel je povinen udržovat harmonogram v aktuálním stavu a v případě změny vždy předat Objednateli bezodkladně aktualizovaný harmonogram.

Kontrola provádění prací

45. Objednatel je oprávněn kontrolovat provádění Díla. Zjistí-li objednatel, že Zhotovitel provádí Dílo v rozporu s povinnostmi vyplývajícími z Dílčí smlouvy, Rámcové dohody, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů nebo příslušných ČSN, je Objednatel oprávněn dožadovat se toho, aby Zhotovitel odstranil vady vzniklé vadným prováděním a Dílo prováděl řádným způsobem. Jestliže tak Zhotovitel neučiní v přiměřené lhůtě, jedná se o podstatné porušení Rámcové dohody.
46. Zhotovitel je povinen písemně vyzvat Objednatele ke kontrole a prověření prací, které v dalším postupu budou zakryty nebo se stanou nepřístupnými. Zhotovitel je povinen vyzvat Objednatele nejméně 3 pracovní dny před termínem, v němž budou předmětné práce zakryty nebo zneprístupněny.
47. Před zakrytím nebo zneprístupněním prací je Zhotovitel povinen pořídit podrobnou fotodokumentaci prací a předat ji Objednateli v digitální podobě na CD nebo DVD nosiči bez zbytečného odkladu po pořízení fotodokumentace.
48. Pokud se Objednatel ke kontrole přes včasné písemné vyzvání nedostaví, je Zhotovitel oprávněn předmětné práce zakrýt. Bude-li se v tomto případě Objednatel dodatečně požadovat jejich odkrytí, je Zhotovitel povinen toto odkrytí provést na náklady Objednatele. Pokud se však zjistí, že práce nebyly řádně provedeny, nese veškeré náklady spojené s odkrytím prací, opravou chybného stavu a následným zakrytím Zhotovitel.
49. Obdobně bude-li Objednatel požadovat vykonání zvláštních zkoušek nebo ověření jakékoliv části Díla z důvodu podezření, že tato část Díla neodpovídá Dílčí smlouvě, Rámcové dohodě, Obchodním podmínkám, Veřejnoprávním podkladům, právním předpisům nebo příslušným ČSN, a bude-li zjištěno, že podezření bylo správné, nese náklady spojené s vykonáním zkoušek nebo ověřením Zhotovitel.
50. Zhotovitel je povinen umožnit výkon technického a autorského dozoru.

Kontrolní dny

51. Pro účely kontroly průběhu provádění Díla může Objednatel nebo jím pověřená osoba provést kontrolní dny v termínech nezbytných pro řádné provádění kontroly.
52. Kontrolních dnů se zúčastní zástupci Objednatele případně osob vykonávajících funkci technického dozoru a případně i autorského dozoru.
53. Zástupci Zhotovitele jsou povinni se kontrolních dnů zúčastňovat. Zhotovitel má právo přizvat na kontrolní den své poddodavatele podílející se v souladu s Rámcovou dohodou a Obchodními podmínkami na provádění Díla.
54. Kontrolní dny vede Objednatel nebo jím pověřená osoba.

55. Obsahem kontrolního dne je zejména zpráva Zhotovitele o postupu prací, kontrola postupu prací, připomínky a podněty osob vykonávajících funkci technického a autorského dozoru a stanovení případných nápravných opatření a úkolů.

56. Objednatel nebo jím pověřená osoba pořizuje z kontrolního dne zápis, který předá všem zúčastněným.

Dodržování zákazu požívání alkoholických nápojů a užívání jiných návykových látek

57. Objednatel je oprávněn provádět u všech osob, které Zhotovitel používá při provádění díla, kontrolu, zda tyto osoby nejsou pod vlivem alkoholu nebo návykové látky. Osoby Objednatele oprávněné k provádění této kontroly jsou určeny v souladu se směrnicí SŽDC č. 120 "Dodržování zákazu kouření, požívání alkoholických nápojů a užívání jiných návykových látek".

58. Zhotovitel seznámí své zaměstnance a osoby, které používá při provádění díla s povinností podrobit se kontrole prováděné Objednatelem.

59. Kontrola bude prováděna orientačním vyšetřením na zjištění přítomnosti alkoholu pomocí analyzátoru alkoholu v dechu (elektronický alkohol tester – kalibrovaný, detekční trubičky) a na zjištění jiné návykové látky pomocí drogových testů ze slin.

60. Kontrola bude prováděna dle směrnice SŽDC č. 120 "Dodržování zákazu kouření, požívání alkoholických nápojů a užívání jiných návykových látek".

61. Pozitivní výsledek ověření bude neprodleně oznámen Zhotoviteli (telefonicky, emailem).

62. Náklady na vyšetření v případě pozitivního výsledku uhradí Zhotovitel.

63. V případě pozitivního výsledku kontroly nesmí dotčená osoba Zhotovitele pokračovat ve vykonávané činnosti a bude jí odebrán „Průkaz ke vstupu do objektů a provozované železniční dopravní cesty SŽDC“.

64. V případě, že osoba, kterou Zhotovitel používá při provádění díla, se odmítne podrobit zjištění, zda není pod vlivem alkoholu nebo návykové látky, nebo je-li u této osoby dosaženo pozitivního výsledku kontroly, je Objednatel oprávněn na základě posouzení souvisejících okolností, uplatnit vůči Zhotoviteli sankci až do výše 100 000,- Kč za každý jednotlivý případ.

Dodržování podmínek stanovisek příslušných orgánů a organizací

65. Zhotovitel se zavazuje dodržet při provádění Díla veškeré podmínky vyplývající z Veřejnoprávních podkladů.

66. Pokud nesplněním těchto podmínek vznikne Objednateli škoda, je Zhotovitel povinen nahradit škodu v plném rozsahu, ledaže prokáže, že škodě nemohl zabránit ani v případě vynaložení veškeré možné péče, kterou na něm lze spravedlivě požadovat.

Použité materiály a výrobky

67. Zhotovitel se zavazuje a odpovídá za to, že při realizaci Díla nepoužije žádný materiál, o kterém je v době jeho užití známo, že je škodlivý. Pokud tak Zhotovitel učiní, je povinen na vyzvání Objednatele provést nápravu, přičemž veškeré náklady s tím spojené nese Zhotovitel.

68. Zhotovitel se zavazuje, že k realizaci Díla nepoužije materiály, které nemají požadovanou certifikaci či předepsaný průvodní doklad, je-li to pro jejich použití nezbytné podle Dílčí smlouvy, Rámcové dohody, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů nebo příslušných ČSN. Certifikace a průvodní doklady Zhotovitele použitých materiálů jsou součástí Dokladů.

Částečné plnění

69. Nabízí-li Zhotovitel Objednateli částečné plnění Předmětu Díla, aniž by částečné plnění bylo výslovně sjednáno v Dílčí smlouvě nebo Rámcové dohodě, není Objednatel povinen částečné plnění přijmout. Přijme-li Objednatel částečné plnění, je Zhotovitel povinen nahradit Objednateli zvýšené náklady způsobené mu částečným plněním.

Ostatní ujednání

70. Vícepráce lze provést a méněpráce neprovést až poté, co budou vícepráce nebo méněpráce dohodnuty včetně změn Ceny díla dodatkem k Dílčí smlouvě. Provede-li Zhotovitel vícepráce v rozporu s tímto odstavcem, ponese náklady na ně ze svého.

71. Dojde-li k jakémukoliv úrazu při provádění Díla nebo při činnostech souvisejících s prováděním Díla je Zhotovitel povinen zabezpečit vyšetření úrazu a sepsání příslušného záznamu. Objednatel je povinen poskytnout Zhotoviteli nezbytnou součinnost.

72. Žádný z podkladů, které Zhotovitel převzal od Objednatele v souvislosti s Dílem ani žádný Doklad není Zhotovitel oprávněn bez předchozího písemného svolení Objednatele užít k jiným účelům, než je provedení Díla, zejména je nesmí poskytnout třetím osobám.

73. Zhotovitel je povinen při provádění Díla postupovat v součinnosti s případnými jinými dodavateli Objednatele, a to dle pokynů udělených Objednatelem a nebudou-li pokyny uděleny, postupovat tak, aby umožnil ostatním dodavatelům v co největší míře plnit jejich závazky.
74. Objednatel se zavazuje poskytovat Zhotoviteli součinnost při provádění Díla v rozsahu a způsobem, ve kterém lze tuto součinnost po Objednateli spravedlivě požadovat. Bude-li Zhotovitelem požadována po Objednateli jakákoliv součinnost dle předchozí věty, je Zhotovitel povinen Objednatele k jejímu poskytnutí s dostatečným předstihem vyzvat a ve výzvě ji dostatečně specifikovat.
75. Zhotovitel na sebe přebírá nebezpečí změny okolností ve smyslu §1765 Občanského zákoníku.
76. Ustanovení §1912, §2595 Občanského zákoníku se neužijí.

ČÁST 9 - ZKUŠEBNÍ PROVOZ

77. Ustavení této části se užití v případě, že z Rámcové dohody nebo Dílčí smlouvy vyplývá, že má být proveden zkušební provoz.
78. Zkušebním provozem se prověřuje, zda Předmět díla je za předpokládaných provozních a výrobních podmínek schopen dosahovat výkonů (parametrů) v kvalitě a množství stanovených Rámcovou dohodou, Obchodními podmínkami, Veřejnoprávními podklady, právními předpisy a příslušnými ČSN.
79. Zkušební provoz je Zhotovitel povinen provést před předáním Díla Objednateli, do doby úspěšného provedení zkušebního provozu není Dílo dokončeno.
80. Zkušební provoz musí trvat minimálně 48 hodin, nestanoví-li Veřejnoprávní podklady, právní předpisy nebo příslušné ČSN jinak.
81. Zhotovitel se zavazuje v průběhu zkušebního provozu neprodleně odstraňovat veškeré vady, které bude Předmět díla vykazovat.
82. Zkušební provoz bude úspěšně proveden, nebude-li Předmět díla k poslednímu dni doby stanovené pro zkušební provoz vykazovat vady bránící jeho užívání.
83. Bude-li k poslednímu dni doby zkušebního provozu Předmět díla vykazovat vady bránící užívání, prodlužuje se délka trvání zkušebního provozu o dobu dle dohody Smluvních stran, jinak o 24 hodin.
84. Úspěšné provedení zkušebního provozu je podmínkou převzetí díla Objednatelem.

ČÁST 10 - PŘEPRAVA DÍLA

85. Ustavení této části se užití v případě, je-li Dílo po svém zhotovení za účelem předání Objednateli přepravováno.
86. Je-li dle Dílčí smlouvy, Rámcové dohody nebo zvyklostí třeba Předmět díla zabalit, Zhotovitel Předmět díla zabalí dle Dílčí smlouvy nebo Rámcové dohody; není-li ujednání o balení Předmětu díla v Dílčí smlouvě nebo v Rámcové dohodě, pak dle zvyklostí, a není-li jich, pak způsobem potřebným pro uchování Předmětu díla a jeho ochranu.
87. Jestliže Zhotovitel označí Obalový materiál nejpozději do doby převzetí Předmětu díla Objednatelem jako vratný, a to přímo na Obalovém materiálu, v Dokladech nebo jiným zřejmým způsobem, ze kterého bude zřejmé, který Obalový materiál je vratný, je Objednatel oprávněn předat Zhotoviteli při předávacím řízení (viz ČÁST 12 - Obchodních podmínek) stejné množství Obalového materiálu téhož druhu a srovnatelného nebo nižšího stupně opotřebení. V rozsahu předání Obalového materiálu Objednatelem Zhotoviteli dle předchozí věty zaniká právo Zhotovitele na vrácení Obalového materiálu.
88. V rozsahu, v němž Objednatel nevrátí vratný Obalový materiál Zhotoviteli dle předchozího odstavce, je Zhotovitel oprávněn Objednateli vyúčtovat zálohu na vratný Obalový materiál. Výše zálohy nesmí přesáhnout dvojnásobek pořizovací ceny Obalového materiálu.
89. Doposud nevrácený vratný Obalový materiál je Objednatel povinen na vlastní náklady dopravit do sídla Zhotovitele, a to nejpozději do jednoho roku od převzetí Předmětu díla Objednatelem. Objednatel je oprávněn nahradit nevrácený vratný Obalový materiál Obalovým materiálem stejného druhu a srovnatelného nebo nižšího stupně opotřebení. Bez zbytečného odkladu po

převzetí vráceného Obalového materiálu nebo jeho náhrady Zhotovitelem, je Zhotovitel povinen vrátit Objednateli zaplacenou zálohu na vratný Obalový materiál. Nevrátí-li Objednatel dosud nevrácený vratný Obalový materiál nebo Obalový materiál stejného druhu a srovnatelného nebo nižšího stupně opotřebení ani do dvou let od převzetí Předmětu díla Objednatelem, stává se nevrácený vratný Obalový materiál vlastnictvím Objednatele a složená záloha se stává vlastnictvím Zhotovitele.

90. Pokud Zhotovitel Předmět díla Objednateli odesílá prostřednictvím dopravce, umožní Zhotovitel Objednateli uplatnit práva z přepravní smlouvy vůči dopravci, pokud o to Objednatel Zhotovitele požádá.
91. Pokud Zhotovitel Předmět díla Objednateli odesílá prostřednictvím dopravce, je Zhotovitel povinen zajistit dopravu u dopravce tak, aby Předmět díla byl dodán Objednateli v době uvedené v odstavci 33 Obchodních podmínek.
92. Je-li třeba provést vyložení Předmětu díla z dopravního prostředku, je vyložení povinen provést Zhotovitel na své náklady.
93. Je-li Objednatel v prodlení s převzetím Předmětu díla, uchová jej Zhotovitel, může-li s ním nakládat, pro Objednatele způsobem přiměřeným okolnostem. Převzal-li Objednatel Předmět díla, který zamýšlí odmítnout, uchová jej způsobem přiměřeným okolnostem. Smluvní strana, která uchovává Předmět díla pro druhou Smluvní stranu, má právo na náhradu účelně vynaložených nákladů spojených s uchováním Předmětu díla, nemůže jej však za účelem zajištění svého práva na úhradu nákladů zadržet.

ČÁST 11 - PODDODAVATELÉ

94. Zhotovitel je oprávněn pověřit provedením části Díla třetí osobu – poddodavatele. Zhotovitel odpovídá za činnost poddodavatele tak, jako by činnost prováděl sám.
95. Zhotovitel je oprávněn pověřit provedením části Díla poddodavatele pouze, pokud je poddodavatel uveden v příloze Rámcové dohody.
96. Zhotovitel se zavazuje, že poddodavatelé splní všechny povinnosti vyplývající Zhotoviteli z Rámcové dohody, a to přiměřeně k povaze a rozsahu poddodávky.
97. Zhotovitel se zavazuje, že poddodavatelé, kterými prokazoval splnění kvalifikace v zadávacím řízení, se budou podílet na provedení příslušné věcně vymezené části Díla v rozsahu dle Nabídky Zhotovitele.
98. Zhotovitel je oprávněn změnit poddodavatele pouze s předchozím písemným souhlasem Objednatele a po uzavření dodatku k Rámcové dohodě. Objednatel vydá písemný souhlas formou zaslání návrhu dodatku do 10 dnů od doručení žádosti Zhotovitele a předložení všech potřebných dokumentů Zhotovitelem (zejména jde-li o poddodavatele nahrazujícího poddodavatele, jímž bylo prokazováno splnění kvalifikace). Objednatel souhlas se změnou nevydává, pokud
 - 98.1. prostřednictvím původního poddodavatele Zhotovitel v zadávacím řízení prokazoval kvalifikaci a nový poddodavatel nebude mít stejnou či vyšší kvalifikaci jako původní nahrazovaný poddodavatel nebo
 - 98.2. po Objednateli nelze spravedlivě požadovat, aby s takovou změnou souhlasil.

ČÁST 12 - PŘEDÁNÍ A PŘEVZETÍ DÍLA

99. Závazek Zhotovitele provést Dílo je splněn jeho dokončením a převzetím Díla Objednatelem, včetně převzetí veškerých Dokladů.
100. Součástí Dokladů je dle povahy a charakteru Díla též
 - 100.1. dodavatelská výrobní a dílenská dokumentace,
 - 100.2. atesty, záruční listy, prohlášení o shodě všech věcí, jež byly použity při provádění Díla,
 - 100.3. zápisy a osvědčení o všech předepsaných zkouškách, měřeních,
 - 100.4. dokumenty osvědčující průběh zkušebního provozu,
 - 100.5. servisní plán, návod k obsluze a návod k použití částí Díla,
 - 100.6. doklady o zabezpečení likvidace odpadů v souladu s právními předpisy,

- 100.7. fotodokumentace z průběhu provádění Díla, zejména fotodokumentace prací a konstrukcí, které byly dalším postupem prací zakryté nebo jinak zneprístupněné.
101. V případě, že Dílčí smlouva, Rámcová dohoda, Obchodní podmínky, Veřejnoprávní podklady, právní předpisy nebo příslušné ČSN předepisují provedení zkoušek, revizí, atestů a měření či zajištění prohlášení o shodě týkajících se Díla, je Zhotovitel povinen zajistit jejich úspěšné provedení před předáním Díla Objednateli.
102. Objednatel Dílo převezme za předpokladu, že provedení Díla odpovídá Dílčí smlouvě, Rámcové dohodě, Obchodním podmínkám, Veřejnoprávním podkladům, právním předpisům a příslušným ČSN, je dokončeno (plně funkční), a je prosté vad s výjimkou ojedinělých drobných vad, které samy o sobě ani ve spojení s jinými nebrání užívání Díla funkčně nebo esteticky, ani jeho užívání podstatným způsobem neomezují.
103. Splnění podmínek pro předání Díla bude ověřeno v rámci přejímacího řízení. Zhotovitel je povinen písemně vyzvat Objednatele k převzetí Díla (zahájení přejímacího řízení). Přejímací řízení bude Objednatel zahájeno do 5 pracovních dnů po obdržení písemné výzvy Zhotovitele.
104. Objednatel je oprávněn přizvat k účasti v přejímacím řízení i jiné osoby, jejichž účast pokládá za nezbytnou.
105. O průběhu přejímacího řízení bude Zhotovitelem pořízen zápis s identifikací vad Díla, pokud budou v průběhu přejímacího řízení zjištěny. Zápis bude použit jako podklad pro zpracování Předávacího protokolu. Zpracování návrhu Předávacího protokolu zajistí Zhotovitel.
106. Předávací protokol obsahuje
- 106.1. výslovný souhlas Objednatele s převzetím Díla
 - 106.2. datum převzetí Díla,
 - 106.3. prohlášení Objednatele, zda přebírá Dílo bez výhrad, nebo s výhradami,
 - 106.4. soupis zjištěných vad nebránících řádnému užívání Díla,
 - 106.5. dohodnuté lhůty k odstranění zjištěných vad nebo jiná opatření (byla-li dohodnuta),
 - 106.6. soupis Dokladů předaných Zhotovitelem Objednateli.
107. Objednatel převezme Dílo bez výhrad, je-li v předávacím řízení zjištěno, že Dílo je prosté vad.
108. Převezme-li Objednatel Dílo s výhradami, postupují Smluvní strany dále obdobně dle ustanovení odstavců 137 - 151 Obchodních podmínek, přičemž pro odstranění vad platí doba sjednaná v Předávacím protokolu, jinak doba 15 dní od oboustranného podpisu Předávacího protokolu a za reklamaci se považuje identifikace vad uvedená v Předávacím protokolu podepsaném Objednatel.
109. V případě, že Objednatel Dílo nepřevzme, bude mezi Smluvními stranami sepsán záznam s uvedením důvodu nepřevzetí Díla a s uvedením stanovisek Smluvních stran. Zpracování záznamu zajistí Zhotovitel.
110. V případě nepřevzetí Díla Smluvní strany sjednají lhůtu pro odstranění zjištěných vad. Nebude-li vada odstraněna ve lhůtě sjednané, jinak do 15 dní, je Objednatel oprávněn zajistit odstranění vady jinou odborně způsobilou osobou na náklady Zhotovitele. Veškeré náklady vzniklé Objednateli v souvislosti s odstraněním vady způsobem dle předchozí věty je Zhotovitel povinen Objednateli uhradit. Zhotovitel je povinen ve stanovené lhůtě odstranit vady i v případě, kdy podle jeho názoru za vady neodpovídá. Náklady na odstranění v těchto sporných případech nese až do vyjasnění nebo do vyřešení rozporu Zhotovitel. Po odstranění vad vyzve Zhotovitel Objednatele k zahájení náhradního přejímacího řízení, které Objednatel zahájí bezodkladně, nejpozději do 2 pracovních dnů od obdržení výzvy Zhotovitele.
111. Podpisem Předávacího protokolu nebo záznamu o nepřevzetí Díla je přejímací řízení ukončeno.
112. Pro průběh náhradního přejímacího řízení se užití ustanovení odstavců 102 - 111 Obchodních podmínek obdobně.
113. Připouští-li to povaha Předmětu díla, a není-li sjednán zkušební provoz, má Objednatel právo, aby byl Předmět díla před ním překontrolován nebo aby byly předvedeny jeho funkce.
114. Ustanovení §1921, §2112, §2605 odst. 2, §2606, §2609, §2618 a §2629 Občanského zákoníku se neuplatní.

ČÁST 13 - VLASTNICKÉ PRÁVO A NEBEZPEČÍ ŠKODY

115. Vlastnické právo k Dílu náleží od počátku Objednateli.

116. Vlastnické právo k dodávkám materiálu a jiných hmotných movitých věcí nabývá Objednatel okamžikem jejich zapracování do Díla, učiněním součástí Díla nebo jakýmkoliv funkčním, estetickým či jiným spojením s Dílem.
117. Vlastnické právo k jakékoli dokumentaci vztahující se k Dílu, která není autorským dílem, nabývá Objednatel okamžikem jejího vyhotovení.
118. Je-li vlastníkem Díla nebo jeho části v souladu s §1083 a §1084 Občanského zákoníku vlastník pozemku, užijí se ustanovení odstavců 115 a 116 přiměřeně.
119. Nebezpečí škody na Díle nese Zhotovitel, na Objednatele přechází okamžikem oboustranného podpisu Předávacího protokolu. Pokud nebyly s Předmětem díla předány zároveň též všechny Doklady, nese Zhotovitel nebezpečí škody na dosud nepředaných Dokladech až do jejich převzetí Objednatelem.
120. Náklady nutné k odstranění škody na Díle vzniklé v době, kdy nebezpečí škody nese Zhotovitele, hradí Zhotovitel v plném rozsahu a tyto náklady nemají vliv na Cenu díla.
121. Škody na Díle vzniklé v době, kdy nebezpečí škody nese Zhotovitele, je povinen Zhotovitel odstranit v součinnosti s Objednatelem jako vlastníkem poškozené věci a dle jeho pokynů.
122. Ustanovení §2599 Občanského zákoníku se neužijí.

ČÁST 14 - VADY PLNĚNÍ A ZÁRUKA

123. Zhotovitel se zavazuje, že Dílo bude v okamžiku jeho převzetí Objednatelem vyhovovat všem požadavkům na dílo stanoveným Rámcovou dohodou, Obchodními podmínkami, Veřejnoprávními podklady, právními předpisy a příslušnými ČSN.
124. Zhotovitel se zavazuje, že Dílo bude vyhovovat též plnění nabídnutému Zhotovitelem v Nabídce.
125. Dílo musí být prosté všech faktických a právních vad. Plnění má právní vadu, pokud k němu uplatňuje právo třetí osoba.
126. Zhotovitel se zavazuje (poskytuje Objednateli záruku), že Dílo a veškeré jeho části si po celou dobu od okamžiku jeho převzetí Objednatelem, až do uplynutí Záruční doby zachová vlastnosti stanovené v odstavcích 123 - 125 Obchodních podmínek.
127. Záruční doba začíná běžet dnem převzetí Díla Objednatelem, nebo jeho poslední části, je-li Dílo dodáváno po částech, nebo ode dne úspěšného ukončení zkušebního provozu, je-li dle Rámcové dohody vyžadován a nastane-li okamžik úspěšného ukončení zkušebního provozu později než okamžik převzetí Díla, resp. jeho poslední části.
128. Dílo má vady (Zhotovitel plnil vadně), jestliže při převzetí Objednatelem nebo kdykoliv od převzetí Objednatelem do konce Záruční doby nebude mít vlastnosti stanovené v odstavcích 123 - 125 Obchodních podmínek.
129. Objednatel má práva z vadného plnění i v případě, jedná-li se o vadu, kterou musel s vynaložením obvyklé pozornosti poznat již při uzavření Dílčí smlouvy.
130. Objednatel nemá práva z vadného plnění, způsobila-li vadu po přechodu nebezpečí škody na věci na Objednatele vnější událost. To neplatí, způsobil-li vadu Zhotovitel nebo jakákoliv třetí osoba, jejímž prostřednictvím plnil své povinnosti vyplývající z Dílčí smlouvy.
131. Zhotovitel neodpovídá za vady spočívající v opotřebení Předmětu díla, které je obvyklé u věci stejného nebo obdobného druhu jako Předmět díla.
132. Zhotovitel odpovídá za vady spočívající v opotřebení Předmětu díla, ke kterému do konce Záruční doby vzhledem k požadavkům Dílčí smlouvy, Rámcové dohody, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů a příslušných ČSN na jakost a provedení Předmětu díla nemělo dojít.
133. Zhotovitel nenese odpovědnost za vady způsobené Objednatelem nebo třetími osobami, ledaže Objednatel nebo takové osoby postupovaly v souladu s Doklady nebo pokyny, které obdrželi od Zhotovitele.

ČÁST 15 - UPLATNĚNÍ PRÁV Z VADNÉHO PLNĚNÍ

134. Odpovídá-li Zhotovitel za vady Díla, má Objednatel práva z vadného plnění.

135. Objednatel je oprávněn vady reklamovat u Zhotovitele jakýmkoliv způsobem, preferovaná je písemná forma. Zhotovitel je povinen přijetí reklamace bez zbytečného odkladu písemně potvrdit. V reklamaci Objednatel uvede popis vady nebo uvede, jak se vada projevuje.
136. Vada je uplatněna včas, je-li písemná forma reklamace odeslána Zhotoviteli nejpozději v poslední den Záruční doby. Případně-li konec Záruční doby na sobotu, neděli nebo svátek, je vada včas uplatněna, je-li písemná forma reklamace odeslána Zhotoviteli nejbližší následující pracovní den.
137. Má-li Předmět díla vady, za které Zhotovitel odpovídá, má Objednatel právo
 - 137.1. na odstranění vady dodáním nového Předmětu díla nebo jeho části bez vady, pokud to není vzhledem k povaze vady zcela zřejmě nepřiměřené, nebo dodání chybějící části Předmětu díla,
 - 137.2. na odstranění vady opravou Předmětu díla nebo jeho části,
 - 137.3. na přiměřenou slevu z Ceny díla, nebo
 - 137.4. odstoupit od Dílčí smlouvy.
138. Objednatel je oprávněn požadovat odstranění vad dodáním nového Předmětu díla nebo jeho části bez vady, vyskytla-li se stejná vada po její opravě opětovně, nebo nemůže-li Objednatel řádně užívat Předmět díla nebo jeho část pro větší počet vad.
139. Objednatel je oprávněn nároky dle odstavce 137 kombinovat, je-li to vzhledem k okolnostem možné. Objednatel není oprávněn kombinovat nároky, které si navzájem odporují (např. dodání nové části Předmětu díla a zároveň slevy z Ceny díla na tutéž část Předmětu díla).
140. Objednatel sdělí Zhotoviteli volbu nároku z vady v reklamaci, nebo bez zbytečného odkladu po reklamaci. Provedenou volbu nemůže Objednatel změnit bez souhlasu Zhotovitele; to neplatí, žádal-li Objednatel opravu vady, která se ukáže jako neopravitelná.
141. Nesdělí-li Objednatel Zhotoviteli, jaké právo si zvolil ani bez zbytečného odkladu poté, co jej k tomu Zhotovitel vyzval, může Zhotovitel odstranit vady podle své volby opravou nebo dodáním nového Předmětu díla nebo jeho části; volba nesmí Objednateli způsobit nepřiměřené náklady.
142. Objednatel má nárok na náhradu nákladů účelně vynaložených v souvislosti s oznámením vad Zhotoviteli.

ČÁST 16 - PODMÍNKY ODSTRANĚNÍ VAD

143. Pokud Objednatel požaduje v reklamaci odstranění vady, je Zhotovitel povinen neprodleně po obdržení reklamace zahájit činnosti vedoucí k odstranění reklamované vady. Pokud Objednatel v reklamaci uvede, že se jedná o havárii, je Zhotovitel povinen zahájit odstraňování vady nejpozději do 48 hodin po obdržení reklamace.
144. Zhotovitel je povinen odstranit Objednatelem reklamovanou vadu nejpozději do 30 dnů ode dne oznámení vady Zhotoviteli. Jde-li o vadu označenou Objednatelem v reklamaci jako havarijní, je Zhotovitel povinen odstranit vadu nejpozději do 5 dnů.
145. Nezahájí-li Zhotovitel činnosti vedoucí k odstranění vady do 10 dnů od oznámení vady Zhotoviteli, nebo nebude-li vada odstraněna ve lhůtě dle předcházejícího odstavce, je Objednatel oprávněn
 - 145.1. zajistit odstranění vady jinou odborně způsobilou právnickou nebo fyzickou osobou na účet Zhotovitele,
 - 145.2. požadovat slevu z Ceny díla, nebo
 - 145.3. od Rámcové dohody odstoupit.
146. Veškeré náklady vzniklé Objednateli v souvislosti s odstranění vady způsobem dle předchozího odstavce je Zhotovitel povinen Objednateli uhradit.
147. Zhotovitel je povinen odstranit vadu bez ohledu na to, zda je uplatnění vady oprávněné či nikoli. Prokáže-li se však kdykoli později, že uplatnění vady Objednatelem nebylo oprávněné, tj. že Zhotovitel za vadu neodpovídal, je Objednatel povinen uhradit Zhotoviteli veškeré jím účelně vynaložené náklady v souvislosti s odstraněním vady.
148. Objednatel je povinen poskytnout Zhotoviteli součinnost nezbytnou k odstranění vady.
149. Do odstranění vady nemusí Objednatel platit dosud nezaplacenou část Ceny díla a případnou příslušnou DPH odhadem přiměřeně odpovídající jeho právu na slevu.

150. Při dodání nového Předmětu díla nebo jeho části vrátí Objednatel Zhotoviteli na náklady Zhotovitele Předmět díla nebo jeho část původně dodanou.
151. Týká-li se vada Dokladů nebo jiného plnění poskytnutého Zhotovitelem dle Rámcové dohody, než Předmětu díla, užití se ustanovení odstavců 134 – 150 obdobně.
152. Ustanovení §1917 – 1924, §2099 – 2101, §2103 – 2117, §2165 – 2172, §2618 a §2629 Občanského zákoníku se neužijí.

ČÁST 17 - POJIŠTĚNÍ

153. Ustanovení této části se užití v případě, že z Rámcové dohody vyplývá, že Zhotovitel je povinen být pojištěn pro případ odpovědnosti za škodu způsobenou při výkonu činnosti.
154. Zhotovitel je povinen mít ode dne zahájení provádění Díla, až do řádného dokončení Díla uzavřeno pojištění v rozsahu uvedeném v Rámcové dohodě.
155. Zhotovitel je povinen předložit Objednateli uzavřenou pojistnou smlouvu nebo odpovídající pojistku v rozsahu uvedeném v Rámcové dohodě, nejpozději však v den zahájení prací na Díle a dále kdykoli v průběhu provádění Díla do 10 dnů ode dne, kdy k tomu byl Objednatel vyzván. V případě změn v pojištění je Zhotovitel povinen bezodkladně tyto změny oznámit Objednateli a předložit dokumenty dokládající tyto změny.
156. Zhotovitel se zavazuje, že všichni poddodavatelé, kteří se budou podílet na provedení Díla, budou nejméně po dobu provádění poddodávky pojištěni pro případ škody způsobené poddodavatelem při výkonu činnosti třetím osobám s limitem pojistného plnění pro 1 pojistnou událost minimálně ve výši odpovídající ceně poddodávky.
157. Porušení jakékoli povinnosti Zhotovitele dle této části je podstatným porušením Dílčí smlouvy a Rámcové dohody.
158. Náklady na pojištění nese Zhotovitel, jsou zahrnuty v Ceně díla.

ČÁST 18 - DUŠEVNÍ VLASTNICTVÍ

159. Zhotovitel je povinen při provádění Díla postupovat tak, aby při provádění Díla ani následným užíváním Díla Objednatel nedošlo k porušení práv duševního vlastnictví. Bude-li v souvislosti s Dílem jakkoliv dotčeno právo k duševnímu vlastnictví, je Zhotovitel povinen upravit veškeré právní vztahy s osobami, kterým taková práva náležejí nebo jež jsou oprávněny je vykonávat, tak, aby zamezil vznášení jakýchkoli oprávněných nároků těchto osob ve vztahu k Objednateli.
160. Zhotovitel tímto poskytuje Objednateli oprávnění k výkonu práva duševního vlastnictví (licenci nebo podlicenci) ke všem plněním poskytnutým Objednateli při provádění Díla, které jsou nebo budou předmětem duševního vlastnictví a ke kterým je oprávněn takové oprávnění poskytnout. Oprávnění Zhotovitel poskytuje
 - 160.1. bezúplatně,
 - 160.2. jako nevýhradní,
 - 160.3. z hlediska časového a územního v rozsahu neomezeném,
 - 160.4. z hlediska věcného rozsahu (způsobu užití) tak, že opravňuje Objednatele ke všem známým způsobům užití,
 - 160.5. bez množstevního omezení.
161. Objednatel není povinen oprávnění využít.
162. Objednatel je oprávněn oprávnění tvořící součást licence nebo podlicence poskytnout nebo též postoupit třetí osobě zcela nebo zčásti.
163. Zhotovitel se zavazuje, že na žádost Objednatele autor nebo autoři autorského díla, jež je součástí nebo příslušenstvím Díla, udělí Objednateli bez zbytečného odkladu bezúplatně právo
 - 163.1. upravit či jinak změnit označení autora,
 - 163.2. autorské dílo nebo jeho název upravit či jinak měnit,
 - 163.3. autorské dílo s jakýmkoliv jiným autorským dílem spojit či zařadit do díla souborného.
164. Žádný výsledek činnosti provedené na základě Rámcové dohody nebo v souvislosti s ní, který je předmětem duševního vlastnictví, není Zhotovitel oprávněn bez předchozího písemného

svolení Objednatele užít k jiným účelům, než je provedení Díla, zejména je nesmí poskytnout třetím osobám.

ČÁST 19 - SANKCE

165. Uplatněním smluvní pokuty není dotčeno právo druhé Smluvní strany na náhradu škody v plné výši.
166. Uplatněním nároku na zaplacení smluvní pokuty ani jejím uhrazením nezaniká povinnost Smluvní strany splnit utvrzenou povinnost.
167. Dopadají-li na jedno skutkově stejnorodé porušení povinnosti dvě a více ustanovení o smluvní pokutě, uplatní se pouze jedna smluvní pokuta, a to ta, která je v nejvyšší částce. Není vyloučen souběh smluvní pokuty za porušení smluvní povinnosti a smluvní pokuty za prodlení s odstraněním následku téže smluvní povinnosti, jelikož se nejedná o skutkově stejnorodé porušení smluvní povinnosti.
168. Smluvní pokuty se uplatňují bez DPH. Je-li základem pro výpočet smluvních pokut Cena Díla či její část, je rozhodná Cena Díla či její část bez DPH stanovená k okamžiku uzavření Dílčí smlouvy; k případným jejím následným úpravám po uzavření Dílčí smlouvy se nepřihlíží.
169. Smluvní pokuta je splatná do třiceti (30) dnů ode dne vystavení daňového dokladu – sankční faktury. Je-li povinná Smluvní strana v prodlení s uhrazením smluvní pokuty, musí uhradit druhé Smluvní straně zákonný úrok z prodlení z dlužné částky smluvní pokuty za každý započatý den prodlení.
170. V případě porušení smluvní povinnosti týkající se neposkytnutí finanční záruky a pojistných smluv nebo jejich neudržování v platnosti nebo účasti poddodavatelů anebo realizačního týmu, které je možné jednáním Zhotovitele do patnácti (15) kalendářních dnů napravit, bude zhotovitel bezodkladně písemně vyzván ke zjednání nápravy v dodatečně lhůtě patnácti (15) kalendářních dnů ode dne doručení výzvy. V případě, že Zhotovitel zjedná nápravu ve stanovené lhůtě, nárok Objednatele na smluvní pokutu nevznikne. V případě marného uplynutí této lhůty vzniká nárok na smluvní pokutu ode dne porušení smluvní povinnosti.
171. Maximální celková výše všech uplatněných smluvních pokut v důsledku porušení Dílčí smlouvy Zhotovitelem je stanovena ve výši 40 % Ceny Díla. Limit dle předchozí věty činí maximálně 30 % Ceny Díla do okamžiku podpisu protokolu o provedení/předání Díla tak, aby na dobu platnosti finanční záruky za odstranění vad připadalo minimálně 10 % Ceny Díla.
172. Dosažení maximální celkové výše veškerých uplatněných smluvních pokut podle předchozího odstavce představuje podstatné porušení Dílčí smlouvy a Rámcové dohody, na základě, kterého je Objednatel oprávněn odstoupit od Dílčí smlouvy a Rámcové dohody.
173. Objednatel je ze zákona povinen uplatnit a vymáhat veškeré smluvní pokuty, na které mu vznikl nárok, a to v plné výši bez možnosti její úpravy.
174. Poruší-li Zhotovitel povinnost provést Dílo, nebo jeho část ve sjednané době, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 0,2 % z Ceny Díla, nebo ceny části Díla, - je-li Dílo dle Dílčí smlouvy prováděno po částech, za každý den prodlení minimálně však 5.000,- Kč za každý započatý den prodlení.
175. Poruší-li Zhotovitel povinnost odstranit vadu Díla, nebo jeho části ve sjednané době, je povinen uhradit Objednateli smluvní pokutu ve výši 0,1 % z Ceny Díla za každý započatý den prodlení až do odstranění vady, minimálně však 5.000,- Kč za každý započatý den prodlení. Jde-li o vadu, kterou Objednatel označil v reklamaci jako havárii, je Zhotovitel povinen uhradit smluvní pokutu ve dvojnásobné výši. Maximální denní výše smluvní pokuty dle tohoto odstavce činí, a to vždy ve vztahu k jednotlivé smluvní pokutě odpovídající Ceně Díla nebo ceně příslušné části Díla, v případě Ceny za plnění Dílčí smlouvy:
 - 175.1. do 10 mil. Kč částku 10 000 Kč,
 - 175.2. do 100 mil. Kč částku 50 000 Kč,
 - 175.3. do 1 mld. Kč částku 100 000 Kč a
 - 175.4. nad 1 mld. Kč částku 200 000 Kč.
176. V případě, že Zhotovitel pověřil prováděním Díla jiného poddodavatele než toho, který byl uveden v příloze Rámcové dohody, bez předchozího písemného souhlasu Objednatele postupem dle části 11 těchto Obchodních podmínek, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 1 % Ceny Díla za každý takový případ.

177. Poruší-li Zhotovitel povinnost provádět vyhrazené významné činnosti přímo Zhotovitelem, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 10 % z Ceny Díla za každý takový případ.
178. V případě, že Zhotovitel nesplní svoji povinnost stanovenou Rámcovou dohodou či Dílčí smlouvou předložit pojistné smlouvy nebo povinnost udržovat po celou dobu provádění Díla v platnosti Objednatelům vyžadované pojistné smlouvy, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 0,05 % z Ceny Díla za každý započatý den neplnění této povinnosti, maximálně však ve výši 40.000,- Kč za každý započatý den prodlení.
179. V případě, že Zhotovitel nesplní svoji povinnost poskytnout Objednateli finanční záruku za odstranění vad Díla nebo udržovat tuto finanční záruku v platnosti v rozsahu vyžadovaném Dílčí smlouvou, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 0,5 % z hodnoty finanční záruky za každý den neplnění této povinnosti, maximálně však ve výši 20.000 Kč za každý započatý den prodlení.
180. V případě, že Zhotovitel poruší plán BOZP, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 1 % z Ceny Díla, maximálně však ve výši 1 % z Ceny Díla za každý takový případ.
181. Poruší-li Zhotovitel povinnost nepostoupit žádnou svou pohledávku za Objednatelům vyplývající z Rámcové dohody a/nebo poruší zákaz zřídit zástavní právo k pohledávce, byť by takové postoupení a/nebo zřízení zástavního práva bylo neplatné či neúčinné, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 20% z nominální hodnoty postoupené a/nebo zastavené pohledávky, včetně hodnoty případného příslušenství ke dni účinnosti postoupení vůči postupníkovi, minimálně však 5.000,- Kč v celkové výši.
182. Pokud bude nutné Dílo dle Dílčí smlouvy provádět během výluk, platí následující podmínky a sankce:

182.1. Překročená výluka je výluka nad rámec výluk uvedených v harmonogramu prací nebo vydanému rozkazu o výluce (ROV) nebo obojímu, ke které dojde nikoliv z viny Objednatelů a ke které dojde překročením sjednaného výlukového času o více než 1 hodinu. V případech, kdy je již vydán ROV, je překročení výluky uvažováno a počítáno ve vztahu k již vydanému ROV. Částka, kterou se Zhotovitel zavazuje za překročenou výluku Objednateli uhradit, bude počítána za každou započatou hodinu výluky nad výše uvedený rámec. Jedná se o poskytnutí služby ve smyslu zákona o dani z přidané hodnoty. V případě výluky překročené o méně než 1 hodinu se předchozí věta neuplatní. V případě výluky překročené o více než 1 hodinu se Zhotovitel zavazuje uhradit veškerý překročený čas výluky, a to včetně první započaté hodiny. Pro vyloučení pochybností se sjednává, že za výluku se v rámci výše uvedeného považuje i každá samostatná etapa výluky v ROV. Níže uvedené částky za každou započatou hodinu jsou uvedeny včetně platné sazby DPH.

výluka trakčního vedení traťové koleje	3.000 Kč/ započatá hodina
výluka traťové koleje	5.000 Kč/ započatá hodina
výluka dvou a více traťových kolejí	10.000 Kč/ započatá hodina
výluka staničních kolejí – dopravní	2.000 Kč/ započatá hodina
výluka ostatních kolejí	1.000 Kč/ započatá hodina
výluka zabezpečovacího zařízení	3.000 Kč/započatá hodina

Výše uvedenému zpoplatnění nepodléhá prodloužení výluk nemající vliv na jízdu vlaků dopravce.

182.2. Zhotovitel se zavazuje zároveň uhradit (i při překročení výluky o méně než 1 hodinu):

- smluvní pokutu za překročení plánovaného času ukončení výluky mající vliv na vlaky dopravců přímo dotčených překročenou výlukou, požadovanou dopravci po Objednateli ve výši stanovené v Prohlášení o dráze,

- veškerou škodu či nemajetkovou újmu a účelně vynaložené náklady vzniklé Objednateli, nebo které vůči Objednateli uplatnili dopravci (v osobní i nákladní dopravě a nasazení lokomotiv nezávislé trakce, včetně případného nasazení náhradní autobusové dopravy) či jiné třetí osoby a které vzniknou v souvislosti s překročenou výlukou.

182.3. Za překročenou výluku se nepovažuje výluka, která byla pozdě zahájena z důvodu na straně řízení Objednatelů, a přitom byl celkový čas výluky dodržen.

- 182.4. Časové prodloužení výluky (o kolik bude překročena a kdy byla hlášena před ukončením výluky) musí být zapsáno a výpravčím potvrzeno v telefonním zápisníku příslušné stanice.
- 182.5. Zhotovitel není povinen hradit platby za překročené výluky, prokáže-li, že ke vzniku těchto překročených výluk došlo vinou na straně Objednatele nebo k překročené výluce vedly:
- zásahy vyšší moci,
 - pokyny Objednatele či stavebního dozoru,
 - jiné nepředvídatelné okolnosti, zejména změny během výstavby a potřeba jejich provedení. Za takové okolnosti se nepovažují rozpory mezi projektovou dokumentací a skutečností zjištěnou na místě, které mohly být identifikovány při přípravě na realizaci zakázky.
- 182.6. V případě, že z důvodu vady Díla nebo jeho části, za kterou odpovídá Zhotovitel, bude nutno v průběhu záruční doby za jakost Díla nebo jeho části zavést pomalou jízdu, je Objednatel oprávněn po Zhotoviteli požadovat zaplacení smluvní pokuty ve výši 5.000,- Kč za každý den trvání pomalé jízdy. Zhotovitel se rovněž zavazuje zaplatit smluvní pokutu ve výši 5.000,- Kč za každé snížení rychlosti o každých 10 km/hod oproti rychlosti předpokládané projektem stavby.
- 182.7. V případě, že Zhotovitel nezajistí realizaci prací tak, aby probíhaly maximálně v deklarované výluce (výluky kratší než 36 hodin) Objednatele, je Objednatel oprávněn po Zhotoviteli požadovat zaplacení smluvní pokuty ve výši 0,5% z Ceny Díla/dílčího plnění za každou neodpracovanou hodinu z potvrzené výluky.
- V případě, že Zhotovitel nezajistí realizaci prací tak, aby v případě nepřetržitých výluk trvajících více než 36 hodin, práce probíhaly minimálně 16 hodin denně včetně sobot a nedělí, je Objednatel oprávněn po Zhotoviteli požadovat zaplacení smluvní pokuty ve výši 0,5% z Ceny díla za každý takový případ nevyužitého dne. Zhotovitel nebude požadovat zálohy ani žádné jiné platby během provádění díla.

ČÁST 20 - OBECNÁ ODPOVĚDNOST ZHOTOVITELE

183. Zhotovitel je povinen po dobu plnění povinností z Rámcové dohody chránit majetek Objednatele i třetích osob před jeho poškozením, znehodnocením, zničením a ztrátou a postupovat tak, aby neomezoval práva osob nad míru nezbytnou k provádění Díla.
184. Způsobí-li Zhotovitel v souvislosti s Dílem nebo porušením svých povinností vyplývajících z Dílčí smlouvy, Rámcové dohody, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů a příslušných ČSN jakoukoli újmu Objednateli nebo třetím osobám, je povinen nahradit Objednateli škodu a nemajetkovou újmu, včetně případných sankcí udělených Objednateli orgány státní správy, jejichž příčinou bylo porušení smluvních povinností Zhotovitele, a jde-li o újmu způsobenou třetím osobám, je povinen způsobenou újmu na vlastní náklady bezodkladně odčinit.
185. Újmou se pro účely Obchodních podmínek rozumí zejm. jakékoliv poškození, znehodnocení, či znečištění věcí nebo prostor nebo jejich jiná nežádoucí změna a jakékoliv neoprávněné omezení práv Objednatele nebo třetích osob.
186. Zhotovitel odpovídá za jakékoliv porušení svých povinností stanovených Dílčí smlouvou, Rámcovou dohodou, Obchodními podmínkami, Veřejnoprávními podklady, právními předpisy a příslušnými ČSN a je povinen uhradit veškeré pokuty udělené mu příslušnými orgány státní správy v souvislosti s prováděním Díla ze svého, ledaže mu byla pokuta udělena v souvislosti s respektováním příkazu Objednatele, proti kterému uplatnil písemnou výhradu a na jehož splnění Objednatel trval anebo v souvislosti s užitím Objednatelem opatřené věci, na jejíž nevhodnost Objednatele písemně upozornil a Objednatel na jejím užití trval.
187. Povinnosti k náhradě újmy způsobené porušením svých povinností z \dílčí smlouvy, Rámcové dohody, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů a příslušných ČSN se Zhotovitel vůči Objednateli zproští, prokáže-li, že mu ve splnění povinnosti zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli. Překážka vzniklá z osobních poměrů Zhotovitele nebo vzniklá až v době, kdy byl Zhotovitel

s plněním povinnosti v prodlení, ani překážka, kterou byl Zhotovitel povinen překonat, jej však povinnosti k náhradě nezprostí.

ČÁST 21 - Odstoupení od dílčí smlouvy a rámcové dohody

188. Poruší-li Smluvní strana Dílčí smlouvu nebo Rámcovou dohodu podstatným způsobem, může druhá Smluvní strana písemnou formou od Dílčí smlouvy a současně i od Rámcové dohody odstoupit. Pokud je Smluvní strana oprávněna odstoupit od Dílčí smlouvy, může vždy současně s odstoupením od Dílčí smlouvy jako celku odstoupit i od Rámcové dohody.
189. Podstatné je takové porušení povinnosti, o němž Smluvní strana porušující Dílčí smlouvu nebo Rámcovou dohodu již při uzavření Rámcové dohody věděla nebo musela vědět, že by druhá Smluvní strana Dílčí smlouvu nebo Rámcovou dohodu neuzavřela, pokud by toto porušení předvídala, nebo je-li porušení povinnosti v Dílčí smlouvě, Rámcové dohodě nebo v Obchodních podmínkách jako podstatné označeno; v ostatních případech se má za to, že porušení podstatné není.
190. Podstatným porušením Dílčí smlouvy je též prodlení Zhotovitele a Objednatele s plněním povinností vyplývajících Zhotoviteli a Objednateli z Dílčí smlouvy o více než 30 dní.
191. Objednatel je oprávněn od Dílčí smlouvy odstoupit též
 - 191.1. z důvodů uvedených v části Předání a převzetí Díla (viz ČÁST 12 - Obchodních podmínek),
 - 191.2. nabylo-li právní moci rozhodnutí o nařízení exekuce vůči Zhotoviteli jako povinnému,
 - 191.3. ocitne-li se Zhotovitel ve stavu úpadku nebo hrozícího úpadku,
 - 191.4. jestliže Zhotovitel nebo jeho poddodavatel, nebo z jejich pokynu jakákoliv osoba, nabídne nebo poskytne jakékoliv osobě úplatek nebo jiný majetkový či jiný prospěch za účelem získání neoprávněného prospěchu nebo výhody v souvislosti s Dílem nebo jeho prováděním,
 - 191.5. uvedl-li Zhotovitel v Nabídce informace nebo doklady, které neodpovídají skutečnosti a měly nebo mohly mít vliv na výsledek řízení,
 - 191.6. stanoví-li tak Rámcová dohoda.
192. Smluvní strana může od Dílčí smlouvy odstoupit, pokud z chování druhé Smluvní strany nepochybně vyplývá, že poruší Dílčí smlouvu podstatným způsobem, a nedá-li na výzvu oprávněné Smluvní strany přiměřenou jistotu.
193. Jakmile Smluvní strana oprávněná odstoupit od Rámcové dohody oznámí druhé Smluvní straně, že od Dílčí smlouvy nebo Rámcové dohody odstupuje, nebo že na Dílčí smlouvě/Rámcové dohodě setrvává, nemůže volbu již sama změnit.
194. Zakládá-li prodlení Smluvní strany nepodstatné porušení její povinnosti z Dílčí smlouvy, může druhá Smluvní strana od Dílčí smlouvy odstoupit poté, co prodlévající Smluvní strana svoji povinnost nesplní ani v dodatečně přiměřené lhůtě, kterou jí druhá Smluvní strana poskytla výslovně nebo mlčky.
195. Oznámí-li Smluvní strana Smluvní straně prodlévající, že jí určuje dodatečnou lhůtu k plnění a že jí lhůtu již neprodlouží, platí, že marným uplynutím této lhůty od Dílčí smlouvy odstoupila.
196. Poskytla-li Smluvní strana Smluvní straně prodlévající nepřiměřeně krátkou dodatečnou lhůtu k plnění a odstoupí-li od Rámcové dohody po jejím uplynutí, nastávají účinky odstoupení teprve po marném uplynutí doby, která měla být prodlévající Smluvní straně poskytnuta jako přiměřená. To platí i tehdy, odstoupila-li Smluvní strana od Rámcové dohody, aniž by prodlévající Smluvní straně dodatečnou lhůtu k plnění poskytla.
197. Plnil-li Zhotovitel zčásti, může Smluvní strana od Dílčí smlouvy odstoupit jen ohledně nesplněného zbytku plnění. Nemá-li však částečné plnění pro Objednatele význam, může Objednatel od Dílčí smlouvy odstoupit ohledně celého plnění. Odstoupil-li od nesplněného zbytku plnění Zhotovitel, je Objednatel oprávněn odstoupit od splněné části Dílčí smlouvy, nemá-li částečné plnění pro Objednatele význam.
198. Zavazuje-li Dílčí smlouva Zhotovitele k opakované činnosti nebo k postupnému dílčímu plnění, může Objednatel od Dílčí smlouvy odstoupit jen s účinky do budoucna. To neplatí, nemají-li již přijatá dílčí plnění sama o sobě pro Objednatele význam.
199. Smluvní strany se dohodly, že dojde-li k odstoupení od Dílčí smlouvy jen ohledně nesplněného zbytku plnění, užijí se na splněnou část plnění obdobně všechna ustanovení Dílčí smlouvy,

Rámcové dohody a Obchodních podmínek týkající se předání a převzetí Díla, přičemž přejímací řízení Smluvní strany zahájí nejpozději do 3 pracovních dnů ode dne odstoupení od Rámcové dohody, a dále všechna ustanovení Dílčí smlouvy, Rámcové dohody a Obchodních podmínek o právech a povinnostech Smluvních stran, které jsou Smluvní strany povinny plnit v době ode dne převzetí Díla Objednatelem, tedy zejm. ustanovení o vadách Díla.

200. Ustanovení §1977, §2002 - 2003 Občanského zákoníku se neužijí.

ČÁST 22 - OSTATNÍ UJEDNÁNÍ

Částečné plnění

201. Ustanovení Dílčí smlouvy, Rámcové dohody a Obchodních podmínek platí obdobně též pro části Díla, provádí-li Zhotovitel Dílo v souladu se Rámcovou dohodou po částech, není-li uvedeno jinak.

Postoupení, započtení

202. Zhotovitel není oprávněn postoupit žádnou svou pohledávku za Objednatelem vyplývající z Dílčí smlouvy nebo Rámcové dohody nebo vzniklou v souvislosti s Dílčí smlouvou nebo Rámcovou dohodou.

203. K pohledávce za Objednatelem vyplývající Dílčí smlouvy nebo Rámcové dohody nebo vzniklé v souvislosti s Dílčí smlouvou nebo Rámcovou dohodou nesmí být zřízeno zástavní právo.

204. Zhotovitel není oprávněn provést jednostranné započtení žádné své pohledávky za Objednatelem vyplývající z Dílčí smlouvy nebo Rámcové dohody nebo vzniklé v souvislosti s Dílčí smlouvou nebo Rámcovou dohodou na jakoukoliv pohledávku Objednatele za Zhotovitelem.

205. Objednatel je oprávněn provést jednostranné započtení jakékoliv své splatné i nesplatné pohledávky za Zhotovitelem vyplývající z Dílčí smlouvy nebo Rámcové dohody nebo vzniklé v souvislosti s Dílčí smlouvou nebo Rámcovou dohodou (zejm. smluvní pokutu) na jakoukoliv splatnou či nesplatnou pohledávku Zhotovitele za Objednatelem.

Mlčenlivost

206. Zhotovitel je povinen zachovávat mlčenlivost o všech skutečnostech a informacích, které jsou obsažené v Dílčí smlouvě a Rámcové dohodě a dále o všech skutečnostech a informacích, které mu byly v souvislosti se Rámcovou dohodou, Dílčí smlouvou nebo jejím plněním jakkoliv zpřístupněny, předány či sděleny, nebo o nichž se jakkoliv dozvěděl, vyjma těch, které jsou v okamžiku, kdy se s nimi Zhotovitel seznámil, prokazatelně veřejně přístupné, nebo těch, které se bez zavinění Zhotovitele veřejně přístupnými stanou. Zhotovitel nesmí takové skutečnosti a informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo třetích osob a nesmí je použít ani v neprospěch Objednatele. Povinnosti dle tohoto odstavce je Zhotovitel povinen zachovávat i po zániku závazku z Rámcové dohody a Dílčí smlouvy, vyjma případů, kdy se takové skutečnosti a informace stanou prokazatelně veřejně přístupné bez zavinění Zhotovitele. Povinnosti dle tohoto odstavce se nevztahují na případy, kdy je Zhotovitel povinen zveřejnit takové skutečnosti nebo informace na základě povinnosti uložené mu právním předpisem nebo rozhodnutím orgánu veřejné moci.

Kontrola

207. Zhotovitel si je vědom, že je ve smyslu §2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, povinen spolupůsobit při výkonu finanční kontroly a zavazuje se finanční kontrolu strpět.

208. Je-li Dílo z jakékoliv části financováno z prostředků Evropské unie, je Zhotovitel povinen

208.1. strpět veškeré kontroly vyplývající z režimu financování Díla z prostředků Evropské unie,

208.2. poskytnout při takových kontrolách veškerou nezbytnou součinnost,

208.3. archivovat veškerou dokumentaci týkající se Rámcové dohody po dobu stanovenou pravidly, jimiž se řídí financování Díla z prostředků Evropské unie.

Jazyk

209. Ve všech záležitostech souvisejících se Dílčí smlouvou nebo Rámcovou dohodou budou zástupci Smluvních stran komunikovat v českém jazyce. Všichni zástupci musí plyně český jazyk ovládat. Jestliže český jazyk plyně neovládají, jsou povinni na náklady své Smluvní strany

zajistit, aby byl po celou dobu vzájemné osobní komunikace k dispozici kvalifikovaný tlumočnick.

Forma, označení času

- 210. Písemnou formou (podobou) se rozumí listina podepsaná oprávněnou osobou Smluvní strany nebo email podepsaný zaručeným elektronickým podpisem oprávněné osoby Smluvní strany.
- 211. Je-li v Dílčí smlouvě, Rámcové dohodě nebo Obchodních podmínkách uvedena lhůta nebo doba počítané podle dnů, měsíců nebo let, rozumí se tím vždy kalendářní den, měsíc nebo rok, není-li uvedeno jinak.

Reference

- 212. Zhotovitel je oprávněn uvádět Dílo a jméno Objednatele jako referenci na svou činnost pouze s předchozím písemným souhlasem Objednatele.

Salvatorní klauzule

- 213. Je-li nebo stane-li se některé oddělitelné ustanovení Dílčí smlouvy, Rámcové dohody nebo Obchodních podmínek neplatné, neúčinné či nevymahatelné, nedotýká se tato skutečnost ostatních ustanovení. Smluvní strany se zavazují nahradit takové ustanovení jiným ustanovením, které svým obsahem a smyslem bude nejvíce odpovídat obsahu a smyslu ustanovení nahrazovaného.

Bližší specifikace plnění

Předmětem plnění VZ je zhotovení (provedení) Díla ve smyslu odst. 2 čl. I. Rámcové dohody, jímž se rozumí provedení bezpečnostních testů (viz níže), jejichž cílem je detekce zranitelností, které se vyskytují v Objednatelem používaných technologiích nebo vznikají nepatřičnými konfiguracemi nebo nevhodným návrhem aplikací / IS. Bezpečnostní testy rovněž slouží k prověření odolnosti ICT infrastruktury, prostředí koncového uživatele a aplikovaných postupů a procesů. Zároveň je jejich cílem prověření stavu fyzického zabezpečení objektů SŽ. Součástí Díla je rovněž Zpráva o výsledku bezpečnostních testů, blíže specifikována níže v této příloze.

Na základě dílčích smluv, budou realizovány bezpečnostní testy z těchto oblastí:

- testy zranitelností,
- penetrační testy,
- testy konfigurací,
- testy fyzického zabezpečení,
- testy bezpečnostních procesů a postupů.

Z pohledu rozsahu a formy mohou být testy realizovány vůči:

- části informačního systému / aplikace,
- prvku ICT Infrastruktury,
- celému informačnímu systému / aplikaci,
- vazbám mezi informačními systémy / aplikacemi,
- bezpečnostním prvkům,
- bezpečnostnímu perimetru organizace,
- lokalitám / objektům (v případě testů fyzického zabezpečení),
- případně dalším.

Pozn.: platí pro informační systémy / aplikace, webové aplikace a služby, prvky ICT Infrastruktury a bezpečnostní prvky dostupné ze sítě internet nebo z interní datové sítě SŽ.

Bezpečnostní testování bude prováděno následovně

White box / Glass box / Full knowledge test – testeři mají k dispozici veškeré informace o cílovém prostředí (dle typu testu může jít o informace: používané platformy nebo zdrojové kódy, seznamy zaměstnanců, plány budov atd.). Tento přístup je vhodný pro určité formy technických auditů i pro simulaci určitých typů útoků (např. útok realizovaný privilegovaným interním zaměstnancem cílové organizace).

Black box/Blind test – testerům nejsou poskytnuty žádné předchozí informace o cílovém prostředí, tento přístup je vhodný pro realistickou simulaci útoku vnějším aktérem vzhledem k tomu, že testeři užívají stejných technik a postupů, které by byl takový aktér nucen použít (OSINT techniky, discovery skeny, socioinženýrský sběr dat atp.).

Grey box test – kombinace výše uvedených přístupů. Testerům jsou při grey box testech poskytnuty pouze vybrané informace o cílovém prostředí (např. pouze informace o umístění a typech bezpečnostních prvků na perimetru datové sítě), což může vést k rychlejší realizaci testů než v případě black box testů, avšak znamená rovněž o něco nižší vypovídací hodnotu testu jako simulace reálného útoku.

Bezpečnostní testy budou zahrnovat

Skenování zranitelností – testeři manuálním / automatizovaným způsobem ověří systémy, které byly určeny Zadavatelem. Mohou být jednorázové nebo pravidelné v návaznosti na požadavcích Zadavatele.

Penetrační testování – prováděno převážně manuálním způsobem. Při takovém testu je testována bezpečnost systému, který byl určen Zadavatelem.

Testování může být dle aktuálního požadavku Zadavatele realizováno v souladu s uvedenými standardy a metodikami:

- Penetrační testování – úvod do problematiky (podpůrný materiál) – vydáno 5. 3. 2024 Národním úřadem pro kybernetickou a informační bezpečnost,
- Technical Guide to Information Security Testing and Assessment (NIST 800-115),
- NIST Special Publication (SP) 800-115,
- SCADA/ICS,
- Open Web Application Security Project (OWASP),
- OWASP Mobile Security Testing Guide a OWASP Mobile Top 10,
- Web Security Testing Guide (WSTG),
- Open Source Security Testing Methodology Manual (OSSTMM),
- OWASP Application Security Verification Standard (ASVS),
- Penetration Testing Execution Standard (PTES),
- Metodiky Licensed Penetration Tester (LPT),
- Information Systems Security Assessment Framework (ISSAF).

Provádění bezpečnostních testů nesmí žádným způsobem ohrozit funkčnost a provozní parametry ICT Infrastruktury Zadavatele (tedy musí být zachována plná funkčnost, nesmí docházet k prodloužení odezvy informačních systémů / aplikací apod.). Výjimky z tohoto požadavku musí být před provedením bezpečnostního testu výslovně odsouhlaseny Zadavatelem.

Zahájení bezpečnostního testu

Před zahájením bezpečnostního testu Objednatel stanoví a oznámí Zhotoviteli, popř. si Objednatel vyžádá od Zhotovitele následující (bez níže uvedených skutečností není možné spustit bezpečnostní testování):

- konkrétní datum a čas provedení bezpečnostních testů,
- cílové IP adresy a porty či jejich rozsahy,
- zdrojové IP adresy a porty či jejich rozsahy,
- seznam osob provádějících testování (za účelem přidělení potřebných přístupových oprávnění do testovaných systémů),
- lokality /objekty organizace, ze kterých budou bezpečnostní testy prováděny.

Výstup bezpečnostního testu (tj. „Zpráva“)

Výsledky bezpečnostního testu zpracuje Dodavatel do podoby Zprávy dodané ve strojově čitelném formátu „pdf“, která bude obsahovat minimálně:

- vymezení rozsahu testování, včetně času a identifikace testu, lokality / objekty, osob,
- popis testovací metody,
- užitá metodika,
- popis testovacího scénáře, popis provedeného způsobu testování a postupů,
- seznam identifikovaných zranitelností,
- hodnocení ke každé identifikované zranitelnosti dle aktuálního standardu CVSS (Common Vulnerability Scoring System),
 - popis způsobu možného zneužití každé zranitelnosti,
- popis a doporučení na odstranění každé zranitelnosti a doporučení na snížení případných dopadů jejího zneužití,
- popis a doporučení nápravných opatření,
- poskytnutí důkazu o identifikované zranitelnosti, nebo způsobu, jak ověřit identifikovanou zranitelnost,

příčemž

- celkový obsah Zprávy a související předávané dokumentace musí být natolik podrobný, aby bylo možné test opakovat podle stejných podmínek.

Zpracování Zprávy v souladu s touto přílohou Rámcové dohody a její akceptace Zadavatelem je nezbytnou podmínkou pro fakturaci realizovaných služeb dle Dílčí smlouvy. Obsah a závěry Zprávy jsou nezávislé na vůli Zadavatele co do zjištěného výsledku testování. Dodavatel bere na vědomí, že činnostmi souvisejících s prováděním Bezpečnostních testů se mohou účastnit rovněž zástupci Zadavatele.

Dodavatel je povinen po předání Zprávy Objednateli poskytnout na výzvu Objednatele konzultaci výsledků testování plynoucích ze Zprávy či jejich prezentaci.

Příklady požadovaných bezpečnostních testů:

Pro příklad uvádí Zadavatel detailnější přehled jednotlivých bezpečnostních testů, které mohou být ze strany Zadavatele vyžadovány:

1) Bezpečnostní testy webových aplikací:

- ověření způsobů přihlašování (autentizace a autorizace) k identifikovaným informačním systémům / aplikacím, webovým aplikacím a službám,
- test webových aplikací a služeb na známé bezpečnostní problémy z databáze zranitelností,
- zjišťování zadních vrátek do webových aplikací a služeb,
- ověření narušení Dostupnosti webových aplikací a služeb,
- ověření narušení Integrity dat,
- ověření narušení Důvěrnosti webových aplikací a služeb,
- ověření správnosti konfigurací webových aplikací a služeb,
- ověření možností eskalace oprávnění s cílem ovládnout webové aplikace a služby,

- ověření možností útoků typu SQL Injection,
- ověření možností útoků typu Cross-site scripting (XSS), Cross-site Request Forgery (CSRF),
- testy při každé změně zasahující do bezpečnostních parametrů a při dalších významných změnách webových aplikací a služeb,
- další zde neuvedené v dané oblasti.

2) Bezpečnostní testování aplikací / IS (včetně ICT infrastruktury určené k jejich provozu):

- identifikace informačních systémů / aplikací a webových aplikací (použité technologie, verze atd.), včetně testovacích verzí a prostředí,
- identifikace prvků ICT Infrastruktury (servery – fyzické i virtuální, switche, routery, modemy, poštovní servery, infrastruktura pro vzdálený přístup – Citrix, RDP, aj., operační systémy, middleware – včetně jejich obslužných nástrojů / konzolí, DNS servery, webové servery, FTP(S) servery, DB servery, aplikační servery apod.),
- identifikace bezpečnostních prvků (VPN koncentrátory, FW, IDS / IPS, NGFW, Proxy soustava, Sandbox, WAF – včetně jejich obslužných nástrojů / konzolí apod.),
- identifikace Wifi sítí,
- komplexní detekce otevřených TCP / UDP portů,
- detekce aktivních IP adres (v4 i v6),
- rozpoznání topologie interní datové sítě / sítí,
- získávání informací o informačních systémech / aplikacích, webových aplikacích a službách,
- získávání informací o prvcích ICT Infrastruktury,
- získávání informací o bezpečnostních prvcích,
- test DNS serverů, průzkum DNS zón, podvržení DNS serverů,
- zachycení odchozí a příchozí komunikace a následné získání informací, přesměrování této komunikace,
- ověření způsobů přihlašování k identifikovaným informačním systémům / aplikacím,
- ověření způsobů přihlašování k identifikovaným prvkům ICT Infrastruktury,
- ověření způsobů přihlašování k identifikovaným bezpečnostním prvkům,
- test identifikovaných informačních systémů / aplikací, na známé bezpečnostní problémy z databáze zranitelností,
- test identifikovaných prvků ICT Infrastruktury na známé bezpečnostní problémy z databáze zranitelností,
- test identifikovaných bezpečnostních prvků na známé bezpečnostní problémy z databáze zranitelností,
- zjišťování zadních vrátek do identifikovaných informačních systémů / aplikací,
- zjišťování zadních vrátek do identifikovaných prvků ICT Infrastruktury,
- zjišťování zadních vrátek do identifikovaných bezpečnostních prvků,
- ověření narušení Dostupnosti informačních systémů / aplikací, prvků ICT Infrastruktury a bezpečnostních prvků (testování odolnosti systému proti útokům směřujícím k odepření služby poskytované systémem) – DoS / DDoS,
- ověření narušení Integrity dat,

- ověření narušení Důvěrnosti (dat i informačních systémů prvků ICT Infrastruktury a bezpečnostních prvků),
- ověření bezpečnosti, odolnosti a spolehlivosti bezpečnostních prvků,
- testy autentizace a autorizace informačních systémů / aplikací, prvků ICT Infrastruktury a bezpečnostních prvků,
- ověření správnosti konfigurací informačních systémů / aplikací, prvků ICT Infrastruktury a bezpečnostních prvků,
- ověření zabezpečení Wifi sítí a souvisejících prvků ICT Infrastruktury proti pokusům o průnik a odposlech, měření přesahů, detekce neoprávněných připojených zařízení, analýza dostupnosti interní datové sítě, pokusy o „přebití“ legitimních Wifi sítí,
- ověření zabezpečení mobilních zařízení a souvisejících prvků ICT Infrastruktury,
- ověření zabezpečení VoIP zařízení a souvisejících prvků ICT Infrastruktury,
- ověření možných vektorů útoků na organizaci,
- ověření výskytu pokročilých útoků (např. APT),
- ověření možností eskalace oprávnění s cílem ovládnout informační systémy / aplikace, prvky ICT Infrastruktury a bezpečnostní prvky,
- testy při každé změně zasahující do bezpečnostních parametrů a při dalších významných změnách informačních systémů / aplikací, prvků ICT Infrastruktury a bezpečnostních prvků.

3) Bezpečnostní testování OT sítí (včetně ICT infrastruktury určené k jejich provozu (aplikační, databázové servery a další.)), testování PLC či jiných specifických OT komponent:

- ověření zabezpečení SCADA / OT (typově bezpečnostní testy uvedené v části 2).

4) Testování personální odolnosti – provádění bezpečnostních testů s využitím technik sociálního inženýrství:

- ověření možností fyzického průniku do zabezpečených oblastí,
- ověření správnosti nastavení procesů a postupů organizace v oblasti zvládnutí kybernetických bezpečnostních incidentů,
- testování personální odolnosti zaměstnanců organizace s využitím pokročilých technik sociálního inženýrství (phishing, spear phishing, vishing, quishing, distribuce výměnných médií apod.).

Detailní požadavky na provedení konkrétního testu budou vždy uvedeny v rámci dílčí smlouvy.

Příloha č. 3 Rámcové dohody

Ceník

Bezpečnostní testování

Cena za 1 MD [Dodavatel doplní] ,- Kč bez DPH

Příloha č. 4 Rámcové dohody

Poddodavatelé

Zhotovitel poskytuje Objednateli předmět plnění dle Rámcové dohody sám.

/

Zhotovitel provádí předmět plnění dle Rámcové dohody prostřednictvím následujících Poddodavatelů:

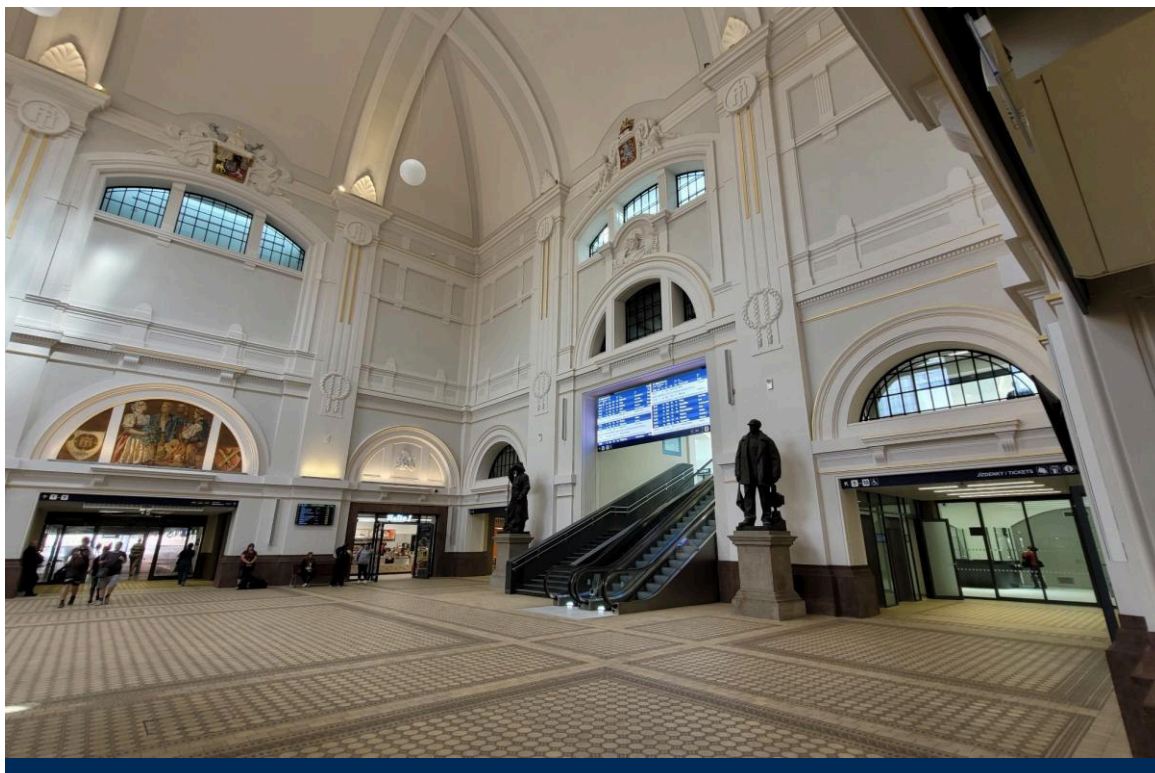
- [OBCHODNÍ FIRMA PODDODAVATELE – NÁZEV, IČO, SÍDLO – DOPLNÍ ZHOTOVITEL]	
- Část plnění dle Rámcové dohody prováděná prostřednictvím Poddodavatele ve finančním procentuálním vyjádření ve vztahu k nabídkové ceně.	- [DOPLNÍ ZHOTOVITEL] %
- Stručný popis činností, které jsou prováděny Poddodavatelem.	- [DOPLNÍ ZHOTOVITEL]

[Pokud Zhotovitel provádí plnění či jeho část prostřednictvím Poddodavatelů, uvede tabulku tolikrát, kolika Poddodavateli bude předmět plnění provádět. Zhotovitel musí uvést všechny Poddodavatele, kteří se budou podílet na provádění plnění dle Rámcové dohody a dílčích smluv.]

Příloha č. 5 Rámcové dohody

Realizační tým

Pozice	Kontaktní údaje	Činnosti prováděné členem Realizačního týmu
Vedoucí týmu	Jméno a příjmení: [DOPLNÍ ZHOTOVITEL] Telefon: [DOPLNÍ ZHOTOVITEL] E-mail: [DOPLNÍ ZHOTOVITEL]	Příprava plánu provádění bezpečnostních testů Řízení práce penetračních testerů Provádění bezpečnostních testů Prezentace výsledků bezpečnostních testů
Penetrační tester	Jméno a příjmení: [DOPLNÍ ZHOTOVITEL] Telefon: [DOPLNÍ ZHOTOVITEL] E-mail: [DOPLNÍ ZHOTOVITEL]	Spolupráce na přípravě plánu provádění bezpečnostních testů Provádění bezpečnostních testů Prezentace výsledků bezpečnostních testů



Platforma SŽ Základní dokument

Červen 2025

Obsah

1	Úvod	6
2	Platforma Správy železnic	6
3	Motivace Platformy SŽ	6
4	Architektonické principy	7
4.1	Bezpečnost a soulad s vnitropodnikovými předpisy	7
4.2	Auditní záznamy	7
4.3	Provozovatelnost řešení	8
4.4	Znovupoužitelnost řešení	8
4.5	Nezávislost na dodavatelích	9
4.6	Nákup a vývoj	9
4.7	Business kontinuita	10
5	Služby Platformy SŽ	10
5.1	Infrastrukturní služby	10
5.2	Platformní služby	10
5.3	Podpůrné služby	10
5.3.1	Bezpečnostní služby	10
5.3.2	Služby monitoringu	11
5.3.3	Služby patch managementu	11
5.3.4	Služby zálohování	11
5.3.5	Síťové služby	11
6	Technologie Platformy SŽ	12
7	Přílohy Platformy SŽ	13

Seznam zkratek

AD	Rozšiřitelná a škálovatelná adresářová služba, která umožňuje efektivně uspořádat síťové prostředky. Kromě informací o objektech v počítačové síti (uživatelské účty, počítače, tiskárny) umožňuje používat stromovou strukturu objektů, nastavovat globálně systémové politiky, instalovat programy na počítače nebo aplikovat kritické aktualizace v celé organizační struktuře. Má úzkou vazbu na DNS (Active Directory)
API	Komplexně definované komunikační rozhraní aplikace (<i>Application Programming Interface</i>)
CEF	Datový formát pro uložení logů (<i>Common Event Format</i>)
CIFS	Síťový komunikační protokol pro přenos souborů. Kompatibilní se SMB verze 1.0 (<i>Common Internet File System</i>)
CSV	Jednoduchý textový souborový formát (Comma-separated values)
DB	Databázový software/aplikace/entita/instance, která je zpravidla provozována na databázovém serveru (<i>Database Entity</i>)
DB	Soubor datových objektů v elektronické formě uložených společně podle jednoho schématu a zpřístupňovaných počítačem (<i>Database</i>)
DB	Komponenta DBMS umožňující operace s daty v databázi. Mnohé DBMS podporují více DB enginů s různými vlastnostmi a specifiky (<i>Database Engine, Storage Engine</i>)
DBMS	Systém řízení databáze (<i>Database Management System</i>)
DNS	Distribuovaný hierarchický jmenný systém používaný v síti Internet. Překládá názvy domén na číselné IP adresy a zpět, obsahuje informace o tom, které stroje poskytují příslušnou službu (Domain Name System)
HTTP	Standardizovaný protokol pro přenos webových stránek (<i>Hyper-text Transfer Protocol</i>)
HTTPS	Standardizovaný zabezpečený protokol pro přenos webových stránek (<i>Secured Hyper-text Transfer Protocol</i>)
HW	Hardware označuje veškeré fyzicky existující technické vybavení počítače
IaaS	Typ cloudové služby, který poskytuje zákazníkům základní IT infrastrukturu jako službu, včetně serverů, úložiště, sítě a virtuálních počítačů. Tyto služby se často poskytují prostřednictvím Internetu a umožňují zákazníkům snadno a rychle využívat IT infrastrukturu bez nutnosti jejího nákupu, instalace a správy. Mezi nejznámější poskytovatele IaaS patří Amazon Web Services, Microsoft Azure a Google Cloud Platform (<i>Infrastructure as a Service</i>)
ICMP	Síťový protokol, který slouží ke komunikaci mezi síťovými prvky (jako jsou routery) a k odesílání zpráv o stavu sítě. Tyto zprávy obsahují informace o stavu spojení, jako jsou například informace o chybách nebo omezeních v síti. ICMP se často používá k diagnostice a řešení problémů v síti, například k zjišťování, zda je určitý cíl dostupný nebo zda existuje cesta k němu (<i>Internet Control Message Protocol</i>)
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
IPMI	Standardizovaný protokol pro vzdálený dohled a management fyzických zařízení
IT	Informační technologie (<i>Information Technology</i>)
JDBC	API v jazyce Java pro jednotné rozhraní k relačním databázím (<i>Java Database Connectivity</i>)
JSON	Datový formát primárně určený pro přenos dat. Jedná se o způsob zápisu dat nezávislý na počítačové platformě, která mohou být organizována v polích nebo agregována v objektech (<i>JavaScript Object Notation</i>)
LEEF	Datový formát pro uložení logů (<i>Log Event Extended Format</i>)
MFA	Více-faktorové ověření identity uživatele (<i>Multi-Factor Authentication</i>)
NFS	Síťový souborový protokol primárně pro připojení vzdálených souborových systémů (<i>Network File System</i>)
OS	Operační systém (<i>Operating System</i>)
PaaS	Typ cloudové služby, která poskytuje vývojářům a IT týmům platformu pro vývoj, nasazení a správu aplikací bez nutnosti starat se o správu hardwaru a infrastruktury. Poskytovatelé PaaS nabízejí vývojové nástroje, databáze, síťové služby a další nástroje jako služby, což umožňuje vývojářům se soustředit pouze na vývoj aplikace (<i>Platform as a Service</i>)

PAM	Řešení zabezpečení identit, které pomáhá chránit organizaci před kybernetickými hrozbami monitorováním, zjišťováním a prevencí neoprávněného privilegovaného přístupu k důležitým prostředkům (<i>Privileged Access Management</i>)
PoC	Tento pojem se pro předběžné vyzkoušení určitého návrhu (zpravidla na reálných datech či jejich výběru), aby došlo k vyzkoušení nebo předvedení použité logiky a proveditelnosti návrhu řešení. V podstatě se může jednat o testovací realizaci nějakého konkrétního návrhu zpravidla ve zjednodušených podmínkách. Cílem PoC je ukázat, že návrh je technicky proveditelný a že má potenciál být úspěšný (<i>Proof of Concept</i>)
REST/API	Webově založené klient-server API (<i>Representational State Transfer</i>)
RFC	Soubor standardů zejména pro oblast sítí, počítačů a Internetu. RFC jsou považovány spíše za doporučení než normy či standardy v tradičním smyslu jako jsou například normy ČSN nebo ISO, avšak v zájmu interoperability jsou dodržovány (<i>Request For Comments</i>)
S2S VPN	Šifrované VPN připojení zajišťující propojení dvou LAN (<i>Site-to-Site VPN, LAN-to-LAN VPN</i>)
SCCM	SCCM je softwarový nástroj společnosti Microsoft určený pro správu a nasazení koncových zařízení a softwarových aplikací v prostředí Windows. SCCM umožňuje centrální správu a monitorování koncových zařízení, aktualizace softwaru a operačních systémů, správu konfiguračních položek a politik, sledování bezpečnostních opatření a mnoho dalšího. SCCM může být použit v podnikovém prostředí pro správu tisíců koncových zařízení, od stolních a notebooků až po mobilní zařízení a servery (<i>System Center Configuration Manager</i>)
SFTP	Zabezpečený protokol pro přenos souborů. Pro zajištění šifrování využívá protokol SSH (<i>SSH File Transfer Protocol</i>)
SLA	Smluvní nastavení záruk, úrovně, dostupnosti a kvality služeb atd. (<i>Service-Level Agreement</i>)
SMB	Komunikační protokol pro přenos souborů. Lidově nazývaný Samba (<i>Server Message Block</i>)
SNMP	Jedná se o protokol pro správu sítí na úrovni aplikační vrstvy síťového OSI modelu, který umožňuje správcům sítě monitorovat a řídit chod síťových zařízení, jako jsou routery, switche a průmyslové kontroléry. Protokol umožňuje správcům sítě získat informace o stavu zařízení, jako jsou statistiky paketů, využití zdrojů a stav služeb, a měnit nastavení zařízení na dálku (<i>Simple Network Management Protocol</i>)
SW	Programové vybavení počítače či jiného obdobného zařízení. Speciálním druhem software je <i>firmware</i> , který je úzce spjatý s konkrétním hardwarem (<i>Software</i>)
SŽ	Správa železnic, státní organizace
SŽT	Správa železniční telematiky, organizační jednotka
UAS	Logická uživatelsko-aplikační síť SŽ, zahrnuje VRF v MPLS sítích a lokální VLAN, běžně se nazývá také „Intranet SŽ“
VoKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů
VPN	Virtuální privátní síť – prostředek pro důvěryhodné propojení komponent informačního systému v rámci obecně nezabezpečené komunikační sítě. Při navazování spojení je obvykle vyžadována autentizace, komunikace je většinou šifrována (<i>Virtual Private Network</i>)
WEC	Technologie předávání logů v prostředí Microsoft Windows (<i>Windows Event Collector</i>)
WEF	Technologie předávání logů v prostředí Microsoft Windows (<i>Windows Event Forwarder</i>)
XDR	Koncepce bezpečnosti informačních technologií, která integruje různé nástroje a technologie pro detekci a reakci na hrozby v jednotném systému. Cílem XDR je zlepšit schopnost detekovat a reagovat na hrozby v celém IT prostředí, včetně cloudových a on-premise systémů. Funkce XDR zahrnují automatickou detekci hrozeb, škálovatelnou analýzu, pokročilou vizualizaci a integraci s jinými bezpečnostními technologiemi (<i>Extended Detection and Response</i>)
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

Seznam vysvětlivek

Build	Označení konkrétní verze software, zpravidla operačního systému.
Disaster Recovery	Plán obnovy po havárii, součást kontinuity IT služeb.
Log Management	System centrálního sběru a ukládání logů
Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.
Syslog	Standardizovaný formát pro ukládání a předávání logů

1 Úvod

Cílem tohoto dokumentu je definovat Platformu SŽ, jakožto souhrn podporovaných infrastrukturních služeb, technologií, a architektonických principů, která určuje základní rámec pro návrh řešení ICT jako celku. Platforma SŽ podporuje naplnění strategických cílů IS/ICT Správy železnic, zejména v oblasti efektivního provozu a rozvoje ICT prostředí Správy železnic.

2 Platforma Správy železnic

Platforma Správy železnic definuje prostředí, které standardizuje a podporuje návrh, implementaci a provozování veškerého ICT řešení pro Správu železnic. Popisuje infrastrukturní a platformní služby, podporované technologie a upravuje pravidla jejich použití i rozšiřování. Primárním cílem Platformy SŽ je poskytnout potenciálním dodavatelům základní přehled o ICT prostředí SŽ a současně umožnit organizaci SŽ zajištění efektivního vytváření a provozování ICT řešení při dodržení vysoké kvality a bezpečnosti služeb.

Dokument včetně příloh je udržován a pravidelně aktualizován organizační jednotkou SŽT.

Platforma SŽ obsahuje:

- Základní popis ICT prostředí (v jednotlivých přílohách)
- Architektonické principy SŽ
- Přehled služeb Platformy SŽ
- Přehled technologií Platformy SŽ (v jednotlivých přílohách)

Při plánování a rozšiřování ICT řešení je nutné respektovat všechny části Platformy SŽ, které se daného řešení dotýkají. Jednotlivé přílohy se pak detailně zabývají vybranými oblastmi od serverové a síťové infrastruktury, přes softwarový vývoj až po integrace, komunikaci a zálohování.

3 Motivace Platformy SŽ

Platforma SŽ je motivovaná schválenou strategií IS/ICT SŽ, a to konkrétně cílem *zajištění dlouhodobého koncepčního rozvoje IS/ICT a jeho souladu se strategickými cíli SŽ, a to zavedením řízení celopodnikové IS/ICT architektury*¹.

Cílem Správy železnic je zajistit:

- Nastavení jasných a povinných požadavků na nová navrhovaná řešení.
- Uchazeči výběrových řízení na ICT řešení mohou být hodnoceni na základě jejich celkové ekonomické efektivity, a nikoliv pouze na základě nabídkové ceny. Podrobná pravidla stanoví Zadávací dokumentace,
- Externí dodávky ICT řešení budou koncepčně a technologicky zapadat do celopodnikového prostředí Správy železnic,
- Dodávané řešení bude možné bezpečně a ekonomicky efektivně provozovat v krátko-, středně-, i dlouhodobém časovém horizontu,
- Provozované technologie SŽ budou perspektivní, moderní a bezpečné,
- Technologická různorodost ICT prostředí SŽ bude:
 - na jednu stranu dostatečně široká, aby neúměrně neomezovala soutěž potenciálních dodavatelů, a

¹ Strategie IT a ICT Správy železnic (157463/2021-SŽ-GŘ-SŽT)

- o na druhou stranu dostatečně ohraničená, aby umožnila efektivní správu systémů jak dodavateli, tak zaměstnanci Správy železnic.

Mezi hlavní přínosy Platformy SŽ patří:

- Nastavení společných (minimálních/maximálních) úrovní vyspělosti jednotlivých technologií napříč IS/ICT SŽ a postupné omezení velkých rozdílů v úrovních používaných technologií.
- Stanovení architektonických a technologických standardů pro tvůrce systémů a pro uchazeče o dodávku IS/ICT pro SŽ.
- Zajištění standardizace technických prostředků.
- Zajištění ochrany předchozích investic zamezením vzniku duplicit.
- Zajištění možnosti bezpečného převzetí systémů do provozu a zajištění provozu interními silami Správy železnic.

4 Architektonické principy

Při návrhu a realizaci ICT řešení je nutné respektovat a dodržet několik základních principů a pravidel stanovených v Platformě SŽ.

4.1 Bezpečnost a soulad s vnitropodnikovými předpisy

- Navrhované řešení a procesy jím podporované musí být v souladu s legislativními a regulačními nároky a vnitropodnikovými předpisy Správy železnic.
- Řešení musí umožnit monitorování akcí uživatelů, zejména jejich práce s daty a dokumenty.
- Musí být zajištěna administrovatelnost a auditovatelnost integračních vazeb.
- Vývoj a test nesmí být realizován na produkčním prostředí.
- Topologie a architektura produkčního a testovacího prostředí musí být identická, odlišovat se může ve výkonu a použitých zdrojích.
- Před nasazením do produkčního prostředí je řešení prokazatelně otestováno.
- Nejsou realizovány integrace mezi produkčními a neprodukčními prostředími.
- Dohled a monitoring je zajištěn na všech vrstvách řešení (HW, OS, DB, aplikační server, aplikace, tenký a tlustý klient, koncový uživatel).
- Musí být zajištěno napojení na centrální dohledovou konzoli.
- Služby poskytované do prostředí Internetu musí projít penetračním testováním.
- Navrhované řešení musí využívat šifrovanou komunikaci a v případě ukládání jakýchkoli citlivých informací (hesla apod.) je ukládat v šifrované podobě. Šifrovací algoritmy musí respektovat doporučení NÚKIB v dokumentu *Minimální požadavky na kryptografické algoritmy* v aktuální verzi, která je uveřejněna na úřední desce NÚKIB.

Zdůvodnění: Bezpečnost umožňuje chránit hodnoty Správy železnic. Ve SŽ je nutné udržovat vysokou míru bezpečnosti, a to především v oblastech, které mohou mít dopady na lidské životy. Navrhovaná řešení také musí být nezbytně v souladu s VoKB.

4.2 Auditní záznamy

Celé řešení i jednotlivé prvky řešení (infrastrukturní prvky, aplikace, OS, webové servery, databáze a middlewary) musí umožňovat vytvářet auditní záznamy tedy logy (záznamy např. čas přihlášení uživatele, čas odhlášení, import, export souborů a podobně) a jejich přenos do centrálního úložiště log management v SŽ.

Veškeré činnosti v systému musí být logovány a to včetně neúspěšných pokusů. Jde zejména o následující činnosti:

- přihlášení a odhlášení uživatelů a administrátorů
- neúspěšný pokus o přihlášení
- činnosti provedené administrátory

- činnosti vedoucí ke změně přístupových oprávnění
- neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů
- zahájení a ukončení činností technických aktiv (například spuštění zastavení služeb)
- automatická varovná nebo chybová hlášení technických aktiv
- pokusy o manipulaci s logy a změny nastavení nástroje pro logování
- použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení
- operace s citlivými daty
- veškeré události spojené se změnou bezpečnostních parametrů systému

Řešení musí být schopno předávat auditní záznamy v minimálně jednom z formátů:

- CEF
- Microsoft Windows Event Log
- LEEF
- Strukturované DB view
- JSON
- CSV

Pomocí aspoň jednoho z protokolů:

- Syslog RFC5424
- WEC
- JDBC
- REST/API
- NFS
- SFTP
- CIFS/SMB
- SNMPv3

A musí obsahovat minimálně následující informace:

- časové razítko
- druh provedené akce
- unikátní identifikátor uživatele nebo služby
- zdroj události (zdrojová IP adresa/hostname komponenty systému, na které k akci došlo)

Zdůvodnění: Auditní záznamy jsou klíčovou součástí bezpečnosti. Ve SŽ je nutné zajistit vysokou míru bezpečnosti, a to mimo jiné i auditovatelností veškerých událostí.

4.3 Provozovatelnost řešení

- Řešení je provozovatelné na službách a technologiích Správy železnic.
- Řešení musí umožňovat převzetí do provozního prostředí Správy železnic
- Řešení umožňuje škálování.

Zdůvodnění: Z důvodu snahy o udržitelnost provozu je stanoven udržitelný počet technologií, které jsou spolehlivé a mají perspektivu svého rozvoje. Aplikace provozovaná na takto definované skupině technologií tak může být v případě potřeby převzata do provozu a spravována týmem IT specialistů SŽ, jež disponuje patřičnými znalostmi, případně vlastní příslušné certifikace, aby mohli tyto technologie či systémy spravovat. Tím dochází nejen ke zvýšení produktivity, ale také k časové a finanční úspoře, především z pohledu lidských zdrojů.

4.4 Znovupoužitelnost řešení

- Řešení musí umožňovat logické oddělení dat pro současné využívání funkcionality různými subjekty (tzv. multitenant).
- V rámci Správy železnic se realizuje minimalizace počtu a rozsahu používaných technologií a aplikací.

- Snižováním počtu a rozsahu používaných technologií a aplikací snižujeme komplexitu správy technologického a aplikačního portfolia.
- Řešení je navrhované s opakováním ověřených jednoduchých návrhových vzorů a designových principů.
- Nasazování změn a nových řešení je seskupováno dle funkcionalit a cílových systémů do jednotlivých „release“. Termíny releaseů jsou stanoveny organizační jednotkou SŽT.
- Nasazované řešení nesmí ke svému provozu vyžadovat pravidelný nutný zásah administrátora (např. restarty, čištění logů, ...)

Zdůvodnění: V rámci Správy železnic usilujeme o minimalizaci počtu prostředí pro stejnou funkcionalitu. Znovupoužitelná řešení vedou k úspoře lidských, finančních, časových i materiálních zdrojů v životním cyklu celého řešení.

4.5 Nezávislost na dodavatelích

- Řešení je navrhované s ohledem na omezení či eliminaci rizika vendor-lock.
- U řešení převzatých do provozu je cíl převzetí schopnosti vytvořit build aplikace bez závislosti na dodavateli.
- Usilujeme o právo zásahu do zdrojových kódů a rozvoje řešení interními kapacitami Správy železnic nebo dalšími dodavateli. Výjimku mohou tvořit jen případy, kdy by takové požadavky byly ekonomicky výrazně nevýhodné nebo je důvod se domnívat, že tato práva budou nadbytečná.

Zdůvodnění: Nebýt závislí na malém počtu dodavatelů umožňuje SŽ být transparentní a flexibilní. Vyšší míra flexibility je také výhodná pro vyjednávání s jednotlivými dodavateli o ekonomických a technických podmínkách.

4.6 Nákup a vývoj

- U nákupu standardizovaných komerčních produktů je požadována schopnost nastavení balíkového řešení interními kapacitami či nezávislými externími dodavateli.
- U standardizovaných agend je preferován nákup a úprava před zakázkovým vývojem zcela nového zákaznického řešení.
- Vzájemné integrace musí být realizované přes aplikační middleware. Integrovaní scénáře zajišťují, aby implementace nových funkcí v řídicí aplikaci minimalizovala vyvolané změny na straně návazných aplikací. Detailněji se integracemi zabývá Příloha 5 – *Integrační standardy*.
- Preferujeme přírůstkovou integraci před přenosem kompletních informací.
- Preferujeme řešení v minimálně třívrstvé architektuře s oddělením databázové, aplikační a prezentační vrstvy.
- Minimalizujeme dodávku řešení s takovými úpravami, které by omezovaly nebo eliminovaly přechod na budoucí vyšší verze produktu.
- V transakčních systémech preferujeme pouze základní operativní reporting. Plný reporting je implementovaný v analytických nástrojích.
- Řešení je řádně dokumentované po stránce vývojové, provozní, administrátorské a uživatelské.
- Případné zdrojové kódy jsou verzovány a ověřeny, že z nich je možno vytvořit interními týmy Správy železnic plnohodnotný a funkční build aplikace. Zdrojové kódy a dokumentace jsou ukládány na standardizované úložiště Správy železnic.
- Návrh prostředí reflektuje trendy technologií a zároveň business potřeby.
- Rozšiřování a doplňování technologií a ICT prostředí je v souladu s normami, interními směrnicemi a Platformou SŽ.

Zdůvodnění: Regulace nákupu a případného do-vývoje integrací a aplikací slouží k co nejsrozumitelnějšímu a transparentnímu užívání daných technologií. Díky danému postupu v nákupu a vývoji je možné se efektivně vyrovnat s novinkami, které nově nakoupené produkty představují a efektivně je začlenit do ICT prostředí Správy železnic.

4.7 Business kontinuita

- Navržené řešení musí odpovídat kritičnosti aplikace a požadovaným parametrům SLA.
- Servisní model a parametry aplikace odpovídají bezpečnostní klasifikaci a byznysové kritičnosti aplikace.
- Dle servisního modelu jsou definované plány obnovy („disaster recovery“ postupy).
- SLA je třeba nastavovat a měřit na celém řetězci navázaných technologií a služeb.

Zdůvodnění: Správa železnic jakožto správce kritické infrastruktury státu, musí být připraven na případné narušení provozu, a proto musí požadovat taková řešení, která umožní zajistit kontinuitu a obnovu klíčových procesů, činností a systémů organizace.

5 Služby Platformy SŽ

Platforma SŽ popisuje služby poskytované v rámci ICT prostředí Správy železnic, které je možné využívat v navrhovaných a dodávaných řešeních a současně nesmí být totožné služby součástí dodávky daného řešení mimo Platformu SŽ. Cílem je zajistit ve fázích přípravy poptávky, návrhu ICT řešení a realizace dodávky kompatibilitu se stávajícím ICT prostředím a v maximální míře využít již provozované komponenty a technologie. Tento seznam služeb a komponent je průběžně aktualizován tak, aby byl popis ICT prostředí v největší míře aktuální.

5.1 Infrastrukturní služby

Infrastrukturní službou je míněno poskytování IT infrastruktury na úrovni HW, virtualizace, operačních systémů a diskových úložišť. Jedná se o obdobu cloudových IaaS.

Detailní přehled o infrastrukturních službách je předmětem Přílohy 3 – *Virtuální prostředí, serverové farmy a servery*.

5.2 Platformní služby

Platformní služba poskytuje standardizované webové či aplikační servery, databázové platformy či portálová řešení, která integrují webové aplikace a služby do jednoho spolupracujícího celku. Podporuje standardizované komunikační rozhraní, protokoly a formáty dat. Jedná se o obdobu cloudových PaaS. Platformní služby jsou v současné době dostupné jen v UAS.

Detailní přehled o infrastrukturních službách je předmětem Příloh Platformy SŽ.

5.3 Podpůrné služby

Podpůrné služby zajišťují komplexní správu a provoz IT infrastruktury v prostředí Správy železnic. Jedná se například o monitorovací systémy, zálohování, patch management, mandatorní síťové služby nebo bezpečnostní systémy.

Podpůrné služby jsou povinné k využití dodavatelem, pokud není Správou železnic určeno jinak.

5.3.1 Bezpečnostní služby

Přehled dostupných služeb bezpečnostních aplikací

Služba	Popis
Antivirus	Antivirové řešení F-Secure, provozované jako virtuální appliance, zajišťuje ochranu koncových stanic a serverové infrastruktury před škodlivým obsahem, zejména malwarem, exploity, síťovými útoky a jinými bezpečnostními hrozbami. Každé datové centrum Správy železnic disponuje vlastní virtuální appliance F-Secure. Nasazením antivirového řešení F-Secure jako virtuální appliance, jsou minimalizovány konzumované výpočetní zdroje a dopad na výkon virtualizační infrastruktury.
PAM	Privileged Access Management je řešení které pomáhá kontrolovat, monitorovat, zabezpečit a auditovat privilegované identity před jejich zneužitím. Omezení: PAM je v současné době dostupný jen v UAS.
XDR	XDR monitoruje síťovou infrastrukturu pomocí sond a uživatelské chování pomocí agentů na serverech a uživatelských stanicích. Bezpečnostní řešení XDR detekuje

	pokročilé bezpečnostní hrozby v prostředí SŽ. Každý server či uživatelská stanice musí mít nainstalovaného agenta XDR. V případě potřeby je možné upravit nastavení agenta pro korektní běh dodávaného systému. Omezení: Služby XDR jsou v současné době dostupné jen v UAS.
Log management	Řešení log managementu provádí sběr auditních záznamů z ICT infrastruktury SŽ. Omezení: V současné době je log management provozován v režimu PoC a je dostupný pouze v UAS.
Active Directory and Domain Services	Adresářová služba společnosti Microsoft pro správu zařízení a identit a jejich autentizaci a autorizaci v podnikových sítích. Dodávaná řešení musí podporovat integraci na službu Active Directory Správy železnic. Správa železnic provozuje multi-forest prostředí, proto musí aplikace umožňovat využití více AD konektorů, za účelem ověření uživatelů. Omezení: Služby Active Directory jsou v současné době dostupné jen v UAS.

5.3.2 Služby monitoringu

Služba dohledu ICT infrastruktury je zajištěna pomocí nástroje Zabbix a dohledových agentů instalovaných na provozovaném prostředí nebo bez-agentově se vzdáleným dohledem, sledování standardními protokoly SNMP, IPMI, HTTP, HTTPS, ICMP apod.

Dodavatelé ve spolupráci s organizační jednotkou SŽT zajistí napojení dodávaných řešení na monitoring Zadavatele. Tím není dotčena případná povinnost dodavatele řešení monitorovat kvalitu a dostupnost dodávaného řešení. Preferovaným řešením je v takovém případě využití služeb monitoringu SŽ s nastavením potřebných notifikací a procesů.

5.3.3 Služby patch managementu

Popis služeb patch managementu, aktualizací a distribuce aplikací

Služba	Popis
Distribuce SW a aktualizace koncových stanic	Technologií System Center Configuration Manager (SCCM) je zajištěna distribuce softwarových balíčků a aktualizace koncových stanic. Patchování klientských stanic probíhá 1 x měsíčně a je plně v gesci Správy železnic.
Aktualizace serverových operačních systémů	Aktualizace serverových operačních systémů Windows Server je řešena skriptovacím jazykem Powershell. Patchování serverových operačních systémů probíhá 1 x měsíčně a je zajištěno Správou železnic, pokud není s dodavatelem řešení dohodnuto jinak.
Aktualizace linuxových operačních systémů	Aktualizace linuxových operačních systémů je řešena vlastním repozitářem (např. Red Hat Satellite). Patchování linuxových operačních systémů probíhá dle potřeby a je zajištěno Správou železnic, pokud není s dodavatelem řešení dohodnuto jinak.

5.3.4 Služby zálohování

Detailní přehled o službách zálohování je předmětem Přílohy 7 – *Standardy zálohování a disaster recovery*.

5.3.5 Síťové služby

Přehled síťových služeb

Služba	Popis
DNS	Domain Name System (DNS) je kritickou službou, která má zásadní vliv na bezpečnost, odezvu a dostupnost služeb SŽ. Je nezbytná pro správný chod podnikové sítě a služeb na bázi Active directory. Správa železnic provozuje interní i externí službu DNS.
Firewall	Zařízení typu firewall jsou velmi důležitým bezpečnostním prvkem ve veškeré elektronické komunikaci v sítích SŽ, jenž pomocí pravidel filtruje síťový provoz a chrání ICT prostředky v síti Správy železnic.
Proxy	Proxy soustava zajišťuje přístup uživatelů a serverů k internetu. Naprostá většina komunikace uživatelů (zaměstnanců SŽ) do sítě Internet prochází přes ni, jiný přístup není povolen. Proxy servery fungují jako prostředník mezi klienty a cílovými servery, mimo perimetr sítě SŽ, překládá klientské požadavky a vůči cílovému serveru vystupuje sám jako klient.
Reverzní proxy	Všechna připojení z internetu směřující na některý ze serverů jsou směrována přes reverzní proxy server, který buďto požadavek zpracuje sám nebo ho předá dál serverům. Umožňuje SSL terminaci a kompresi.
VPN	Služba virtuální privátní sítě, umožňující dodavateli zabezpečený přístup konkrétních zaměstnanců ke konkrétním prostředkům v prostředí Správy železnic. Omezení: Jedná se o jmenovanou VPN s MFA pro konkrétního externistu.
VPN S2S	Služba virtuální privátní sítě Site-to-Site.

6 Technologie Platformy SŽ

V rámci služeb poskytovaných Platformou SŽ je využívána celá řada ICT technologií.

Tyto technologické služby, softwarové i hardwarové prostředky nesmějí být přímo použity v návrhu řešení mimo využití těch, které již Platforma SŽ poskytuje.

Pro některé případy výběrových řízení pro aplikační software je přípustné použití tzv. zapouzdřených technologií, jež nejsou součástí Platformy SŽ, ale nabízené řešení vyžaduje jejich nasazení. Zapouzdřená technologie je zpravidla součástí jiné primární technologie jako tzv. podpůrný program. Takový program nevyžaduje samostatnou instalaci, jelikož je instalován jako součást dané komponenty.

Použití takových zapouzdřených technologií je možné jen v následujících případech:

1. Jejich použití nebude klást žádné dodatečné provozní, finanční ani implementační nároky po celou dobu životnosti primární technologie.
2. Nebudou vyžadovat žádné dodatečné licence nad rámec licencí hlavního dodávaného řešení.
3. Aktualizace zapouzdřených technologií bude probíhat pouze současně s aktualizací hlavního dodávaného řešení.
4. Jejich podpora bude poskytována současně a ve stejném rozsahu jako podpora hlavního dodávaného řešení.
5. Zapouzdřené technologie nebudou vyžadovat žádné speciální provozní podporu, ze strany Správy železnic.
6. Zapouzdřené technologie jsou v souladu se standardy kybernetické bezpečnosti (ZoKB, VoKB).

Při použití zapouzdřených technologií je nutné danou technologii identifikovat nejméně v následujícím rozsahu – Název, Verze, Výrobce, Licence, Termín a úroveň podpory.

7 Přílohy Platformy SŽ

Jednotlivé oblasti jsou dále detailně zpracovány v těchto přílohách:

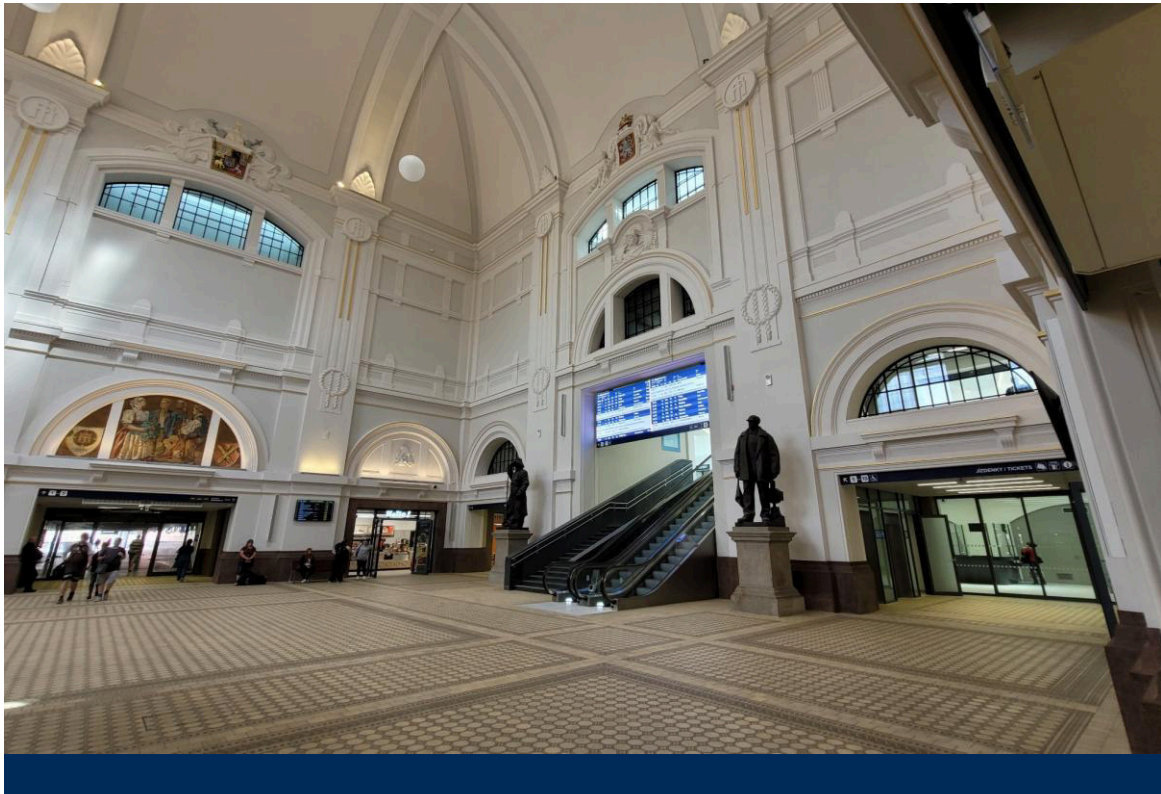
- Příloha 1 – Standardy softwarového vývoje
- Příloha 2 – Datová centra a serverovny
- Příloha 3 – Virtuální prostředí, serverové farmy a servery
- Příloha 4 – Konektivita a síťové prostředí
- Příloha 5 – Integrovaní standardy
- Příloha 6 – Komunikační standardy
- Příloha 7 – Standardy zálohování a disaster recovery
- Příloha 8 – Cloudové prostředí

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Standardy vývoje software

Červen 2025

Obsah

1	Úvod	5
2	Standardy vývoje informačních systémů Správy železnic	5
2.1	Prostředí	5
2.1.1	Vývojové prostředí	5
2.1.2	Testovací prostředí	5
2.1.3	Produkční prostředí	5
2.2	Dvouvrstvá architektura	5
2.2.1	Datová vrstva	6
2.2.2	Aplikační vrstva	6
2.3	Třívrstvá a vícevrstvá architektura	6
2.3.1	Datová vrstva	6
2.3.2	Aplikační vrstva	7
2.3.3	Prezentační vrstva	7
2.3.4	Integrační vrstva	7
2.4	Požadavky na prezentační vrstvu	8
2.4.1	Uživatelské rozhraní	8
2.4.2	Uživatelská zkušenost	8
2.5	Bezpečnost	9
2.5.1	Zabezpečení aplikací	9
2.5.2	Autentizace a autorizace	10
2.5.3	Zpracování osobních údajů	11
2.6	Dokumentace	11
2.6.1	Technická dokumentace jádra systému	11
2.6.2	E-R modely databáze	11
2.6.3	Objektový model pro aplikace	11
2.6.4	Procesní diagramy, schémata toků dat	11
2.6.5	Komunikační rozhraní	11
2.6.6	Drátové modely všech obrazovek uživatelského rozhraní aplikací	11
2.6.7	Popis konfigurace provozního prostředí	12
2.6.8	Uživatelská příručka	12
2.6.9	Příručka administrátora	12
2.6.10	Disaster Recovery postup (D/R Postup)	12
2.7	Modelování EA architektury	12
2.8	Předávání vývoje do provozu	12

Seznam zkratek

2FA	Dvou-faktorové ověření (<i>Two-Factor Authentication</i>)
3NF	Třetí normální forma návrhu tabulek databází řeší tranzitivní závislosti v rámci návrhu tabulek databází
DDL	(<i>Data Definition Language</i>)
EA	Podniková architektura (<i>Enterprise Architecture</i>)
GDPR	GDPR neboli Obecné nařízení o ochraně osobních údajů je zákon Evropské unie, který byl přijat v roce 2016 a začal platit v květnu 2018. GDPR upravuje ochranu osobních údajů občanů EU a stanovuje pravidla pro sběr, zpracování, uchování a předávání osobních údajů. Cílem GDPR je posílit ochranu osobních údajů a zvýšit kontrolu občanů nad jejich údaji. V ČR je implementován zákonem o zpracování osobních údajů č. 110/2019 Sb. (<i>General Data Protection Regulation</i>)
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
IT	Informační technologie (<i>Information Technology</i>)
LDAP	(<i>Lightweight Directory Access Protocol</i>)
MFA	Více-faktorové ověření identity uživatele (<i>Multi-Factor Authentication</i>)
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
SAP	Modulární ERP systém od německé firmy SAP AG
SOA	Architektura orientovaná na služby – jedná se o softwarovou architekturu, která se zaměřuje na organizaci a strukturu aplikací a systémů jako soubor nezávislých a dobře definovaných služeb (<i>Service-Oriented Architecture</i>)
SQL	Standardní jazyk pro manipulaci s relačními databázemi. SQL umožňuje ukládat, manipulovat a vyhledávat data v relačních databázích. SQL je založeno na dotazech (queries) na data v databázích. Dotazy lze pak definovat a modifikovat strukturu databází, vytvářet a upravovat tabulky, indexy a další prvky, vkládat a aktualizovat data, mazat data a další operace. SQL je nezávislý na platformě, což znamená, že může být použit na různých operačních systémech a s různými databázovými systémy, avšak každá databázová platforma může mít různé změny v syntaxi (<i>Structured Query Language</i>)
SSO	(<i>Single Sign-On</i>)
SW	Programové vybavení počítače či jiného obdobného zařízení. Speciálním druhem software je <i>firmware</i> , který je úzce spjatý s konkrétním hardwarem (<i>Software</i>)
SŽ	Správa železnic, státní organizace
SŽT	Správa železniční telematiky, organizační jednotka SŽ
UI	(<i>User Interface</i>)
UNICODE	Univerzální kódování znaků s možností reprezentace všech národních znakových sad
UX	(<i>User Experience</i>)
VoKB	Vyhláška o kybernetické bezpečnosti č. 82/2018 Sb.
ZoKB	Zákon o kybernetické bezpečnosti č. 181/2014 Sb.
ZZOU	Zákon o zpracování osobních údajů č. 110/2019 Sb.

Seznam vysvětlivek

E-R model

(Entity-Relationship model)

Platforma SŽ

Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.

1 Úvod

Cílem tohoto dokumentu je definovat Platformu SŽ, jakožto souhrn podporovaných infrastrukturních služeb, technologií, a architektonických principů, která definuje základní rámec pro návrh řešení ICT. Platforma SŽ naplňuje strategické cíle IS/ICT SŽ, zejména v oblasti efektivního provozu a rozvoje ICT prostředí Správy železnic.

2 Standardy vývoje informačních systémů Správy železnic

Při vývoji software ve Správě železnic je požadováno, aby byly plně respektovány obvyklé metodiky a „best-practice“ pro návrh a vývoj software pomocí vícevrstvé architektury. Konkrétní užití jednotlivých vzorů se řídí vhodností, plánovanou zátěží a požadavky na dostupnost vyvíjeného software.

Aplikace či informační systém musí vždy podporovat škálování výkonu, redundanci a více-jádrové serverové systémy bez ohledu na zvolenou architekturu řešení.

2.1 Prostředí

Vývoj software, jeho testování i produkční nasazení musí probíhat v oddělených vzájemně se neovlivňujících prostředích.

2.1.1 Vývojové prostředí

Vývoj ve vývojovém prostředí (DEV) probíhá zpravidla u dodavatele. V prostředí Správy železnic probíhá vývoj v odůvodněných případech. Vývoj software současně využívá zcela oddělené instance databází a plně anonymizovaná data.

2.1.2 Testovací prostředí

Testování probíhá v testovacím prostředí (TEST) v prostředí Správy železnic. Mimo prostředí Správy železnic probíhá testování jen v odůvodněných případech. Při testování se používají zcela oddělené instance databází a plně anonymizovaná data. Testovací prostředí musí co nejdříve simulovat produkční prostředí, včetně konfigurace a objemu dat, aby případné chyby a nedostatky byly zachyceny ještě před nasazením změn do ostrého provozu.

2.1.3 Produkční prostředí

Po úspěšně akceptovaném testování je možné software přenést do ostrého produkčního prostředí (PROD) v prostředí Správy železnic. V případě software poskytovaného jako SaaS lze využít i cloudové prostředí Správy železnic nebo v odůvodněných případech i prostředí dodavatele.

2.2 Dvouvrstvá architektura

Dvouvrstvou architekturu při vývoji software lze využít v případě, kdy se jedná o menší, samostatný software, který nebude integrován na další informační systémy, nebo datové zdroje Správy železnic. Užití takového software je plánováno pro menší desítky uživatelů, bez požadavku na vysokou dostupnost a možnosti škálování výkonu a rozložení zátěže prostřednictvím clusterování. U tohoto typu software nejsou definovány požadavky na vysokou odolnost proti chybám, rychlou reakci systému, nebo správu dat pro velké sítě.

Využití dvouvrstvé architektury musí být předem diskutováno s Oddělením IT architektury, které v odůvodněných případech vydá příslušnou výjimku.

2.2.1 Datová vrstva

Realizace datové vrstvy je požadována prostřednictvím preferované relační databáze (dle služeb Platformy SŽ) a respektováním metodiky 3NF. Je požadován jednoznačný datový model s minimální redundancí dat a datové struktury budou modelovány a popsány jazykovými konstrukcemi DDL, které jsou kompatibilní s určeným databázovým systémem.

Celá struktura dat bude popsána formálně prostředky E-R modelování. K datovému modelu je požadováno dodat korespondující SQL DDL skripty, který budou plně odpovídat dodané databázi. Je požadováno, aby správnost, úplnost a optimalizace datového modelu byla řešena již v rámci návrhu řešení.

V rámci dvouvrstvé architektury je umožněno, aby logika byla rozprostřena částečně v databázi a částečně v aplikační, resp. prezentační vrstvě.

2.2.2 Aplikační vrstva

Aplikační vrstva a prezentační vrstva je ve dvouvrstvé architektuře realizována jako jedna, společná a nedělitelná vrstva. Je požadováno, aby tato vrstva byla realizována v souladu s principy objektově orientovaného programování a komunikace mezi vrstvami byla realizována standardními zabezpečenými a šifrovanými protokoly. Je požadováno, aby uživatelské identity nebyly z aplikační vrstvy prezentovány do datové vrstvy, přičemž tyto vrstvy musí mezi sebou komunikovat technickým účtem, k tomu účelu v databázi vytvořeném.

Je požadováno, aby aplikační vrstva podporovala Multitasking, tedy umožňovala provádění několika procesů současně a systém byl již v rámci návrhu a vývoje optimalizován plánovaný výkon.

V rámci vývoje musí být ošetřena všechna bezpečnostní rizika popsaná v kapitole 2.5.

2.3 Třívrstvá a vícevrstvá architektura

Třívrstvá a vícevrstvá architektura je požadována při vývoji software ve všech případech, mimo výjimek uvedených v kapitole 2.1 nebo pokud není v zadávací dokumentaci VZ specifikováno jinak. Specifikace řešení vyžadující třívrstvou architekturu tak může disponovat následujícími vlastnostmi:

- Má být integrován na jiný software Správy železnic, nebo software třetích stran, a to z důvodu jednotného přístupu k datům a procesům vyvíjeného software
- Je plánováno využití pro větší počty uživatelů
- Je požadována vysoká dostupnost (HA)
- Je požadován Clustering pro rozložení zátěže a škálování výkonu
- Je požadována vysoká odolnost proti chybám, rychlá reakce systému, nebo správa dat pro velké sítě

2.3.1 Datová vrstva

Realizace datové vrstvy je primárně požadována prostřednictvím relační databáze nabízené Platformou SŽ, avšak pokud dodavatel navrhne jiné řešení (např. objektovou databázi či NoSQL), je povinen toto řešení zahrnout do své ceny implementace a provozu IS. Tento přístup zohledňuje různé typy úloh, kde využití relační databáze nemusí být vždy optimální.

Datový model musí být jednoznačný, s minimální redundancí dat, a datové struktury budou modelovány a popsány jazykovými konstrukcemi DDL, kompatibilními s určeným databázovým systémem. Formální popis celé struktury dat bude realizován prostředky E-R modelování, přičemž je možné povolit také objektový model, například formou diagramu tříd. K datovému modelu je nutné dodat odpovídající SQL DDL skripty, které plně reflektují implementovanou databázi. Důraz je kladen na to, aby správnost, úplnost a optimalizace datového modelu byly zajištěny již ve fázi návrhu řešení.

V rámci třívrstvé nebo vícevrstvé architektury není přípustné, aby logika byla rozdělena mezi databázi a aplikační vrstvu. Veškerá aplikační logika musí být umístěna výhradně v aplikační vrstvě.

2.3.2 Aplikační vrstva

Je požadováno, aby tato vrstva byla realizována v souladu s principy objektově orientovaného programování a komunikace mezi vrstvami byla realizována standardními zabezpečenými a šifrovanými protokoly. Je požadováno, aby uživatelské identity nebyly z aplikační vrstvy prezentovány do datové vrstvy, přičemž tyto dvě vrstvy musí mezi sebou komunikovat technickým účtem, k tomu účelu v databázi vytvořeném.

Je požadováno, aby aplikační vrstva podporovala Multitasking, tedy umožňovala provádění několika procesů současně a v již rámci návrhu a vývoje optimalizovat plánovaný výkon.

V rámci vývoje musí být ošetřena všechna bezpečnostní rizika popsaná v kapitole 2.5.

2.3.3 Prezentační vrstva

Pro interakci s uživatelem je požadováno, aby prezentační vrstva byla realizována desktopovým klientem (tlustým), nebo webovým klientem (tenkým), a to v závislosti na vhodnosti použití a požadavcích na software kladených. Komunikace mezi prezentační a aplikační vrstvou musí být realizována standardními zabezpečenými a šifrovanými protokoly.

V rámci prezentační vrstvy a desktopového klienta je možné přenesením části aplikační logiky na klienta, tedy využití prostředků klientské stanice ke zvýšení výkonu systému, ale pouze za předpokladu, že tento systém bude zabezpečovat konzistenci aplikační logiky, napříč všemi desktopovými klienty.

Bez aktualizčních mechanismů, které zajistí stejné verze software, na všech klientských stanicích v reálném čase není tato možnost povolena.

2.3.4 Integrační vrstva

V případě, kdy vyvíjený software má být integrován na jiný software Správy železnic, nebo software třetích stran, je požadováno, aby tato integrační vrstva byla realizována jako samostatná vrstva, umožňující škálování výkonu a rozložení zátěže.

Realizace integrací mezi aplikačními komponentami musí splňovat principy SOA. Veškerá komunikace tedy musí probíhat prostřednictvím definovaných služeb rozhraní, a není tedy povolena výměna dat prostřednictvím přímých vazeb, jako je sdílení paměti, souborů, nebo databází. Pokud je k dispozici, komunikace probíhá prostřednictvím k tomu určené sběrnice (ESB) nebo integrační platformy.

V případě, že má být vyvíjená komponenta integrována se **spisovou službou SŽ**, musí splňovat požadavky na integraci prostřednictvím Národního standardu pro elektronické systémy spisové služby¹ a integrace musí být rozhraními definovanými v tomto standardu také realizována.

V případě, že má být vyvíjená aplikace integrována s programovým prostředím komponent **systému SAP**, musí být realizována prostřednictvím určené integrační platformy (SAP Cloud Platform, příp. produktu, který jej nahradí). Detailní parametry požadavku na integraci budou definovány v příslušných případech.

Bez ohledu na zvolenou architekturu je zásadní klást důraz na kvalitní návrh a plánování celého řešení před zahájením implementace. Pečlivě promyšlený architektonický návrh výrazně snižuje riziko pozdějších problémů a nákladných úprav. Všechny požadované funkcionality by

¹ NSESSS, <https://www.mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx>

proto měly být detailně navrženy a prověřeny již před implementací, čímž se předejde nutnosti dodatečně přepisovat nevhodně navržené části řešení. Zároveň je vhodné navrhovat systém modulárně s jasně definovanými komponentami a rozhraními. Oddělení jednotlivých funkčních celků zvyšuje soudržnost kódu a usnadňuje testování i budoucí údržbu.

Již v rámci architektonického návrhu je nutné zohlednit také bezpečnostní požadavky (např. způsob autentizace uživatelů, řízení oprávnění) a celkovou spolehlivost systému. Do návrhu je vhodné začlenit mechanismy pro ošetření chyb a podrobné logování, stejně jako podporu monitorování aplikace, aby bylo možné provozní problémy rychle detekovat a diagnostikovat. Před finálním schválením architektury by měl návrh projít revizí. Konečná podoba architektury musí být srozumitelná všem zainteresovaným stranám, což usnadní spolupráci při implementaci i následné řešení incidentů.

2.4 Požadavky na prezentační vrstvu

2.4.1 Uživatelské rozhraní

Pomocí uživatelského rozhraní může uživatel komunikovat se zařízením, počítačem a programy. Při navrhování vysoce kvalitního uživatelského rozhraní je požadováno zohlednit nejen vzhled rozhraní, ale také jeho logickou strukturu, aby s ním uživatel mohl snadno a rychle komunikovat a dosáhnout požadovaného výsledku bez zbytečného úsilí. Cílem je vytvořit rozhraní, které poskytuje jednoduchou, srozumitelnou a pohodlnou interakci uživatele s informačním systémem.

Pro návrh UI informačních systémů SŽ platí následující zásady:

- standardní ovládací prvky
- uživatelské rozhraní jednoduché a přehledné
- konzistentní prostředí
- účelné rozvržení obrazovek
- aplikace musí podporovat světlý i tmavý režim dle nastavení operačního systému a současně nastavení režimu nezávisle na nastavení operačního systému
- barvy a písma dle grafického manuálu
- hierarchie daná typograficky
- informování uživatele, co systém právě dělá
- odpovídající tvar a velikost ovládacích prvků
- kódování znaků UNICODE
- datumové položky dle českého standardu „DD.MM.RRRR“
- jednotný vizuální styl (pro některé projekty dle korporátní identity)
- webové aplikace musí mít responzivní design přizpůsobený určeným zařízením koncových uživatelů

2.4.2 Uživatelská zkušenost

Uživatelská zkušenost je to, co uživatel pocítí a pamatuje si v důsledku použití aplikace, systému nebo webu. UX formuje uživatelské chování a musí plnit požadavky uživatelů na danou aplikaci či webovou stránku. UX musí být bráno v úvahu při vývoji uživatelského rozhraní, vytváření informační architektury a testování použitelnosti informačních systémů SŽ. Po určení cílového publika a charakteristiky uživatelů je požadováno vytvořit seznam UX požadavků na projekt.

UX informačních systémů SŽ musí splňovat následující vlastnosti:

- usnadnění/zefektivnění práce uživatele
- návodné ovládání
- ergonomie
- jednoduché, intuitivní
- pravidla přístupnosti, tam kde je požadováno
- zobrazování relevantních a požadovaných dat

- doba zpracování požadavku na serveru by neměla přesáhnout 0,5 sekundy, aby celková doba odezvy uživatelských prvků byla kratší než 0,8 sekundy. Pokud bude předpokládaná doba odezvy delší než 0,8 sekundy, ale kratší než 2 sekundy, zobrazí se uživateli čekací kurzor. V případě, že doba odezvy přesáhne 2 sekundy, bude uživateli zobrazen indikátor průběhu operace (progress bar) pro lepší informovanost o stavu zpracování
- použít lazy loading tak, aby uživatel měl co nejrychlejší odezvu
- jednotná terminologie v celém systému
- ne všechno na jedné obrazovce
- ne všechno v rozbalovacím menu (příliš mnoho položek)
- navigace, kde se uživatel v aplikaci nachází
- minimalizace použití dlouhých textů
- vhodné využití grafických a obrazových prvků
- nepoužívat drobný text
- pečlivé plánování dialogů (logické skupiny)
- ne překrývající se dialogy
- jednotné, stejné ovládací prvky v dialozích na stejných místech s popisky s jednotnou terminologií

2.5 Bezpečnost

Všechny vyvíjené aplikace musejí splňovat požadavky kladené platnou legislativou. Požadovaný je také soulad s NÚKIB (Bezpečný vývoj aplikací).

Z pohledu požadavků na vyvíjený software je nutné zajistit oblasti:

- Zálohování a obnova
- Bezpečnost komunikací
- Řízení přístupu
- Ochrana před škodlivým kódem
- Logování a monitoring
- Bezpečné předávání a výměna informací
- Akvizice, vývoj a údržba

2.5.1 Zabezpečení aplikací

Je požadováno, aby jednotlivé vrstvy splňovaly minimálně tyto požadavky:

- Ke komunikaci mezi jednotlivými vrstvami je používán systémový účet, který lze v případě ohrožení kybernetické bezpečnosti deaktivovat, nebo změnit.
- Systémový účet, který je využíván ke komunikaci mezi vrstvami není privilegovaným účtem.
- Všechny vrstvy jsou ošetřeny proti nejzávažnějším bezpečnostním rizikům jako jsou²:
 - Injection
 - Broken Authentication
 - Sensitive Data Exposure
 - XML External Entities (XXE)
 - Broken Access Control
 - Security Misconfiguration
 - Cross-Site Scripting (XSS)
 - Insecure Deserialization
 - Using Components with Known Vulnerabilities
 - Insufficient Logging&Monitoring
- Jednotlivé vrstvy uchovávají své konfigurační parametry v šifrované podobě.

K zajištění bezpečnosti již během samotného vývoje je požadováno zavést a důsledně dodržovat jednotné standardy psaní kódu. Jasně definovaný styl psaní kódu (názvosloví, formátování, ošetření výjimek, validace vstupů apod.) zajistí konzistentní kvalitu kódu napříč vývojovým týmem a pomáhá předcházet chybám včetně bezpečnostních zranitelností.

² Dle aktuálního seznamu nejzávažnějších bezpečnostních rizik definovaných OWASP (<https://owasp.org/>).

Dodržování těchto standardů je potřeba průběžně ověřovat pomocí automatizovaných nástrojů, které dokáží odhalit porušení konvencí nebo potenciálně rizikové konstrukce již v rané fázi vývoje.

Neméně důležitou součástí procesu vývoje je pravidelná revize kódu prováděná druhým vývojářem před sloučením změn do hlavní vývojové větve. Uplatnění principu „čtyř očí“ pomáhá odhalit chyby a nedostatky ještě před nasazením do produkce a ověřit dodržování stanovených standardů i architektonických principů. Každý podstatný zásah do kódu proto musí projít nezávislou kontrolou, aby se do produkčního prostředí dostal pouze prověřený kód odpovídající požadované kvalitě.

Aplikace musí důsledně logovat všechny podstatné události v systému. Zejména veškeré administrátorské akce, změny konfigurací nebo zásadních oprávnění a přístupy k citlivým datům musí být zaznamenány v auditních záznamech s informací o tom, kdo a kdy danou operaci provedl.

Logy je doporučeno centralizovat pomocí nástroje typu SIEM, což umožní efektivní vyhledávání a detekci podezřelých aktivit a vytvoření ucelené auditní stopy pro potřeby bezpečnostních kontrol či vyšetřování incidentů. Je zároveň nezbytné zajistit integritu a důvěrnost těchto záznamů – přístup k nim smí mít pouze pověřené osoby a úložiště logů musí být chráněno proti neoprávněným zásahům.

2.5.2 Autentizace a autorizace

2.5.2.1 Autentizace

Autentizace je proces ověření proklamované identity subjektu. Je požadováno, aby aplikace umožňovala následující typy autentizace:

- SSO (Single Sign-On), autentizaci pomocí protokolu Kerberos, nebo OpenID proti Active Directory
- Autentizaci pomocí protokolu LDAP, proti Active Directory
- Řešení 2FA či MFA

Zvláště u kritických systémů a všech privilegovaných účtů je požadováno použití silné MFA autentizace. Tento přístup výrazně snižuje riziko neoprávněného přístupu v případě prozrazení hesla.

Manuální přihlášení a autentizaci pomocí vyvíjeného software (uživatelská jména a hesla jsou uložena v databázi v šifrované podobě) je možné jen na základě schválené výjimky Odborem IT architektury SŽT.

2.5.2.2 Autorizace

Je požadováno, aby vyvíjený software obsahoval vlastní autorizační modul, který bude minimálně umožňovat:

- Vytváření uživatelských účtů
- Vytváření rolí
- Přidělování jednotlivých uživatelských účtů k rolím
- Přidělování konkrétních oprávnění na role

Kromě uvedené funkčnosti je nutné v rámci správy přístupů důsledně uplatňovat princip minimálních oprávnění. Každému uživateli se přidělují pouze taková práva, která nezbytně potřebuje k výkonu své role – nic víc. Správa privilegovaných účtů (administrátorů apod.) vyžaduje zvýšenou pozornost: každý administrátor musí používat svůj vlastní individuální účet s vyššími právy (nesmí se využívat sdílené ani výchozí „Administrator“ účty) a počet těchto účtů je třeba omezit na nezbytné minimum. Je nutné pravidelně prověřovat používání privilegovaných účtů a okamžitě odebrat přístupy, které již nejsou nutné. Zároveň platí striktní oddělení odpovědností – žádná jednotlivá osoba by neměla mít plnou a nekontrolovanou správu kritického systému bez kontroly další osoby.

Pro zvýšení bezpečnosti privilegovaných přístupů jsou tyto řízeny nástroji PAM (Privileged Access Management). Tyto nástroje umožňují například dočasné udělení administrátorských oprávnění na nezbytně nutnou dobu (princip „just-in-time“), bezpečné uložení a

automatizovanou obměnu hesel privilegovaných účtů a detailní monitorování akcí prováděných administrátory.

V rámci naplnění povinností vyplývajících ze ZoKB a VoKB je požadováno, aby vyvíjený software umožňoval správu uživatelů a rolí pomocí externího nástroje na řízení identit. Integrace mezi vyvíjeným softwarem a Identity management bude realizována prostřednictvím integrační vrstvy vyvíjeného software.

2.5.3 Zpracování osobních údajů

Je požadováno kompletní splnění všech požadavků na zpracování osobních údajů dle zákona o zpracování osobních údajů č. 110/2019 Sb. (GDPR). Analýza a návrh opatření musí být řešen již v rámci návrhu řešení.

2.6 Dokumentace

Veškerá dokumentace musí být průběžně aktualizována při každé podstatné změně systému. Aktualizace příslušných dokumentů je nedílnou součástí dokončení každé vývojové etapy/milníku. Zastaralé nebo neúplné informace v dokumentaci mohou vést k nesprávným rozhodnutím a chybám při provozu či dalším vývoji systému.

Dokumentaci je zároveň nutné udržovat snadno dostupnou všem členům týmu i dalším zainteresovaným stranám (sdílený repozitář). Dobře strukturované a přehledné dokumentační výstupy usnadňují spolupráci v týmu a zaučování nových členů. Zároveň slouží jako spolehlivý zdroj informací při řešení incidentů a plánování změn, což přispívá k vyšší kvalitě a stabilitě dodávaného software.

Je požadováno, aby součástí dodávky vyvíjeného software byla dokumentace, a to minimálně v rozsahu:

2.6.1 Technická dokumentace jádra systému

Dokumentace jádra systému, jeho funkcí, služeb a rozhraní. Dokumentace bude obsahovat kompletní popis architektury jádra systému, výčet a podrobný popis všech jeho funkcí, přehled a popis služeb, které jádro poskytuje dalším komponentám systému, modulům a knihovnám.

2.6.2 E-R modely databáze

Kompletní dokumentace ve formě E-R schémat pro všechny implementované databáze včetně korespondujících DDL SQL skriptů.

2.6.3 Objektový model pro aplikace

Dokumentace obsahující objektové modely všech funkcí, jejich komponent, modulů, vztahů.

2.6.4 Procesní diagramy, schémata toků dat

Dokumentace obsahující procesní diagramy a mapu všech toků dat celého řešení.

2.6.5 Komunikační rozhraní

Dokumentace všech typů komunikačních rozhraní, všech jejich registrovaných služeb a všech funkcí, struktur dat a vlastností těchto služeb.

2.6.6 Drátové modely všech obrazovek uživatelského rozhraní aplikací

Dokumentace všech částí software musí obsahovat drátové modely všech obrazovek UI včetně popisu funkcí prvků každé obrazovky.

2.6.7 Popis konfigurace provozního prostředí

Dokumentace musí obsahovat soupis všech požadavků na nastavení hardwarových a softwarových komponent běhového prostředí jako jsou:

- mapování souborových systémů
- požadavky na operační paměť a počty jader
- konfigurační parametry jednotlivých podpůrných SW prostředků (např. specifika pro nastavení databáze, aplikačního serveru, webového serveru, apod.)

2.6.8 Uživatelská příručka

Příručka bude distribuována uživatelům. Musí obsahovat kompletní popis všech uživatelských funkcí pro práci se software. Příručka bude využívána jako základní materiál pro školení nových uživatelů. Příručka musí obsahovat kvalitně a jednoznačně zpracovaný popis kroků pro jednotlivé implementované funkce s vhodným doprovodným obrazovým materiálem ve formě výřezů obrazovek. Musí být napsána v českém jazyce a před finálním odevzdáním zpracovaná jazykovým korektorem.

2.6.9 Příručka administrátora

Příručka bude distribuována úzké skupině uživatelů, administrátorům systému. Musí obsahovat kompletní popis všech funkcí pro práci s administrací software. Příručka bude využívána jako materiál pro školení nových administrátorů. Příručka musí obsahovat kvalitně a jednoznačně zpracovaný popis kroků pro jednotlivé implementované funkce s vhodným doprovodným obrazovým materiálem ve formě výřezů obrazovek. Musí být napsána v českém jazyce a před finálním odevzdáním zpracovaná jazykovým korektorem.

2.6.10 Disaster Recovery postup (D/R Postup)

Dokumentace Disaster Recovery postupu bude obsahovat kompletní plán pro obnovu klíčových systémů a dat v případě mimořádné události nebo havárie. Tento plán bude zahrnovat podrobný popis zálohovacích strategií, metod obnovy, a kroků nutných pro minimalizaci výpadků a rychlou obnovu provozu. Dokumentace bude sloužit jako základní materiál pro školení týmů odpovědných za implementaci a správu obnovovacích procesů.

2.7 Modelování EA architektury

Každý Dodavatel je povinen řádně dokumentovat dodávané řešení v podobě modelu Enterprise Architektury. V rámci SŽ je využíván jako modelovací nástroj SPARX Enterprise Architect ve verzi 16 a notace Archimate 3.2.

Za účelem udržení kompatibility všech vytvářených modelů má SŽ vytvořený přehled povolených elementů pro jednotlivé vrstvy, včetně popisu jejich charakteristik a povinných atributů (závaznou metodiku tvorby a údržby EA modelů). Dodavatel může doplnit další elementy, jejich schválení však podléhá Odboru IT architektury SŽT.

Modelování bude realizováno na repozitory SŽ, kam bude Dodavateli vytvořen přístup za účelem možnosti sdílet vytvořené prvky a jejich definované vazby, tak aby byla zachována kompatibility.

Hlavním schvalovatelem předkládaných modelů je Odbor IT architektury SŽT.

2.8 Předávání vývoje do provozu

Pokud nebude určeno jinak, veškeré výstupy (zdrojové kódy, konfigurační soubory, testovací data, dokumentace atp.) musejí být předávány prostřednictvím určeného repositáře. Bez předání kompletní dokumentace nelze danou aplikaci či informační systém považovat za bezchybný a akceptovatelný v rámci procesu akceptace.

Pro bezproblémové nasazování nových verzí do provozu se doporučuje využívat metodiky Continuous Integration/Continuous Deployment (CI/CD). Každá změna zdrojového kódu by

měla projít automatizovaným procesem sestavení a sadou testů v rámci CI pipeline, aby se zamezilo proniknutí chyb do produkční verze. Před ostrým nasazením nové verze je zároveň nutné nasadit ji nejprve do testovacího prostředí, které věrně kopíruje produkční podmínky, a ověřit v něm bezchybnou funkčnost systému.

Pro nasazování do produkčního prostředí je požadována co největší automatizace, aby se vyloučila rizika plynoucí z ručních zásahů a byl zajištěn opakovatelný proces. Pro každý release musí existovat předem připravený a otestovaný postup pro rychlé navrácení systému k předchozí funkční verzi v případě, že se po nasazení vyskytnou závažné problémy. Každé nasazení je zároveň nutné řádně logovat a verzovat, aby byl k dispozici přesný záznam o nasazené verzi a provedených změnách.

Po nasazení nové verze do produkce je nezbytné aktivně monitorovat její provoz. Centrální dohled nad logy aplikace a klíčovými metrikami umožní týmu včas odhalit případné problémy a rychle na ně reagovat. Doporučuje se nastavit notifikace (např. e-mailové alerty) pro případ selhání některé z funkcionalit, aby odpovědné osoby byly neprodleně informovány o vzniklých chybách. Doporučuje se využít verzovací systém k uchování kompletní historie všech změn i nasazení včetně identifikace autorů a popisů, což zajistí plnou sledovatelnost a usnadní následné audity.

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Datová centra a serverovny

Červen 2025

Obsah

1	Úvod	4
2	Datová centra	4
2.1	Datové centrum CDP Praha	4
2.2	Datové centrum CDP Přerov	5
3	Serverovny	5
3.1	Významné serverovny	5
3.2	Serverovny dle geografických oblastí.....	5
3.3	Serverovny vybraných organizačních jednotek.....	5
3.4	Technologické serverovny	5
3.5	Technologické a sdělovací místnosti	5
4	Technologické vybavení	5
4.1	Stavební provedení	6
4.2	Napájení	6
4.3	Chlazení.....	6
4.4	Bezpečnost	7
4.5	Síťová infrastruktura	7
4.6	Ostatní vybavení	7

Seznam zkratek

ASHS	Stabilní hasicí zařízení, běžně se označuje i zkratkou SHZ a zpravidla bývá na bázi vodních sprinklerů nebo směsi inertních plynů, které jsou ekologicky neškodné
CDP	Centrální dispečerské pracoviště v kontextu organizační struktury SŽ (CDP Praha, CDP Přešov)
EPS	Technologie pro detekci a signalizaci požáru v budovách. Systém EPS zahrnuje detektory požáru, které jsou umístěny v různých částech budovy a slouží k detekci ohně nebo kouře. Detektory jsou připojeny k řídicí jednotce, která sbírá a analyzuje data z detektorů a rozhoduje, zda má být spuštěna alarmová signalizace. Systémy EPS mohou být konfigurovány pro přenos informací o požáru na centrální monitorovací stanice nebo na místní hasičské sbory, aby byla zajištěna rychlá reakce a minimalizovány škody a ztráty na životech (<i>Elektronická požární signalizace</i>)
EZS	Technologie pro ochranu majetku, budov a objektů před neoprávněným vstupem a krádežemi. EZS zahrnuje detektory pohybu, otvírání dveří a oken, kamerové systémy, zabezpečovací panely a další zařízení pro monitorování a signalizaci neoprávněného vstupu nebo pokusů o krádež (<i>Elektronická zabezpečovací signalizace</i>)
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
IT	Informační technologie (<i>Information Technology</i>)
OJ	Organizační jednotka SŽ
OŘ	Oblastní ředitelství SŽ
OT	Provozní technologie (<i>Operations Technology</i>)
SŽ	Správa železnic, státní organizace
TIER	Klasifikace datových center dle Uptime Institute. Datová centra se pak označují jako TIER 1 (nejnižší zabezpečení) až TIER 4 (nejvyšší zabezpečení)
UPS	Zdroj nepřerušovaného napájení je zařízení, které zajišťuje souvislou dodávku elektrické energie pro spotřebiče, které nesmějí být neočekávaně vypnuty (<i>Uninterruptible Power Supply</i>)

Seznam vysvětlivek

Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.
---------------------	--

1 Úvod

Cílem této části Platformy SŽ je, dle kategorizace datových center a serveroven v prostředí Správy železnic, definovat technické požadavky na jejich výstavbu a s tím související popis používaných technologií v datových centrech, serverovnách a technologických místnostech. Současně dokument slouží jako popis fyzického ICT prostředí, kde jsou provozovány ICT technologie a provozovány informační systémy.

Z pohledu ICT infrastruktury jde o lokality, kde jsou umístěny zpravidla serverové technologie pro provoz aplikací a podpůrných systémů, technologie datových spojů, telefonie a další. Může zde být umístěna i technika externích dodavatelů či napojení na kritické podpůrné systémy externích subjektů (HZS ČR, PČR, ČEZ).

Datová centra jsou obecně definována jako samostatné budovy sloužící výhradně pro provoz ICT infrastruktury. Z pohledu provozu a dostupnosti jsou pak kategorizována hodnotami TIER. Kategorizace mimo jiné zohledňuje redundanci napájení, chlazení, konektivity, fyzické zabezpečení a technologické vybavení samotných prostor. Vše je následně přepočteno na nominální dostupnost v procentech za jeden rok (viz ukazatel TIER).

Serverovny jsou pak definovány obdobně jako datová centra, jen již není požadována vyhrazená samostatná budova, ale běžně bývají součástí administrativních či provozních a technologických budov. Většina menších serveroven, technologických a sdělovacích místností ve Správě železnic vznikla přebudováním stávajících místností v příslušné budově.

Tabulka 1. Rozdělení DC a serveroven dle velikosti a významu

Dat centrum / serverovna / rack	Počet rackových skříní	Kritické aplikace	Serverová infrastruktura	Redundance (napájení, chlazení, konektivita)
Datové centrum	10-200+	ANO	ANO	ANO
Významná serverovna	6-25	ANO	ANO	ANO
Menší serverovna	4-16	ČÁSTEČNĚ	ANO	ČÁSTEČNĚ
Lokální serverovna	1-8	NE	ČÁSTEČNĚ	NE
Technologické místnosti	1-5	NE	ČÁSTEČNĚ	NE
Sdělovací místnosti	1-6	NE	NE	NE
Samostatné rackové skříně v budovách	1-3	NE	NE	NE

Výstavba a projektování datových center a serveroven je standardizována v souboru norem **ČSN EN 50600** a fyzické zabezpečení datových center je dále interně ve Správě železnic specifikováno ve směrnici **SM07** a jejích přílohách.

2 Datová centra

Správa železnic disponuje dvěma datovými centry, kde jsou umístovány technologie jak IT, tak OT. Tato datová centra jsou součástí technologických řídicích center, odkud je dálkově řízen železniční provoz.

2.1 Datové centrum CDP Praha

Jedná se o primární datové centrum Správy železnic, které zajišťuje běh velkého počtu provozovaných informačních systémů a aplikací. V datovém centru jsou v samostatných sálech umístěny IT technologie i páteřní prvky celorepublikových sítí a rozsáhlé zařízení OT. Objekt je vně i uvnitř zabezpečen v souladu s běžnými standardy i interními směrnici.

Z technologického pohledu je zajištěno redundantní chlazení i napájení s kapacitou příkonu v průměru 3,5 kW pro jeden každý rack.

2.2 Datové centrum CDP Přerov

Jedná se o sekundární datové centrum Správy železnic, které zajišťuje záložní lokalitu pro běh provozovaných aplikací. V datovém centru jsou v hlavním sále umístěny veškeré serverové vybavení, technologické zařízení i síťové prvky.

Datové centrum v současné budově CDP Přerov je na své kapacitní hranici (jak fyzické, tak co se podpůrných technologií týká, jako jsou napájení nebo chlazení). V současné době probíhají práce na dostavbě a rozšíření CDP Přerov o druhou budovu, a to včetně nových datových sálů a nového řešení zálohovaného napájení.

3 Serverovny

Větších či menších serveroven Správa železnic provozuje desítky v mnoha lokalitách po celém území republiky.

3.1 Významné serverovny

Správa železnic provozuje řadu serveroven, které jsou z pohledu SŽ významné svým umístěním nebo účelem, nikoli však třeba velikostí nebo provozovanými technologiemi. Patří sem třeba serverovny v budově Generálního ředitelství SŽ, serverovny kde se realizuje připojení k vnějším sítím a tvoří tak perimetr sítě.

3.2 Serverovny dle geografických oblastí

Serverovny OR slouží primárně pro provoz ICT infrastruktury a aplikací určených pro jednotlivá OR.

3.3 Serverovny vybraných organizačních jednotek

Vybrané specializované OJ provozují serverovny dedikované pro své potřeby. Jedná se především o různé vysoce specializované aplikace informační systémy.

3.4 Technologické serverovny

Technologické serverovny slouží k provozu OT serverové infrastruktury a dalších technologických zařízení.

3.5 Technologické a sdělovací místnosti

Technologické a sdělovací místnosti jsou umístěny téměř v každé železniční stanici a v mnoha administrativních či přímo technologických budovách. Úroveň jejich technologického a provozního vybavení je na nižší úrovni a pramení výhradně ze základních potřeb provozovaných systémů. Tyto prostory nejsou primárně určeny k provozu serverových technologií.

4 Technologické vybavení

Technické a bezpečnostní vybavení je velmi důležitým parametrem daného prostoru. V datových centrech a serverovnách jsou tyto nároky nejvyšší, ale i v běžných administrativních budovách jsou některé prvky nutné. Následující kapitoly popisují jednotlivé klíčové technologické prvky:

- **Stavební provedení** – Specifické stavební provedení datových center a serveroven je předpokladem pro bezpečné a spolehlivé provozování ICT infrastruktury.
- **Napájení** – Specifickým prvkem pro datová centra a serverovny je redundantní zálohované napájení.
- **Chlazení** – Stejně tak je pro datová centra typické chlazení datových sálů.
- **Elektronická zabezpečovací signalizace (EZS)** – Tyto systémy fyzické bezpečnosti se týkají všech typů budov Správy železnic včetně administrativních budov.
- **Přístupové a docházkové systémy** – Přístupové a docházkové systémy se používají napříč prostředím Správy železnic.
- **Kamerový systém** – Kamerové systémy uvnitř i vně budov jsou součástí fyzického zabezpečení budov.
- **Elektronické požární signalizace (EPS)** – Požární signalizace je dnes standardem jak v datových centrech a serverovnách, tak ve všech moderních administrativních budovách.
- **Automatické hasicí systémy (ASHS)** – Pro datová centra je ASHS nutným standardem a v případě požáru dokáže minimalizovat škody.
- **Ochrana proti vodě** – V datových centrech by měla být instalována ochrana proti vodě pro případ havárie.
- **Monitoring prostředí** – Monitoring prostředí (teplota, vlhkost) je pro datová centra a serverovny nepostradatelný prvek zajišťující bezpečný a spolehlivý provoz.
- **Dohled prostor** – Dohled je základní součástí fyzické bezpečnosti budov.

Cílem je pak zajistit pro SŽ datová centra s dostatečnými technickými parametry odpovídajícími minimálně klasifikaci TIER II a současně s dostatečnou fyzickou kapacitou pro umístění ICT infrastruktury.

4.1 Stavební provedení

Datová centra, serverovny a datové sály musí být projektovány v souladu se souborem norem ČSN EN 50600. Nepsaným standardem je například dvojitá zvýšená podlaha nebo dostatečně dimenzovaný přístup umožňující přepravu rackové skříně na výšku na paletovém vozíku.

4.2 Napájení

Napájení datových center a serveroven je klíčovou součástí provozu těchto zařízení. V datových centrech se provozuje mnoho kritických aplikací a systémů a proto je důležité zajistit spolehlivé napájení s dostatečnou kapacitou a zálohováním.

Potřeba elektrické energie v serverové infrastruktuře se během poslední dekády díky virtualizacím a rostoucí potřebě výkonu posunula pro každou serverovou rackovou skříň na hodnotu v průměru minimálně 5 kW špičkového příkonu (2,5 kW provozního příkonu).

Pro zálohování napájení se u datových center a významných serveroven používají diesel-generátory, záložní zdroje napájení a napájení z více zdrojů elektrické energie (distribuční soustava, UNZ). Určujícím faktorem je vždy kritičnost instalovaných technologií a požadavek na dobu zálohy.

Významným požadavkem je pak využívání centrálních záložních zdrojů v rámci prostor, jejich dimenzování a postupné rozšiřování. Cílem o omezit vznik většího počtu menších „ostrovních“ záložních zdrojů v jedné serverovně, nebo technologické či sdělovací místnosti.

4.3 Chlazení

Chlazení datových center je důležitým faktorem pro udržení vysoké dostupnosti a spolehlivosti serverů a dalších zařízení v datovém centru. Provoz datových center vyžaduje velké množství elektrické energie a výsledkem je produkce velkého množství tepla. Pokud se teplo neodvádí

dostatečně rychle, může dojít k přehřátí zařízení, přerušení provozu a v některých případech i porušení či ztrátě dat.

Pokud je to technicky možné, je nutné zajistit chlazení koncepcí zakrytované studené uličky, což musí respektovat i směr montáže aktivních prvků. V datových centrech a významných serverovnách je dále vyžadována redundance chladících jednotek.

4.4 Bezpečnost

V datových centrech i serverovnách je nutné zajistit plně funkční EZS, EPS, přístupový systém i kamerový systém, který obsáhne nejen vnější perimetr budovy, ale i jednotlivé sály a uličky mezi rackovými řadami.

Automatický hasicí systém jako rozšíření systému EPS je preferovaným řešením, jelikož v případě požáru dokáže výrazně snížit způsobené škody na ICT infrastruktuře.

Nedílnou součástí je také fyzická bezpečnost a fyzické zabezpečení datových center a budov, kde jsou umístěny významné serverovny.

4.5 Síťová infrastruktura

Datová centra a serverovny musí být síťově odděleny od zbytku sítě pomocí firewallu. Pro místní síťové připojení je nutné používat výhradně síťové prvky detailně definované v Příloze 4 – *Konektivita a síťové prostředí*.

4.6 Ostatní vybavení

Monitorování prostředí v datových centrech je velmi důležité, protože kritické IT systémy jsou citlivé na změny teploty, vlhkosti a kvality vzduchu. Při narušení těchto parametrů může dojít ke vzniku problémů, jako jsou selhání systémů a ztráta dat. Proto se v datových centrech používají speciální senzory a zařízení pro monitorování a řízení prostředí.

Nová i rekonstruovaná datová centra a serverovny musí monitorovat minimálně tyto parametry:

- Teplota
- Vlhkost
- Stav napájení (zálohovaného i nezálohovaného)

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz

```
hdac0: <NVIDIA (0x0083) HDA CODEC> at cad 0
hdac0: <NVIDIA (0x0083) Audio Function Group
pem0: <NVIDIA (0x0083) (HDMI/DP 8ch)> at nid
pem1: <NVIDIA (0x0083) (HDMI/DP 8ch)> at nid
pem2: <NVIDIA (0x0083) (HDMI/DP 8ch)> at nid
pem3: <NVIDIA (0x0083) (HDMI/DP 8ch)> at nid
ugen0.1: <0x0086 XHCI root HUB> at usb0
uhub0: <0x0086 XHCI root HUB, class 9/0, rev
nvd0: <Samsung SSD 960 PRO 512GB> NVMe namesp
nvd0: 488386MB (100215216 512 byte sectors)
ada0 at ahcich0 bus 0 scbus0 target 0 lun 0
ada0: <ST320LT012-9WS14C 0001LVM1> ATAB-ACS S
ada0: Serial Number W0VDEFBC
ada0: 300.000MB/s transfers (SATA 2.x, UDMA6,
ada0: Command Queueing enabled
ada0: 305245MB (625142448 512 byte sectors)
ada0: quirks=0x1<4K>
ada1 at ahcich4 bus 0 scbus4 target 0 lun 0
ada1: <ST4000DM000-1F2168 CC52> ATAB-ACS SATA 3
ada1: Serial Number Z300YNBS
```

Platforma SŽ

Virtuální prostředí, serverové farmy, servery

Červen 2025

Obsah

1	Úvod	4
2	Virtualizační prostředí.....	4
2.1	Virtualizace serverů.....	4
2.2	Virtualizace koncových počítačů	4
2.3	Kontejnerizace.....	4
3	Serverové farmy.....	4
3.1	Konvergovaná infrastruktura	4
3.2	Hyper-konvergovaná infrastruktura	5
4	Fyzické servery	5
5	Datová úložiště.....	5
5.1	Datová úložiště farem.....	5
5.2	Datová úložiště pro zálohy a archivaci	5
5.3	Datová úložiště pro off-line zálohy	6
5.4	Kancelářská datová úložiště	6
6	Virtuální servery	6
6.1	Služba virtuálních strojů	6
6.2	Služby diskových uložišť	7
7	Databázové servery	7
8	Webové servery.....	7
9	Aplikační servery	8

Seznam zkratek

ACI	Technologie aplikačně orientované infrastruktury firmy Cisco (<i>Cisco ACI</i>)
CPU	Hlavní procesor zařízení či počítače, který je zodpovědný za plynulé spouštění software (<i>Central Processing Unit</i>)
DB	Databázová aplikace (<i>Database Engine</i>)
DR	Plán obnovy po havárii, součást kontinuity IT služeb (<i>Disaster Recovery</i>)
FC	Vysokorychlostní datové rozhraní primárně používané pro datová úložiště (<i>Fibre Channel</i>)
HCI	Jde o formu softwarově definované serverové infrastruktury. V principu se jedná o virtualizační platformu, která redundantně sdílí v rámci clusteru vše – výpočetní výkon, paměť i datové úložiště (<i>Hyperconverged Infrastructure</i>)
HTTP	Standardizovaný protokol pro přenos webových stránek (<i>Hyper-text Transfer Protokol</i>)
HW	Hardware označuje veškeré fyzicky existující technické vybavení počítače
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
iSCSI	Protokol, který umožňuje připojení k diskovým zdrojům přes počítačovou síť. To umožňuje serverům, aby mohly vzdáleně používat disky jako by byly připojeny přímo k nim, což umožňuje centralizaci a vzdálený přístup k datům. iSCSI je často používán v malých a středních podnicích jako alternativa k SAN (<i>Internet Small Computer System Interface</i>)
IT	Informační technologie (<i>Information Technology</i>)
LTO	Otevřený formát magnetické pásky určené pro záznam velkých objemů dat (<i>Linear Tape Open</i>)
NAS	Zařízení pro ukládání a správu dat, které je připojeno k počítačové síti a umožňuje přístup k datům přes souborové protokoly jako SMB, NFS, FTP a HTTP. NAS může být malé zařízení pro jeden či několik disků určené pro domácnosti nebo může jít profesionální zařízení určené pro montáž do racku (<i>Network Attached Storage</i>)
OS	Operační systém
SAN	Oddělená datová síť pro připojení datových úložišť. Zpravidla používá protokol FC nebo iSCSI (<i>Storage Area Network</i>)
SAP	Modulární ERP systém od německé firmy SAP AG
SOHO	Obecné označení pro zařízení pro domácí a kancelářské použití (<i>Small Office / Home Office</i>)
SW	Software je sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost
SŽ	Správa železnic, státní organizace
SŽT	Správa železničních informačních technologií
VDI	Technologie, která umožňuje uživatelům pracovat na virtuálním desktopu odděleném od jejich fyzického zařízení. Tyto virtuální desktopy jsou hostovány na centrálním serveru a uživatelé se k nim připojují pomocí klientských zařízení, jako jsou stolní počítače, notebooky nebo mobilní zařízení (<i>Virtual Desktop Infrastructure</i>)
VM	Virtuální počítač (<i>Virtual Machine</i>)

Seznam vysvětlivek

Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.
---------------------	--

1 Úvod

Cílem této části Platformy SŽ je popis podporovaných infrastrukturních služeb, technologií, a architektonických principů v oblasti virtualizačního prostředí, fyzických serverů a virtuálních serverů všech typů v ICT prostředí Správy železnic. Tato příloha definuje jak poskytované infrastrukturní služby v rámci veřejných zakázek a návrhů dodávaných řešení, tak i samotné budování a rozšiřování virtualizačního prostředí Správy železnic.

Cílem je zajistit ve fázích přípravy poptávky, návrhu ICT řešení a realizace dodávky kompatibilitu se stávajícím ICT prostředím Správy železnic a v maximální míře využít již provozované komponenty a technologie.

2 Virtualizační prostředí

Správa železnic postupně transformuje starší serverovou infrastrukturu na moderní virtuální řešení avšak s ohledem na rozsáhlost ICT prostředí SŽ je tento proces stále aktuální. Velmi efektivní je stále také virtualizace koncových počítačů (VDI) ve spojení s centralizovaným řízením dopravy.

2.1 Virtualizace serverů

Správa železnic ve svém ICT prostředí provozu větší množství serverových farem poskytujících virtuální prostředí pro běh virtuálních serverů.

Starší a konzervativnější technologií jsou virtualizace na software MS HyperV (nepreferované řešení určené výhradně pro singlenody) a na software VMware vSphere (vícenodové farmy s dedikovanou storage připojenou zpravidla přes Fibre Channel).

Novější technologií je pak HCI s využitím software VMware vSphere a VMware vSAN.

2.2 Virtualizace koncových počítačů

Virtualizace typu VDI je provozována na řešení VMware Horizon a slouží především pro dispečerské stanice dálkového řízení.

S ohledem na specifické určení není tato technologie součástí infrastrukturních služeb nabízených Platformou SŽ.

2.3 Kontejnerizace

V ICT prostředí Správy železnic probíhá testování a development virtualizačního řešení pro platformy Docker a Kubernetes. V současné chvíli není možné toto nabídnout jako infrastrukturní službu v rámci Platformy SŽ.

3 Serverové farmy

Správa železnic provozuje větší množství serverových farem různých velikostí od 3 nodů až po 16 serverových nodů na různých technologiích (klasická virtualizace, virtualizace v OS, HCI, VDI). Z důvodu vzájemné kompatibility jsou využívány výhradně CPU x86_64 verze 3 od firmy Intel.

3.1 Konvergovaná infrastruktura

V rámci konvergované infrastruktury provozuje SŽ tyto druhy farem:

- Jedno-nodové virtualizace na řešení Microsoft Hyper-V – jedná se o nepreferované řešení výhradně jen pro virtualizaci OS Windows Server.
- Jedno-nodové virtualizace na řešení VMware – jedná se obecně o nepreferované řešení, výhradně určené jen pro vzdálené lokality s minimálními nároky na virtualizaci.
- Klasická virtualizace s dedikovanou storage – preferované řešení pro menší clustery
- Virtualizace VDI – výhradní řešení pro virtualizaci koncových počítačů

3.2 Hyper-konvergovaná infrastruktura

V minulých letech Správa železnic úspěšně adoptovala technologii HCI a v současné době na ní provozuje více než 10 serverových farem ve velikostech od 4 nodů až po 16 nodů.

Všechny tyto nové HCI clustery umožňují v budoucnosti zapojení do topologie Cisco ACI jako Remote Leaf.

Rozšiřování těchto farem musí respektovat tato pravidla a současně je z důvodu kompatibility nutné dodržet vždy shodné parametry serverových nodů a technologií.

4 Fyzické servery

Nové samostatné fyzické servery již není možné do ICT prostředí Správy železnic umísťovat. Pokud je to technicky možné musí být nahrazeny virtualizovaným řešením. Výjimkou jsou návrhy řešení a dodávky hotových fyzických appliance, pokud jejich výrobce nedodává virtualizovanou verzi.

U fyzických serverů nedokáže Správa železnic zajistit stejné a plnohodnotné podpůrné služby jako u virtualizovaných serverů (monitoring, patch management, zálohování, ...).

Výjimky posuzuje Odbor IT architektury SŽT v procesu tvorby a/nebo akceptace technické specifikace veřejné zakázky.

5 Datová úložiště

V ICT prostředí Správy železnic je provozováno více druhů datových úložišť.

5.1 Datová úložiště farem

Pro farmy klasické konvergované infrastruktury jsou provozovány datová úložiště:

- Umísťují se do rackových skříní.
- Slouží výhradně pro připojení daného serverového clusteru.
- Využívají výhradně disky typu SSD nebo NVMe v redundanci minimálně RAID6 nebo obdobném ekvivalentu. Preferovaná je modernější technologie NVMe.
- Velikost i výkon musí odpovídat potřebám konkrétní farmy.
- Preferované připojení je pomocí Fibre Channel, případně i iSCSI nebo přímé připojení SAS.

5.2 Datová úložiště pro zálohy a archivaci

Pro ukládání záloh a archivaci jsou určena datová úložiště:

- Umísťují se do rackových skříní.
- Slouží výhradně pro ukládání záloh.
- Využívají výhradně disky typu NL-SAS nebo SAS v redundanci minimálně RAID5 nebo vyšším. Disky nesmí používat technologii SMR.
- Velikost i výkon musí odpovídat potřebám zálohování farem.

- Preferované připojení je pomocí Fibre Channel, případně i iSCSI nebo přímé připojení SAS.

5.3 Datová úložiště pro off-line zálohy

Pro archivaci a offline ukládání záloh jsou určeny páskové knihovny:

- Umísťují se do rackových skříní v DR lokalitách a připojují se na backup server.
- Slouží výhradně pro ukládání offline záloh na LTO pásky.
- Využívají pásky typu LTO 9.
- Počet mechanik i počet pásek v knihovně musí odpovídat potřebám offline zálohování.
- Preferované připojení je pomocí Fibre Channel nebo přímé připojení SAS.
- Musí být zajištěn proces pravidelné a bezpečné manipulace s páskami a jejich ukládáním.

5.4 Kancelářská datová úložiště

Lokální zařízení typu NAS nejsou preferovaná a jejich zapojení do sítě Správy železnic podléhá schválení Odboru IT architektury SŽT.

Mála SOHO zařízení typu NAS umísťovaná mimo rackové skříně, typicky do kancelářských prostor, jsou nepřijatelná a nesmí být připojována do ICT prostředí Správy železnic.

Větší disková úložiště typu NAS umísťovaná do rackových skříní lze na základě posouzení a výjimky Odboru IT architektury připojit do sítě SŽ. Redundance disků musí na úrovni RAID5 nebo vyšší.

6 Virtuální servery

Virtualizace v ICT prostředí Správy železnic poskytuje základní infrastrukturní služby jejichž seznam a popis prezentuje Platforma SŽ.

6.1 Služba virtuálních strojů

Infrastrukturní služba VM je provozována na vysoce dostupných virtualizačních technologiích VMware. Parametry služby jako sizing virtuálních strojů, výběr OS podporovaných Platformou SŽ, počet a konfigurace síťových karet jsou konfigurovány individuálně na základě požadavků projektu, resp. dodávaného řešení.

Správa železnic zajišťuje vysokou dostupnost služby virtuálních strojů na úrovni virtualizace i sítě, a to v rámci jednoho datového centra či serverovny. Pokud navrhované řešení vyžaduje také georedundanci nebo redundanci napříč datovými centry, musí být dodavatelem v rámci dodávky zajištěno řešení loadbalancingu.

Služby virtuálních serverů

Služba	Popis
Win.VMware.x86_64	Služby virtuálního serveru s operačním systémem Windows Server na virtualizaci VMware a architektuře x86_64
RHEL.VMware.x86_64	Služby virtuálního serveru s operačním systémem RHEL (RedHat Enterprise Linux) na virtualizaci VMware a architektuře x86_64
Debian.VMware.x86_64	Služby virtuálního serveru s operačním systémem Debian Linux na virtualizaci VMware a architektuře x86_64 Omezení: Preferované řešení pro kontejnerizaci.
SLES.VMware.x86_64	Služby virtuálního serveru s operačním systémem SLES (SUSE Linux Enterprise Server) na virtualizaci VMware a architektuře x86_64 Omezení: Využití pro výhradně pro SAP

6.2 Služby diskových úložišť

Disková kapacita těchto infrastrukturních služeb je provozována v datových úložištích farem, ať už dedikovaných, nebo interních v rámci technologie VMware vSAN, kde je zajištěna dostatečná úroveň redundance.

V rámci virtualizačních clusterů jsou dostupné výhradně disky SSD a NVMe. Starší rotační disky (HDD) jsou dostupné jen jako součást úložišť pro zálohy a archivace. Případný tiering není součástí služby a je nutné ho řešit na úrovni SW navrhovaného řešení.

Služby diskových úložišť

Služba	Popis
Datový disk HDD	Služba diskových úložišť pro zálohy a archivaci. Nelze použít pro systémové disky a/nebo pro provoz aplikací.
Datový disk SSD	Služba diskových úložišť pro aplikace. Není vhodné využívat pro zálohy a archivaci z důvodu enormní ceny řešení.

7 Databázové servery

V prostředí Správy železnic je provozováno několik typů databázových serverů a v rámci Platformy SŽ jsou poskytovány tyto platformní služby:

Služby databázových prostředí

Služba	Popis
Oracle DB na Oracle Exadata	Databázová služba Oracle DB provozovaná na optimalizovaném hardware Oracle Exadata Database Machine – kombinovaná hardwarová a softwarová platforma.
MS SQL na Win.VMware.x86_64	Služba virtuálních databázových serverů MS SQL Server provozovaná na serverech s operačním systémem Windows Server a virtualizační platformě VMware.

8 Webové servery

V prostředí Správy železnic je provozováno několik typů webových serverů a v rámci Platformy SŽ jsou poskytovány tyto platformní služby:

Služby webových serverů

Služba	Popis
Microsoft IIS na Win.VMware.x86_64	Služba webového serveru postavená na technologii Microsoft Internet Information Services (IIS) provozovaná na serverech s operačním systémem Windows Server s virtualizací VMware.
Apache HTTP Server na Win.VMware.x86_64	Služba webového serveru postavená na open-source technologii Apache provozovaná na serverech s operačním systémem Windows Server s virtualizací VMware.
Apache HTTP Server na RHEL.VMware.x86_64	Služba webového serveru postavená na open-source technologii Apache provozovaná na serverech s operačním systémem RHEL s virtualizací VMware.

9 Aplikační servery

V prostředí Správy železnic je provozováno jedno portálové řešení, které je v rámci Platformy SŽ poskytováno jako platformní služba:

Služba zabezpečeného portálového řešení

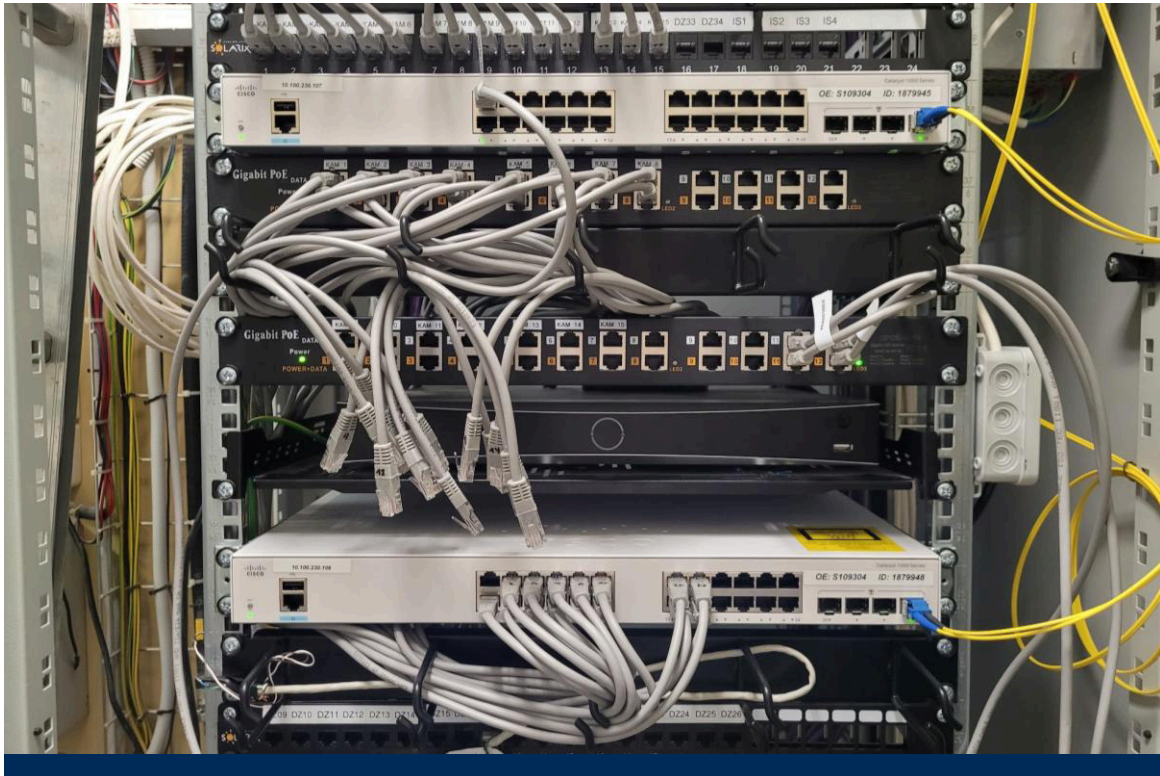
Služba	Popis
Liferay na Win.VMware.x86_64	Liferay je přední open-source podnikové portálové řešení založené na jazyce Java, které umožňuje správu dat, aplikací, procesů a integrace současných i nových aplikací z jednoho centrálního uživatelského rozhraní.

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Konektivita a síťové prostředí

Červen 2025

Obsah

1	Úvod	8
2	Perimetr Správy železnic	8
2.1	Perimetr	8
2.2	Demilitarizovaná zóna	8
2.2.1	Demilitarizovaná zóna pro OT	8
2.3	Přístup přes VPN	8
2.3.1	Uživatelské VPN s MFA	9
2.3.2	Site to Site VPN	9
2.4	Komunikační směry	9
3	Fyzické sítě Správy železnic	10
3.1	Uživatelsko-aplikační síť	10
3.2	Technologické datové sítě	10
3.2.1	Segmentace sítě	10
3.2.2	Ostrovni oddělené sítě	10
4	Logické síťové prostředí	11
4.1	Komunikace mezi sítěmi	11
4.2	Georedundance	11
4.3	Řešení High Availability	11
5	Sítě APN	12
6	Síťová zařízení	12
6.1	Používané technologie	12
6.1.1	VLAN	12
6.1.2	VRF	12
6.1.3	Technologie DWDM	13
6.1.4	Sítě MPLS	13
6.1.5	Síťová spine-leaf topologie	13
6.1.6	Technologie Cisco ACI	13
6.1.7	Sítě OOB	14
6.2	Firewally	14
6.3	Routery	14
6.4	Switche	15
6.4.1	Switche pro datová centra	15
6.4.2	Switche pro fibre channel	15
6.4.3	Switche pro kamerové systémy	15
6.4.4	Switche pro management zařízení	16
6.4.5	Switche pro lokální sítě	16
6.5	Bezdrátová zařízení	16
6.6	Huby	16
6.7	Modemy a datová zařízení	16
6.8	Centralizovaná správa síťových prvků	17

Seznam zkratek

ACI	Aplikačně orientovaná infrastruktura
APN	Jméno brány mezi mobilní datovou sítí a jinou počítačovou sítí (může obsahovat MCC a MNC daného mobilního operátora) (<i>Access Point Name</i>)
CLI	Příkazový řádek (<i>Command Line Interface</i>)
DB	Databáze
DC	Datové centrum v kontextu lokalit (<i>Datacenter</i>)
DCS	Distribuovaný systém řízení technologií (<i>Distributed Control System</i>)
DDoS	Distribuované odmítnutí služby je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele, a to útokem mnoha koordinovaných útočnicků (<i>Distributed Denial of Service</i>)
DMZ	Část síťové infrastruktury organizace, ve které jsou soustředěny služby poskytované někomu z okolí, případně celému Internetu. Tyto vnější (veřejné) služby jsou obvykle nejsnazším cílem internetového útoku; úspěšný útočník se ale dostane pouze do DMZ, nikoli přímo do vnitřní sítě organizace (<i>Demilitarized Zone</i>)
DoS	Odmítnutí služby je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele (<i>Denial of Service</i>)
DR	Plán obnovy po havárii, součást kontinuity IT služeb (<i>Disaster Recovery</i>)
DSL	Technologie pro vysokorychlostní připojení k internetu, která využívá telefonní linku. DSL umožňuje přenos dat přes kovový vedení telefonní sítě s využitím frekvenčního spektra, které není využíváno pro telefonní hovory (<i>Digital Subscriber Line</i>)
DWDM	Typ vlnového multiplexu, který je založený na multiplexování více optických signálů v jednom optickém vlákne na různých vlnových délkách nebo různých typech laserů (<i>Dense Wavelength Division Multiplex</i>)
GPRS	GPRS je mobilní datová služba první generace. Dnes je GPRS již zastaralou technologií a byla nahrazena modernějšími technologiemi, jako jsou například 4G a 5G (<i>General Packet Radio Service</i>)
HA	Vysoká dostupnost služeb. Předpokladem řešení je použití dvou a více nezávislých zařízení s cílem zajistit funkčnost v případě výpadku (<i>High Availability</i>)
HW	Hardware označuje veškeré fyzicky existující technické vybavení počítače
ICS	Průmyslové řídicí systémy (<i>Industrial Control System</i>)
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
IKEv2	Protokol pro šifrování síťových spojení, který se používá k zabezpečení VPN a jakýchkoliv jiných síťových spojení. Tento protokol je specifikován jako standard Internet Engineering Task Force, nabízí vysokou úroveň bezpečnosti, dostupnosti a rychlosti. Dále pak podporuje automatické obnovování spojení, umožňuje rychle reagovat na změny síťového prostředí a také poskytuje podporu pro více typů šifrování a autentizace.
Industrial DMZ	Část síťové infrastruktury organizace, ve které jsou soustředěny služby poskytované někomu z okolí, případně do jiných sítí. Případným úspěšným útokem se ale útočník dostane pouze do Industrial DMZ, nikoli přímo do vnitřní sítě s vyšší bezpečnostní úrovní (<i>Industrial DeMilitarized Zone</i>)
IPsec	Jedná se o protokol, který se používá k šifrování a ochraně dat přenášených přes Internet. IPsec se často používá k ochraně VPN spojení, ale také může být použit k ochraně jakýchkoli dat přenášených přes internetové sítě. Šifrování zabraňuje neoprávněnému čtení dat, zatímco autentizace zajišťuje, že data pocházejí od autorizovaného zdroje. Tyto funkce pomáhají chránit síť před neoprávněným přístupem, únikem dat a jinými bezpečnostními hrozbami (<i>Internet Protocol Security</i>)
IT	Informační technologie (<i>Information Technology</i>)
LAN	Místní počítačová síť (<i>Local Area Network</i>)
LTE	Řešení mobilního bezdrátového vysokorychlostního přenosu dat čtvrté generace (<i>4G / Long Term Evolution</i>)
MFA	Více-faktorové ověření identity uživatele (<i>Multi-Factor Authentication</i>)

MGMT	Řízení, dohled, konfigurace, sběr dat a vzdálený přístup k serverům a aktivním síťovým prvkům (<i>Management</i>)
MPLS	Multi-protokolové přepojování podle značek – metoda směrování síťového provozu používaná ve vysokorychlostních telekomunikačních sítích, která pro směrování nepoužívá relativně dlouhé a protokolově závislé síťové adresy, ale krátké značky pevné délky. Standard je definován v RFC 3031 (<i>Multiprotocol Label Switching</i>)
NGFW	Oproti běžným FW nabízí také doplňkové funkce jako AVC, AMP, IPS, IDS, DPI, DLP, TD, IdM a dešifrování a kontrolu TLS/SSL obsahu (<i>Next-Generation Firewall</i>)
OOB	Oddělená síť určená pro management serverů a aktivních síťových prvků. Z oprávněných provozních a technických důvodů lze požadavek na oddělení splnit užitím vyhrazených VLAN nebo VRF VPN (<i>Out-of-Band MGMT LAN</i>).
OŘ	Oblastní ředitelství SŽ
OS	Operační systém (<i>Operating System</i>)
OT	Provozní technologie (<i>Operations Technology</i>)
PAM	Řešení zabezpečení identit, které pomáhá chránit organizaci před kybernetickými hrozbami monitorováním, zjišťováním a prevencí neoprávněného privilegovaného přístupu k důležitým prostředkům (<i>Privileged Access Management</i>)
PLC	Programovatelný automat, typické koncové zařízení v OT (<i>Programmable Logic Controller</i>)
PoE	Technologie napájení zařízení přes standardní ethernetový kabel. PoE existuje v několika standardech, které se liší především přenášeným elektrickým výkonem (<i>Power over Ethernet</i>)
RJ45	Standardizovaný metalický konektor pro počítačové sítě (<i>Registered Jack 45</i>)
S2S VPN	Šifrované VPN připojení zajišťující propojení dvou LAN (<i>Site-to-Site VPN, LAN-to-LAN VPN</i>)
SAN	Oddělená datová síť pro připojení datových úložišť. Zpravidla používá protokol FC nebo iSCSI (<i>Storage Area Network</i>)
SCADA	Softwarové řešení zpravidla dispečerského dohledu a monitorování technologií (<i>Supervisory Control And Data Acquisition</i>)
SFP	Typ slotu a modulu pro datovou komunikaci zpravidla po optických vláknech. Podporuje rychlost maximálně 1 Gbps (<i>Small Form Factor Pluggable</i>)
SFP+	Typ slotu a modulu pro datovou komunikaci zpravidla po optických vláknech. Podporuje rychlost maximálně 10 Gbps (<i>Small Form Factor Pluggable Plus</i>)
SMS	Krátká textová zpráva
SW	Programové vybavení počítače či jiného obdobného zařízení. Speciálním druhem software je firmware, který je úzce spjatý s konkrétním hardwarem (Software)
SŽ	Správa železnic, státní organizace
SŽT	Správa železniční telematiky, organizační jednotka SŽ
TDS	Technologické datové sítě SŽ, jedná se o více VRF zpravidla vyhrazených pro OT, běžně se nazývají také „Techlan“
UAS	Logická uživatelsko-aplikační síť SŽ, zahrnuje VRF v MPLS sítích a lokální VLAN, běžně se nazývá také „Intranet SŽ“
VM	Virtuální počítač (<i>Virtual Machine</i>)
VPN	Virtuální privátní síť (<i>Virtual Private Network</i>)
VRF	Virtuální směrování a předávání technologie, která v počítačových sítích založených na protokolu IP umožňuje souběžnou existenci více instancí směrovací tabulky v rámci sítě stejného směrovače ve stejnou dobu (<i>Virtual Routing and Forwarding</i>)
WAF	WAF je druh firewallu, který se specializuje na zabezpečení webových aplikací a webových stránek. WAF slouží k ochraně webových aplikací před různými druhy útoků, jako jsou SQL injection, Cross-Site Scripting a další. WAF využívá různé techniky pro detekci a blokování nežádoucího provozu, včetně filtrace vstupů, detekce neobvyklých činností a analýzy protokolu HTTP. WAF může být nasazen jako samostatné zařízení, jako virtuální síťový prvek nebo jako součást firewallu sítě. WAF může být konfigurován pro konkrétní webové aplikace a stránky, aby poskytoval co nejlepší ochranu před útoky. Mezi funkce WAF patří například blokování útoků v reálném čase, sledování webových aplikací a identifikace bezpečnostních rizik, správa povolených a zakázaných přístupů a další. WAF může fungovat i jako load balancer pro webové servery (<i>Web Application Firewall</i>)

ZoKB

Zákon o kybernetické bezpečnosti č. 181/2014 Sb. a souvisejících zákonů v
pozdějším znění

Seznam vysvětlivek

Active-Active	Distribuce zátěže na více nebo všechny síťové prvky.
Industrial DMZ	Část síťové infrastruktury organizace, ve které jsou soustředěny služby poskytované někomu z okolí, případně do jiných sítí. Případným úspěšným útokem se ale útočník dostane pouze do Industrial DMZ, nikoli přímo do vnitřní sítě s vyšší bezpečnostní úrovní
Jump server	Zabezpečené a monitorované zařízení, které spojuje dvě různé bezpečnostní zóny.
Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.
Purdue Model	Strukturální model pro zabezpečení průmyslových řídicích systémů.
Site-to-Site	Propojení dvou a více vzdálených sítí.
Spine-Leaf	Dvouvrstvá síťová topologie switchů spine a leaf vyvinutá pro datová centra.
Standard IEEE 802.3af	Standard pro PoE napájení. Maximální přenášený výkon je 15,4 W.
Standard IEEE 802.3at	Standard pro PoE napájení, který se označuje jako PoE+. Maximální přenášený výkon je 30 W.
Standard IEEE 802.3bt	Standard pro PoE napájení, který se označuje jako PoE++. Maximální přenášený výkon je 60 W.

1 Úvod

Tento dokument je přílohou a nedílnou součástí Základního dokumentu Platformy SŽ a definuje základní principy a pravidla síťové komunikace v ICT prostředí Správy železnic. Současně popisuje síťové prostředí a poskytované služby ze strany Správy železnic.

2 Perimetr Správy železnic

2.1 Perimetr

Perimetrem se označuje část systémů, které jsou využity pro komunikace mimo interní síť SŽ. Jde o významnou součást celé ICT infrastruktury. Hlavními aspekty pro perimetr sítě jsou dvě oblasti:

- **Bezpečnost** – kontrola komunikace a ochrana před proniknutím z oblastí mimo síť Správy železnic (Internet, síť externích dodavatelů).
- **Výkonnost** – předpokladem perimetru je koncentrace komunikace v obou směrech, tedy, jak překlad provozu na vnitřní aplikace (web služby, mail systém, VPN), tak i komunikace ze sítě ven (Internet, aplikace a služby třetích stran).

Perimetr a vnější zabezpečení sítě v sobě spojuje více služeb dále využívaných v ICT infrastruktuře. Jde primárně o služby ochrany proti DDoS, oddělené DMZ a terminace VPN připojení.

2.2 Demilitarizovaná zóna

Demilitarizovaná zóna (DMZ) je bezpečnostní mechanismus, který se používá v síťové architektuře pro umístění systémů dostupných z Internetu, či dalších lokalit mimo bezpečnostní perimetr. DMZ se v prostředí SŽ nachází na hranici sítě mezi Internetem a vnitřní sítí organizace a obsahuje servery, WAF, VPN koncentrátoři a další zařízení, která mají být přístupná ze sítě Internet.

Definici DMZ určují pravidla v NGFW, na základě těchto pravidel je striktně zakázána komunikace z vnitřní sítě přímo do Internetu bez použití DMZ a stejně tak i opačný směr.

2.2.1 Demilitarizovaná zóna pro OT

Princip industriální DMZ spočívá v použití firewallu mezi IT a OT sítí, neboli mezi uživatelskou a technologickou sítí a vytvoření bezpečného prostředí pro umístění aplikací a zařízení pro přenos dat mezi těmito sítěmi, např. jump servery, integrační koncentrátoři, integrační servery a jiné. V síti SŽ je totiž striktně zakázán přímý přístup z uživatelské do technologické sítě a naopak.

2.3 Přístup přes VPN

Jde o službu pro realizaci šifrované komunikace z externího prostředí na aplikace či hardware ve vnitřních sítích a také pro jejich správu. VPN bývá provozována ve dvou základních režimech, a to jako Site to Site VPN (určeno pro připojení celých počítačových sítí nebo serverů) nebo jako uživatelská Client to Site VPN s MFA (multifaktorovou autentizací) pro přístup zaměstnanců a externistů k zařízením a službám v prostředí Správy železnic.

Pro externí Dodavatele je možné zřídit VPN přístup na konkrétní servery a systémy v UAS nebo v TDS.

2.3.1 Uživatelské VPN s MFA

Klientské VPN jsou řešené pomocí Cisco AnyConnect klientů s ověřením přes multifaktorovou autentizaci (MFA). MFA je vyžadováno pro další ověření uživatele pomocí jednorázového kódu doručeného prostřednictvím SMS na zaregistrované telefonní číslo.

Pro tyto VPN platí následující pravidla:

- Není povolený split-tunnel.
- Pro externisty není přes VPN povolen přístup k síti Internet.
- Pro řešení MFA je krom SMS používán i MS Authenticator nebo Cisco DUO.
- Ověřování uživatelů se provádí pomocí Cisco ISE.

Pro přístup na cílová zařízení je povinné využít bezpečnostní systém PAM. Přístup na cílové technologie mimo systém PAM je umožněn pouze na výjimku ze strany Odboru Kybernetické bezpečnosti SŽT, například pokud cílový systém není možné integrovat do systému PAM. Při zavádění systému je nutné poskytnout aktivní spolupráci Dodavatele se Správou železnic (poskytnout potřebné informace – použité protokoly pro vzdálený přístup, testovací účty, ověření funkčnosti) pro zprovoznění vzdáleného přístupu skrze bezpečnostní systém PAM.

2.3.2 Site to Site VPN

Pro připojení vzdálených lokalit či podpůrných systémů mimo síť SŽ se používají S2S VPN s protokolem IPsec IKEv2. Z důvodů vyžadovaných ZoKB musí být komunikace z těchto S2S VPN explicitně omezena jen na konkrétní vyjmenovaná zařízení (servery apod.) a je nutné u připojené protistrany zajistit průkaznou identifikaci uživatelů, kdo a kdy vyžil přístup skrze S2S VPN. Tyto záznamy musí poskytnout na požádání SŽ. Je nutné mít odůvodněný požadavek pro použití S2S VPN. Pokud je to provozně/technicky možné jsou preferované jmenné VPN vázané na konkrétní osobu.

2.4 Komunikační směry

Správa železnic má na základě běžných síťových standardů a praktik vydefinovány povolené a zakázané směry síťové komunikace, tak aby byla zajištěna nejvyšší úroveň zabezpečení sítí, informačních systémů i celého ICT prostředí.

Pravidla síťové komunikace na perimetru SŽ

Zdroj	Směr	Cíl	Stav
UAS	→	DMZ	filtrováno
UAS	←	DMZ	zakázáno
VPN	←	DMZ	filtrováno
APN	↔	DMZ	filtrováno
APN	↔	UAS	zakázáno
APN	↔	TDS	zakázáno
APN	↔	Industrial DMZ	filtrováno
UAS	←	VPN	filtrováno
TDS	↔	DMZ	zakázáno
TDS	↔	Industrial DMZ	filtrováno
UAS	↔	Industrial DMZ	filtrováno
UAS	↔	TDS	zakázáno
UAS	→	Internet	filtrováno
Internet	←	VPN (zaměstnanecká)	filtrováno
Internet	↔	VPN (externisté)	zakázáno
Internet	↔	S2S VPN	zakázáno
Internet	↔	DMZ	filtrováno
Internet	→	UAS	zakázáno
Internet	↔	TDS	zakázáno

Na základě těchto pravidel veškerá komunikace mezi vnitřními sítěmi a Internetem probíhá výhradně přes aplikace nebo zařízení umístěná v DMZ na perimetru Správy železnic. Přímá komunikace z uživatelsko-aplikační sítě do sítě Internet není povolena, existují však specifické výjimky. Tato omezení platí i pro zabezpečené sítě datových center a serveroven a tedy stejně tak, přímá komunikace ze serverů do sítě Internet (aktualizace, stažení instalačních balíčků) není povolena. Vždy je nutné využít nepřímé komunikace přes proxy server nebo obdobná zařízení. I zde existuje výjimka a pro specifické systémy lze tuto komunikaci povolit.

Pokud nějaké konkrétní zařízení nebo informační systém není schopen z objektivních technických důvodů tato omezení dodržet při zachování své funkce, je nutné před implementací takového řešení požádat o výjimku u Odboru IT architektury SŽT, kde bude výjimka posouzena a povolena nebo zakázána, případně bude zvoleno alternativní řešení.

3 Fyzické sítě Správy železnic

3.1 Uživatelsko-aplikační síť

Jedná se o rozsáhlou komunikační síť pro veškerý kancelářský i podpůrný provoz, jsou zde umístěny běžné uživatelské počítače, tiskárny, skenery, ale i serverovny a datacentra pro provoz farem a aplikací. Servery pro IT jsou provozovány výhradně v této síti.

V současné době je uživatelsko-aplikační síť (UAS) provozována ve staré MPLS síti, kdy páteřní uzly komunikační infrastruktury UAS jsou navzájem propojeny, zajišťují směrování síťových komunikací a na vybraných trasách i redundanci v případě ztráty průchodnosti tras.

3.2 Technologické datové sítě

Tyto sítě jsou v prostředí Správy železnic určeny primárně pro OT zařízení a převážně pro provozní drážní a jejich podpůrné systémy. Jsou striktně definované a vlastnostmi odpovídají nejvyšším zabezpečovacím standardům pro provoz kritické i nekritické infrastruktury.

Jednotlivé technologické sítě v TDS jsou rozdělené dle konkrétních technologií na úrovni separátních VRF. Od UAS jsou odděleny pomocí firewallů, přístup k OT zařízením je umožněn pouze přes jump servery či jiné systémy (koncentrátory) umístěné v IT/OT DMZ. Zařízení ani uživatelé v TDS nemají přímý přístup do sítě UAS ani Internet a to včetně aktualizací SW atp.

3.2.1 Segmentace sítě

V nedávné době proběhl v prostředí SŽ projekt „Rekonstrukce a segmentace technologických sítí“, jejímž cílem byla migrace z původní sítě do nově segmentované MPLS sítě, včetně zřízení šesti segmentů propojených přechodovými firewallly.

Segmentace UAS se v současné době aktivně připravuje, čili tato síť zatím není segmentována, rozdělena.

3.2.2 Ostrovní oddělené sítě

V prostředí SŽ se z důvodu kritické infrastruktury vyskytují rovněž oddělené (ostrovní) sítě, ty jsou fyzicky nebo virtuálně síťově odděleny od ostatních sítí pomocí firewallu tak, aby jejich provoz nemohl být narušen. Typickým příkladem mohou být sítě pro elektro dispečinky.

4 Logické síťové prostředí

V logickém síťovém prostředí je aplikován modifikovaný Purdue model pro ICS v podobě 8 vrstev. Potřebné oddělení mezi IT a OT prostředím pomocí industriální DMZ je prováděno IT/OT firewally. Jedná se o zásadní prvek zabezpečení OT provozu.



Obrázek 1: Purdue ICS model

4.1 Komunikace mezi sítěmi

Komunikace mezi sítěmi je řízena na základě výše zmíněného Purdue modelu, je řízena a kontrolována firewally v dané oblasti, firewally v perimetru nebo v datových centrech. Datová komunikace uživatelů je primárně navazována ze zóny s vyšší bezpečnostní úrovní do zóny s nižší bezpečnostní úrovní. Komunikace systémů s nižší bezpečnostní úrovní do zóny s vyšší bezpečnostní úrovní je ve výchozím stavu zakázána. Komunikace mezi jednotlivými OT sítěmi (VRF VPN) jsou řízeny pomocí FW, který je v rámci lokality nebo OŘ anebo centrální v rámci struktury WAN.

4.2 Georedundance

Díky možnostem rozsáhlé sítě Správy železnic se naplno využily výhody georedundance, čili distribuce na více fyzických lokalit, ať už z důvodu vysoké dostupnosti či rozdělení zátěže jednotlivých systémů. V rámci nového perimetru sítě je zajištěna sekundární konektivita do sítě Internet, v tuto chvíli se však nejedná o georedundantní řešení.

4.3 Řešení High Availability

Pro všechny klíčové prvky síťového prostředí je požadován provoz ve vysoké dostupnosti, tedy zajištění síťového provozu bez přerušení pomocí redundance.

- Clustering – redundance dvou a více prvků je možné provozovat v módech active-passive nebo active-active (Load Balancing), např. perimetr sítě je implementován v plném active-active režimu, segmentační firewally jsou v active-passive režimu, vždy záleží na konkrétní implementaci zařízení a nárocích na vysokou dostupnost.
- Síťové prvky i optické propoje páteřní MPLS sítě jsou redundantní a je realizováno připojení vždy z více směrů.

5 Síť APN

Pro některé konkrétní, striktně definované aplikace jsou využívány mobilní služby přenosu dat protokolem LTE nebo GPRS. Každá taková aplikace je provozována v uzavřené síti (APN), zakončená na perimetru SŽ, s definovaným rozsahem IP adres a firewallovými pravidly. Pro přenos dat do sítě UAS se vždy používá DMZ, přímý přístup z APN do sítě Internet je zakázán. Vlastní APN slouží např. pro tablety strojvedoucích, sběr měřených hodnot z kolejových vozidel, IoT a další zařízení nekritické infrastruktury připojené mimo síť Správy železnic.

6 Síťová zařízení

Tato kapitola popisuje seznam komoditních ICT služeb a jednotlivých HW/SW komponent, které tvoří standard v rámci Správy železnic. Cílem je zajistit ve fázích přípravy poptávky, návrhu ICT řešení a realizace dodávky kompatibilitu se stávajícím ICT prostředím a v maximální míře využít již provozované komponenty a technologie. Seznam služeb a komponent je průběžně aktualizován.

6.1 Používané technologie

Níže je výčet a popis základních síťových technologií používaných v prostředí Správy železnic.

6.1.1 VLAN

Aktivní síťové prvky musí plně podporovat VLAN. Pro aktivní datovou komunikaci v sítích SŽ je zakázáno, pokud je to technicky možné, používat defaultní VLAN 1 a tato VLAN se nesmí používat jako nativní (PVID) VLAN na trunk portech. Nastavení trunk portů musí být statické. Automatické vyjednávání je povoleno, jen v krajním případě z technických důvodů na co nejkratší možnou dobu, kdy není jiná možnost.

6.1.2 VRF

Virtual Routing and Forwarding (VRF) je technologie používaná v sítích pro oddělení a izolaci síťového provozu na virtuální síťové segmenty. Každá VRF reprezentuje oddělenou síť, která má vlastní směrovací tabulky a rozhraní. Využívá se zejména v prostředí, kde se vyskytují různé typy síťového provozu, které se musí oddělit a izolovat, aby nedocházelo ke kolizím nebo únikům dat. VRF umožňuje vytvořit více logických sítí v jedné fyzické síti a zajistit tak bezpečné oddělení a izolaci síťového provozu.

Využití VRF VPN se obvykle pojí s technologií MPLS, která umožňuje efektivní směrování a přepínání datových toků mezi jednotlivými virtuálními sítěmi.

VRF Lite je technologie Virtual Routing and Forwarding (VRF) bez podpory MPLS. Oproti VRF VPN, která využívá MPLS pro směrování datových toků mezi různými virtuálními sítěmi, VRF Lite používá standardní směrování IP paketů v sítích založených na protokolu IP.

Správa železnic využívá VRF pro segmentaci MPLS sítí.

6.1.3 Technologie DWDM

U technologie DWDM jde o metodu vlnového multiplexování, díky tomu se optické vlákno využije pro více vlnových délek (více barev) pro oddělené datové přenosy. V rámci celorepublikového řešení síťové infrastruktury Správy železnic jsou použity DWDM propoje mezi jednotlivými lokalitami jako nosná přenosová technologie pro MPLS síť i pro přímé propoje datacenter, kde nejsou k dispozici přímá vlákna. DWDM síť obsahuje mnoho plnohodnotných přípojných bodů a více opakovačů pro zajištění spojů na velkou vzdálenost, zároveň poskytuje redundantní připojení jednotlivých DWDM bodů z více směrů.

Výčet používaných / preferovaných typů zařízení DWDM

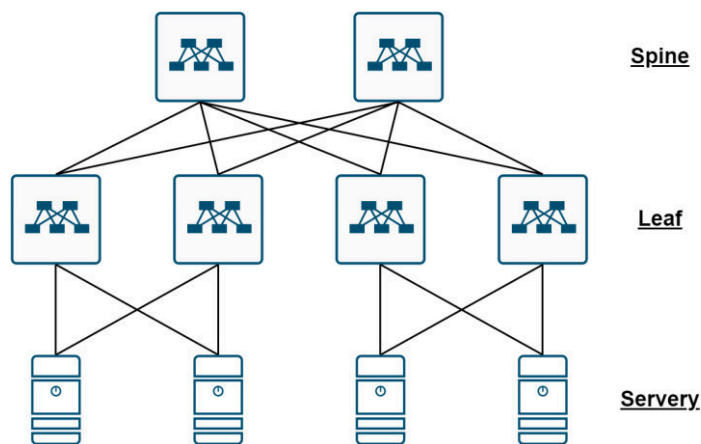
Typ zařízení	Popis	Konkrétní řady
DWDM	Přípojný bod	NCS 1000 NCS 2000

6.1.4 Síť MPLS

MPLS je technologie sítí, která umožňuje efektivní a spolehlivý přenos datových paketů vysokého objemu v rozsáhlých sítích. V prostředí Správy železnic jsou vybudovány dvě MPLS sítě. Stará MPLS síť pro uživatelsko-aplikační síť a některé technologické prvky a nová MPLS síť určená primárně pro technologické datové síť. Záměrem SŽ je starou MPLS síť postupem času opustit.

6.1.5 Síťová spine-leaf topologie

Na rozdíl od klasické 3vrstvé topologie (Access-Distribution-Core) umožňuje Spine-Leaf díky dvouvrstvé topologii mimo jiné snížení latence mezi servery, snížení počtu fyzických switchů v datacentru, snížení počtu hopů při komunikaci mezi servery, zvyšuje propustnost a omezuje riziko vzniku úzkého hrdla.



Obrázek 2: Schéma Spine-Leaf topologie

Všechny nově instalované datacentrové switchy v síťovém prostředí Správy železnic již plně podporují integraci do Spine-Leaf topologie, ať už přímým napojením, nebo jako Remote Leaf.

6.1.6 Technologie Cisco ACI

Cisco ACI (Application Centric Infrastructure) je softwarově definované síťové řešení, které zjednodušuje, automatizuje a zabezpečuje provoz sítí v datových centrech. V prostředí SŽ se používá výhradně v Network-Centric módu, který je síťově zaměřen na tradiční přístup k subnettingu a používání VLAN. Jedná se o poměrně nové řešení, v datových centrech se tato technologie postupně rozšiřuje, z toho důvodu všechny nově instalované switchy v datových centrech již podporují integraci do Cisco ACI.

6.1.7 Síť OOB

V datových centrech SŽ je vyžadováno, aby všechny servery a síťové prvky měly k dispozici dedikovaný síťový port pro dohled a konfiguraci těchto zařízení. Tyto porty se propojují do oddělené OOB (Out-of-band) sítě, která je síťově oddělena od hlavní datové sítě. Lokálně v datovém centru se jedná o fyzicky oddělenou síť, v rámci intranetu jsou odděleny virtuálně pomocí VLAN a VRF.

6.2 Firewally

Vzhledem k množství a různorodosti datových sítí jsou z pohledu kybernetické bezpečnosti firewally nejdůležitějšími síťovými prvky pro Správu železnic. Je kladen velký důraz na striktně oddělené provozy mezi uživatelskými a technologickými sítěmi, mezi uživatelskými sítěmi a datovými centry a samozřejmě mezi sítěmi SŽ a Internetem. Perimetrický firewall musí umožňovat testovací mód FW pravidel, který umožní odladit pravidla bez dopadu na probíhající provoz, dále musí podporovat HA zapojení a distribuovanou konfiguraci. Podle logického umístění firewallu je zvolen konkrétní model viz následující tabulka.

Výčet používaných / preferovaných typů firewallů

Typ routeru	Popis	Konkrétní řady
Perimetr	Hraniční firewall	Palo Alto vyšších řad
Pro segmentaci	Segmentační firewally pro IT síť a IT/OT DMZ	Cisco Firepower 1xxx Cisco Firepower 31x0 Cisco Firepower 4xxx
Pro datová centra	Firewall pro aplikační farmy, clustery, single nody, NAS atd.	Cisco Firepower 31x0 Fortinet Fortigate 600F Fortinet Fortigate 1801F Fortinet Fortigate 2601F
Pro aplikace	Firewall na aplikační vrstvě OSI modelu (WAF)	F5 BIG-IP
Pro load balancing	Loadbalancer pro vyrovnání zátěže serverů	Kemp LoadMaster

6.3 Routery

Routery, nebo také směrovače, jsou zásadní aktivní síťové prvky pro segmentaci sítí. Podle způsobu použití jsou děleny na routery pro provoz v MPLS síti, routery v datových centrech a perimetru sítě, případně pro IT nebo OT síť.

Jsou podporovány routery Cisco s požadovanými protokoly:

- **HSRP** – pro hraniční routery
- **VRF** – pro MPLS routery
- **VRF-Lite** – pro routery bez MPLS
- **BGP** – pro hraniční a MPLS routery
- **TACACS+**
- **RADIUS**

V následující tabulce jsou uváděny jednotlivé řady vždy pro konkrétní použití.

Výčet používaných / preferovaných typů routerů

Typ routeru	Popis	Konkrétní řady
MPLS	Routery typu P, PE a RR v MPLS síti	Cisco ASR Cisco NCS Cisco 8000
MPLS	Routery typu CE	Cisco C9400 Cisco C9300 Cisco C8000 Cisco ISR
IT	Routery pro datová centra a IT síť	Cisco C9300 Cisco ISR
OT	Lokální routery pro OT síť	Cisco IR

6.4 Switche

V prostředí SŽ jsou switche (přepínače) nejčastější síťová zařízení, proto existuje velké riziko možného nasazení nekompatibilních typů s následnou problematickou výměnou za kompatibilní. Obecně jsou preferované switche od renomovaného výrobce Cisco řady C9xxx a pro datacentra řada Nexus 9300, u nichž jsou do značné míry zaručené jednotné konfigurační prostředí (CLI), podpora VLAN bez omezení jejich počtu, kompatibilita používaných síťových protokolů, možnost stohování dedikovaným portem aj.

Jsou požadovány síťové a autorizační protokoly jako:

- **HSRP** – Hot Standby Router Protocol
- **PVST+** – Per-VLAN Spanning Tree Plus
- **TACACS+**
- **RADIUS**

Platí zákaz používání switchů bez managementu. V následujících podkapitolách jsou uváděny jednotlivé řady vždy pro konkrétní použití.

6.4.1 Switche pro datová centra

K již zmiňovaným požadavkům je u switchů pro datová centra vyžadováno redundantní napájení.

Výčet používaných / preferovaných typů

Typ switche	Popis	Konkrétní řady
Spine	Spine switch v topologii Spine-Leaf	Cisco Nexus 9332C Cisco Nexus 9364C
Leaf/ToR	Leaf switch v topologii Spine-Leaf nebo Top of Rack / Top of Row switch	Cisco Nexus 93180YC Cisco Nexus 93240YC Cisco Nexus 93360YC
Backend	Lokální propojení nodů farem (HCI)	Cisco Nexus 93180YC Cisco C9300X
Access	Jako access switch v malých serverovnách	Cisco C9300X Cisco C9300

6.4.2 Switche pro fibre channel

K již zmiňovaným požadavkům je u switchů pro datová centra vyžadováno redundantní napájení.

Výčet používaných / preferovaných typů

Typ switche	Popis	Konkrétní řady
Fibre Channel	Fibre Channel switche převážně pro připojení síťových úložišť typu SAN	Cisco MDS 9124T/V Cisco MDS 9132T/V Cisco MDS 9148T/V

6.4.3 Switche pro kamerové systémy

Pro kamerové systémy jsou požadovány switche s napájením PoE+ podle standardu 802.3at, případně PoE++ podle standardu 802.3bt.

Výčet používaných / preferovaných typů pro kamerové systémy

Typ switche	Popis	Konkrétní řady
Access	Běžný PoE switch pro připojení kamerových systémů	Cisco C9200, resp. C9200L Cisco C9300, resp. C9300L

6.4.4 Switche pro management zařízení

Pro OOB switche v datových centrech platí mimo jiné požadavek na redundantní napájení. V ostatních lokalitách, kde nejsou zajištěny dvě nezávislé napájecí větve, je tento požadavek bezpředmětný.

Výčet používaných / preferovaných typů pro management zařízení

Typ switche	Popis	Konkrétní řady
OOB	Běžný access switch s metalickými RJ45 porty pro připojení MGMT portů	Cisco C9200, resp. C9200L
OOB	Velká datacentra spine-leaf	Cisco Nexus 9348GC

6.4.5 Switche pro lokální síť

Tyto switche pro lokální síť musí být umístitelné v 19" racku přímo na jeho ližiny. Redundantní zdroj není vyžadován.

Výčet používaných / preferovaných typů pro lokální síť

Typ switche	Popis	Konkrétní řady
Access	Běžný access switch pro připojení pracovních stanic, tiskáren atp.	Cisco C9200 všech variant Cisco C9300 všech variant
OT	Lokální switche pro OT síť	Cisco IE2xxx
End of Support	Dosluhující řada, postupně se nahrazují	Cisco C2960 více variant Cisco C2950

6.5 Bezdrátová zařízení

Tato zařízení pro obsluhu bezdrátových sítí (WLAN) jsou používána v prostředí Správy železnic.

Výčet používaných / preferovaných typů pro zařízení pro bezdrátová síť

Typ zařízení	Popis	Konkrétní řady
Controller	Controller pro bezdrátové síť WLAN	Cisco Catalyst 9800
Access Point	Bezdrátové přípojné body (AP)	Cisco Catalyst 91xx

6.6 Huby

Ethernetový hub neboli síťový rozbočovač se v prostředí SŽ nenachází a jeho použití je zakázané.

6.7 Modemy a datová zařízení

V prostředí rozlehlé sítě SŽ se používají různé typy modemů, tedy zařízení pro převod mezi digitálním a analogovým rozhraním. Jde např. o GSM modemy s protokolem LTE nebo GPRS, DSL modemy, 2-pair / dial-up.

Výčet používaných / preferovaných modemů a datových zařízení

Výrobce	Technologie	Popis	Konkrétní řady/modely
Patton	DSL		1088, 3200, 3088
Albis / Siemens	DSL		BSTU4 / ULAF+
RAD	DSL		ASMI50
Patton	2-pair		3202

CONEL	GPRS	GPRS modem, již ukončená výroba	ER75i
Siemens	GPRS		M35i
Teltonika	4G/LTE	Průmyslové LTE routery s rozhraním RS232, RS485, Ethernet, M-bus	TRBxxx
Advantech	4G/LTE	Průmyslové LTE routery s rozhraním RS232, RS485, Ethernet	ICR-xxxx

6.8 Centralizovaná správa síťových prvků

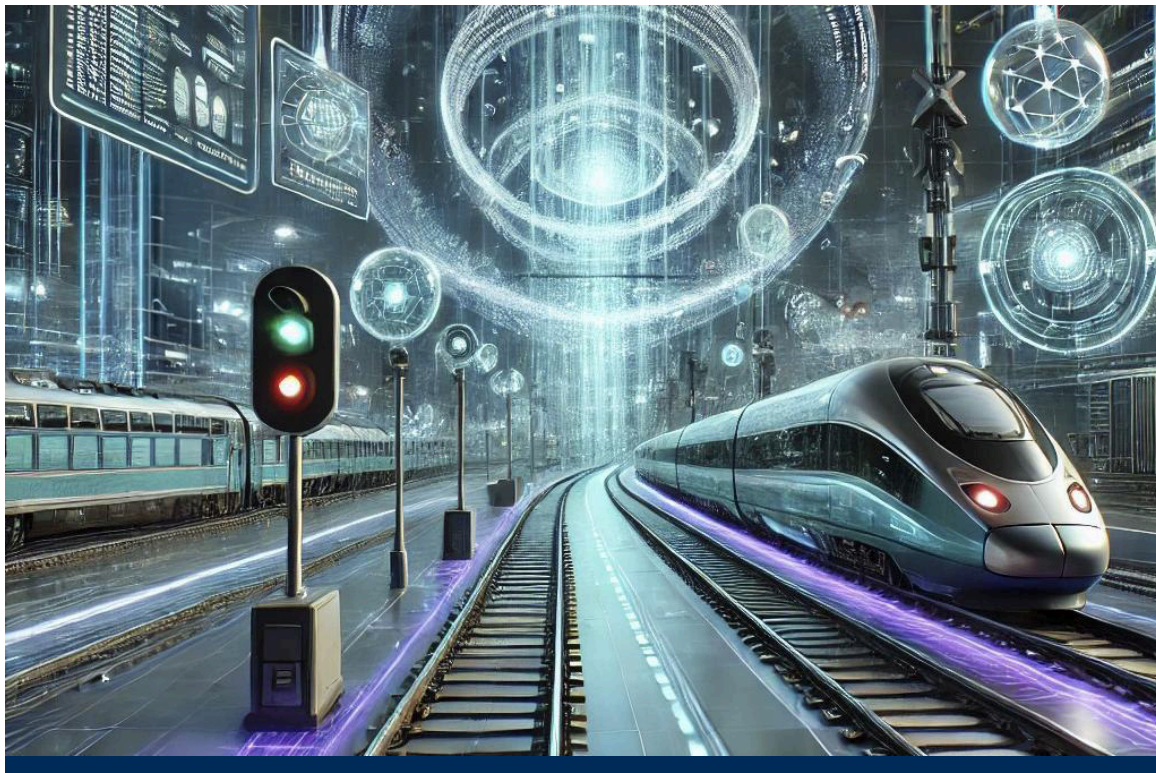
V prostředí Správy železnic se pro centralizovanou správu síťových prvků používají nástroje Cisco Catalyst Center (dříve Cisco DNA Center) a Cisco Nexus Dashboard Fabric Controller (dříve Cisco Data Center Network Manager). Tyto nástroje slouží pro správu, maintainance, aktualizace, zajištění jednotné konfigurace pomocí šablon i dohled nad celou sítí.

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Integrační standardy

Červen 2025

Obsah

1	Úvod	4
2	Moderní architektonické rámce	4
2.1	Flexibilita	4
2.2	Škálovatelnost	4
2.3	Bezpečnost	4
2.4	Efektivita	4
3	Architektura integrací	5
3.1	Microservices Architecture	5
3.2	Event-Driven Architecture	5
3.3	API-First Approach	5
3.4	Hybridní architektura	5
4	Typy integrací	5
5	Softwarová architektura Enterprise Service Bus	6
6	Primární integrační scénáře	6
6.1	Integrační platforma	6
6.2	SAP Business Technology Platform	7
6.3	Microsoft nástroje a Azure	7
6.4	Integrace stávajících aplikací	7
7	Datové formáty	9
8	Metody	10
9	Dokumentace integračních scénářů	10
10	Řízení integračních scénářů	11

Seznam zkratek

API	Komplexně definované komunikační rozhraní aplikace (<i>Application Programming Interface</i>)
CSV	Jednoduchý textový souborový formát (Comma-separated values)
ESB	Softwarová architektura a technologie používaná v oblasti podnikové integrace a správy služeb (<i>Enterprise Service Bus</i>)
IoT	Internet věcí je souborné označení pro síť fyzických zařízení, která vzájemně, centrálně nebo i s vnějším světem komunikují a mají možnost předávat data. Každé z těchto zařízení je jasně identifikovatelné díky implementovanému výpočetnímu systému, ale přesto je schopno pracovat samostatně v existující infrastruktuře sítě (<i>Internet of Things</i>)
IT	Informační technologie (<i>Information Technology</i>)
ITIL	(<i>Information Technology Infrastructure Library</i>)
JSON	Datový formát primárně určený pro přenos dat (<i>JavaScript Object Notation</i>)
KII	Kritická informační infrastruktura
REST/API	Webově založené klient-server API (<i>Representational State Transfer</i>)
SAP	Modulární ERP systém od německé firmy SAP AG
SFTP	Zabezpečený protokol pro přenos souborů. Pro zajištění šifrování využívá protokol SSH (<i>SSH File Transfer Protocol</i>)
SMTP	Základní síťový protokol pro přenos elektronické pošty (<i>Simple Mail Transfer Protocol</i>)
SOA	Architektura orientovaná na služby – jedná se o softwarovou architekturu, která se zaměřuje na organizaci a strukturu aplikací a systémů jako soubor nezávislých a dobře definovaných služeb (<i>Service-Oriented Architecture</i>)
SŽ	Správa železnic, státní organizace
XML	Standardizovaný jazyk používaný pro serializaci dat (<i>Extensible Markup Language</i>)

Seznam vysvětlivek

Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.
Platforma WSO2	Open-source platforma pro správu služeb (ESB) a integraci aplikací (API Management) vyvinutá společností WSO2 Inc. WSO2 poskytuje komplexní sadu nástrojů a produktů, které pomáhají organizacím implementovat a spravovat architekturu orientovanou na služby (SOA) a rozhraní pro programování aplikací (API) v jejich IT infrastruktuře.

1 Úvod

Tento dokument slouží jako příloha k základního dokumentu Platformy SŽ, který je součástí veřejných zakázek a podrobněji rozvádí integrační standardy naší organizace. Cílem je poskytnout jasný a konzistentní rámec pro všechny integrační aktivity. Naše cíle dále zahrnují modernizaci a konsolidaci současných integračních mechanismů za účelem zvýšení efektivity a snížení nákladů na údržbu. Dokument specifikuje požadavky a standardy, které musí být dodrženy při implementaci integračních scénářů, s důrazem na bezpečnost a využití hybridních řešení kombinujících on-premise a cloudovou infrastrukturu s ohledem na celkovou IT strategii. Všechny aktivity musí cílit na ITIL rámec pro řízení IT služeb, neboť tímto rámcem se naše organizace rozhodla řídit IT služby.

2 Moderní architektonické rámce

V rámci moderního IT prostředí naše organizace využívá pro nová řešení různé architektonické rámce a principy k zajištění flexibility, škálovatelnosti a efektivního poskytování služeb. Tato kapitola se zaměřuje na popis klíčových architektonických principů a jejich implementaci v naší organizaci. Použití současně moderní architektury nám umožňují efektivně reagovat na měnící se potřeby a technologické požadavky.

2.1 Flexibilita

Naše architektura umožňuje snadné přizpůsobení se měnícím se potřebám businessu. Tím, že kombinujeme lokální a cloudové infrastruktury, jsme schopni efektivně reagovat na dynamické požadavky a přizpůsobit naše služby v reálném čase. Hybridní řešení nám umožňují optimalizaci výkonu a nákladů tím, že strategicky využíváme výhody obou typů prostředí. Tato flexibilita nám dává možnost optimalizovat zdroje podle aktuálních potřeb a strategických cílů, ale hlavně dodržování bezpečnostních kritérií.

2.2 Škálovatelnost

Díky využití mikroslužeb a škálovatelné cloudové infrastruktury můžeme dynamicky přizpůsobovat kapacitu našich systémů podle aktuální požadavků. To zajišťuje, že naše služby jsou vždy dostupné a výkonné, i při náhlých změnách v zatížení. Implementujeme mechanismy automatického škálování, které umožňují plynulý růst a adaptaci bez potřeby manuálního zásahu, což přispívá k vyšší efektivitě a spolehlivosti.

2.3 Bezpečnost

Naše integrační architektura zahrnuje robustní bezpečnostní opatření na všech úrovních. Zajišťujeme ochranu dat a služeb pomocí pokročilých metod autentizace a autorizace, šifrování dat a pravidelného monitorování bezpečnostních hrozeb. Primárně z pohledu Compliance a regulace dbáme na dodržování všech relevantních bezpečnostních standardů a právních předpisů, což zajišťuje důvěryhodnost a právní jistotu pro business partnery.

2.4 Efektivita

Využití automatizace v rámci integračních procesů nám umožňuje snížit provozní náklady a zvýšit produktivitu. Automatizované workflow a orchestrace služeb minimalizují potřebu manuálních zásahů a zvyšují přesnost a rychlost procesů. Tohoto stavu jsme dosáhli díky centrálnímu řízení integrací prostřednictvím platformy ESB, ta nám umožňuje efektivně monitorovat a spravovat všechny integrační toky, což přispívá k vyšší přehlednosti a lepší koordinaci mezi jednotlivými systémy.

3 Architektura integrací

V rámci naší organizace se zaměřujeme na implementaci moderní architektury integrací, která podporuje jak on-premise, tak cloudové prostředí. Tato hybridní přístup zajišťuje flexibilitu, škálovatelnost a bezpečnost, což jsou klíčové faktory pro úspěšné řízení IT služeb podle ITIL principů. Cílový stav architektury je ESB.

Naše integrační architektura je postavena hlavně na následujících architekturních principech:

3.1 Microservices Architecture

Naše organizace implementuje architekturu mikroslužeb, což znamená decentralizaci a rozdělení monolitických aplikací na menší, nezávislé služby. Tento přístup zajišťuje vysokou flexibilitu a usnadňuje správu jednotlivých služeb. Díky mikroservisům můžeme rychleji reagovat na změny a inovace, což nám umožňuje poskytovat kvalitnější služby našim zákazníkům v podobě businessu.

3.2 Event-Driven Architecture

Pro lepší škálovatelnost a reaktivitu využíváme architekturu řízenou událostmi. Tento přístup umožňuje systémům komunikovat prostřednictvím událostí, což zvyšuje jejich schopnost rychle reagovat na provozní incidenty. Díky tomu můžeme dosahovat vyšší efektivity a pružnosti v našich provozních procesech.

3.3 API-First Approach

Při návrhu a vývoji systémů se naše organizace řídí principem API-First. API jsou navrhována a vyvíjena jako primární prostředek komunikace mezi systémy. Tento přístup je v souladu s ITIL principy, které se zaměřují na poskytování hodnoty zákazníkům prostřednictvím dobře definovaných služeb. API-First nám umožňuje dosahovat vyšší konzistence a standardizace v naší IT infrastruktuře.

3.4 Hybridní architektura

Pro zajištění flexibility a škálovatelnosti kombinujeme on-premise a cloudová řešení. Tento hybridní přístup nám umožňuje využívat výhod obou prostředí, což zajišťuje kontinuitu služeb a splnění compliance požadavků. Díky hybridní architektuře můžeme optimalizovat naše IT zdroje a lépe podporovat business v naší organizaci. Toto je obzvláště důležité z důvodu kritické infrastruktury informací (KII), která vyžaduje vysokou míru bezpečnosti a spolehlivosti. Hybridní přístup nám umožňuje zajistit, že klíčové systémy a data jsou chráněny a zároveň flexibilně škálovatelné dle aktuálních potřeb.

4 Typy integrací

Pro celkové pochopení integrací je nutné zmínit úrovně integrací. Existuje totiž několik pohledů, které následně definují oblasti soustředění a úroveň detailu. Je potřeba podotknout, že při komplexním řešení integrací dochází k jejich vzájemnému prolínání. Zde jsou vyjmenovány ty hlavní z nich:

- **Datová integrace** – Tento typ integrace se zabývá shromažďováním dat z různých zdrojů a jejich následným poskytnutím uživatelům v jednotné a konzistentní struktuře a formátu. Datová integrace umožňuje kombinaci dat umístěných v různých zdrojích a poskytuje uživateli sjednocený pohled na tyto data.
- **Procesní integrace** – Procesní integrace má za cíl propojit aplikace z hlediska podnikových procesů. Jakmile skončí jedna činnost, je vykonána činnost druhá. Při dokončení prvního procesu se spustí proces další, a tím že různé procesy mohou být realizovány odlišnými subsystemy je důležité zajistit, že tyto procesy jsou správně a efektivně koordinovány.

- **Aplikační integrace** – U aplikační integrace jde v zásadě o realizaci výměny informací (různého charakteru) mezi různými aplikacemi. Výměna přitom může probíhat s využitím široké škály transportních technologií – např. přes webové služby, databáze, sdílený soubor, messaging apod.
- **Systémová integrace** – Systémová integrace je proces spojování různých softwarových komponent, subsystémů, v jeden fungující celek. Cílem je, aby tento celek pracoval co možná nejefektivněji, tedy z pohledu jednotlivých subsystémů, aby komunikace mezi nimi probíhala podle definovaného schématu.

Každý z těchto typů integrace má své výhody a nevýhody a je důležité na základě analýz vybrat ten vhodný typ integrace, který bude respektovat konkrétní potřeby a požadavky jednotlivých projektů.

5 Softwarová architektura Enterprise Service Bus

ESB je softwarová architektura pro distribuované výpočty. ESB implementuje komunikační systém mezi vzájemně interagujícími softwarovými aplikacemi v rámci SOA. ESB je centralizovaný, standardizovaný hub, který přijímá, transformuje a poskytuje data, aby různé aplikace a služby napříč organizací mohly snadno komunikovat. ESB je cílový stav architektury, která je preferovaná v naší organizaci. Vzhledem ke složitosti prostředí však je doplňován i jinými způsoby integrací na základě výše popsáných architektur integrací.

ESB poskytuje hlavně tyto funkce:

- **Transformace dat** – provádí transformování zpráv do formátů, které jsou pro příjemce zpracovatelné a srozumitelné
- **Směrování zpráv** – dokáže rozhodovat, kam má zprávu odeslat na základě atributů obsažených v obsahu daných zpráv
- **Mediace služeb** – může poskytnout jednotné rozhraní pro více služeb
- **Orchestrace** – koordinuje interakce mezi službami

ESB je navržen tak, aby zjednodušil vazby a pomohl se oprostit od „Spaghetti“ architektury, která v organizaci zatím dominuje. ESB je sada nástrojů, která posílá zprávu přímo do konkrétní destinace mezi buď aplikací a/nebo komponentami. Ať už je to klient nebo proces, cokoli, co je připojeno k ESB, nekomunikuje přímo mezi sebou, protože komunikují prostřednictvím samotného ESB platformy.

6 Primární integrační scénáře

6.1 Integrační platforma

Naše organizace plánuje rozvinout integrační platformu WSO2 do podoby ESB, který bude sloužit jako hlavní integrační páteř. WSO2 bude poskytovat následující funkcionality:

- **Service Orchestration** – Koordinace a řízení komunikace mezi různými službami, což podporuje efektivní řízení provozu služeb a incidentů.
- **Data Transformation** – Převod a mapování datových formátů mezi různými systémy, což umožňuje jednotné zpracování dat v rámci celé infrastruktury.
- **Security Enforcement** – Implementace bezpečnostních politik a autentizace, což je klíčové pro řízení rizik a zajištění integrity služeb.

6.1.1.1 Preferované Protokoly pro Integraci s WSO2

- **REST/HTTPS** – Pro aplikační a datové integrace díky své jednoduchosti a široké podpoře, což umožňuje snadnou správu a podporu služeb.
- **SOAP** – Pro integrace, kde je vyžadována robustní bezpečnost a transakční podpora, což je v souladu s potřebami řízení kritických služeb.
- **MQTT** – Pro event-driven integrace a IoT komunikace, které podporují rychlou reakci na změny a incidenty.
- **AMQP** – Pro spolehlivý a škálovatelný messaging mezi aplikacemi, což zajišťuje stabilní a efektivní komunikaci.

6.2 SAP Business Technology Platform

SAP BTP hraje klíčovou roli v naší integrační strategii. Specifické požadavky na integraci SAP BTP zahrnují:

- **Integration Suite** – Použití SAP Integration Suite pro propojení SAP a non-SAP systémů, což podporuje jednotnou správu a provoz služeb.
- **Event Mesh** – Využití SAP Event Mesh pro událostmi řízenou architekturu, což umožňuje rychlé a efektivní řízení změn a incidentů.
- **Business Process Management** – Automatizace a optimalizace obchodních procesů pomocí SAP Workflow Management, což zajišťuje efektivní poskytování služeb.

6.2.1.1 Preferované Protokoly pro Integraci s SAP BTP

- **OData** – Pro přístup k datům a jejich manipulaci přes standardizované API, což podporuje transparentní správu dat.
- **RFC/BAPI** – Pro volání vzdálených funkcí v SAP systémech, což zajišťuje spolehlivou integraci služeb.
- **IDoc** – Pro elektronickou výměnu dat mezi SAP a non-SAP systémy, což umožňuje efektivní řízení datových toků.
- **SOAP** – Pro služby vyžadující vysokou úroveň bezpečnosti a transakční podporu, což zajišťuje integritu a důvěryhodnost služeb.

6.3 Microsoft nástroje a Azure

Integrace s Microsoft technologiemi, včetně Azure, zahrnuje tyto základní komponenty:

- **Azure Logic Apps** – Automatizace a orchestraci pracovních toků, což podporuje efektivní správu a provoz služeb.
- **Azure API Management** – Správa a bezpečné publikování API, což zajišťuje jednotný přístup a kontrolu nad službami.
- **Azure Service Bus** – Spolehlivá messagingová platforma pro integraci aplikací, což podporuje stabilní a efektivní komunikaci.
- **Azure Arc** – Pro správu a orchestraci zdrojů v hybridním prostředí, což umožňuje jednotnou správu a kontrolu napříč on-premise a cloudovými systémy.

6.3.1.1 Preferované Protokoly pro Integraci s Azure

- **REST/HTTPS** – Pro širokou škálu aplikačních a datových integrací, což podporuje snadnou správu a podporu služeb.
- **gRPC** – Pro vysoce výkonné, nízko-latentní komunikace mezi mikroservisami, což zajišťuje rychlou a efektivní komunikaci.
- **Event Grid** – Pro event-driven architekturu a notifikace, což umožňuje rychlou reakci na změny a incidenty.
- **Service Bus** – Pro messaging a integraci podnikových aplikací, což zajišťuje spolehlivou komunikaci a řízení služeb.

6.4 Integrace stávajících aplikací

Mnoho aplikací, je stále ještě integrováno point-to-point, ty budou postupně převedeny do centralizovaného integračního prostředí. Hlavní kroky zahrnují:

- **Inventarizace a Analýza** – Zmapování současných integrací a identifikace klíčových závislostí, což podporuje efektivní správu a plánování změn.
- **Standardizace API** – Vytvoření standardních API pro všechny aplikace, což zajišťuje jednotný přístup a kontrolu nad službami.
- **Refaktoring a Modernizace** – Přepsání nebo refaktoring stávajících integrací podle moderních standardů, což podporuje efektivní a bezpečné poskytování služeb.

Tabulka protokolů

Protokol	Použití	Výhody	Nevýhody	Důvod Preference/Nepreference
REST/HTTPS	Aplikační, datové	Jednoduchost, široká podpora, škálovatelnost	Omezená bezpečnost ve srovnání s jinými protokoly	Preferovaný pro svou jednoduchost a širokou podporu
SOAP	Kritické služby	Vysoká úroveň bezpečnosti, transakční podpora	Složitost, větší režie	Preferovaný pro kritické a transakční služby
MQTT	Event-driven, IoT	Nízká režie, efektivní pro nízko-šířková pásma	Omezená podpora pro složitější operace	Preferovaný pro IoT a event-driven architekturu
AMQP	Messaging	Spolehlivost, škálovatelnost	Komplexita implementace	Preferovaný pro spolehlivý a škálovatelný messaging
OData	Data, API	Standardizace, jednoduchý přístup k datům	Omezená funkčnost ve srovnání s plně funkčními API	Preferovaný pro transparentní správu dat
RFC/BAPI	SAP integrace	Efektivní volání SAP funkcí	Specifické pro SAP	Preferovaný pro spolehlivou integraci SAP
IDoc	EDI, SAP integrace	Robustní, vhodné pro velké objemy dat	Specifické pro SAP, složitost	Preferovaný pro EDI a integraci SAP
WebSocket	Real-time komunikace	Obousměrná komunikace, nízká latence	Omezená bezpečnost	Preferovaný pro real-time aplikace
gRPC	Mikroservisy	Vysoký výkon, nízká latence	Menší podpora ve srovnání s HTTP	Preferovaný pro výkonné komunikace mikroservis
FTP/SFTP	Přenos souborů	Jednoduchost, široká podpora	Zastaralost (FTP), bezpečnostní rizika (FTP)	Preferovaný (SFTP) pro bezpečný přenos souborů, FTP je nepreferovaný kvůli bezpečnostním rizikům
JMS	Messaging	Spolehlivost, asynchronní komunikace	Komplexita, omezená podpora	Preferovaný pro robustní messagingové potřeby
SMTP	Email	Široká podpora, standardní pro email	Zastaralost, omezená bezpečnost	Nepreferovaný pro datové a aplikační integrace kvůli zastaralosti
CORBA	Distribuované aplikace	Jazyková nezávislost, robustnost	Komplexita, zastaralost, velká režie	Nepreferovaný kvůli zastaralosti a komplexitě
RMI	Java aplikace	Efektivní pro Java, jednoduchost	Omezené na Java, bezpečnostní rizika	Nepreferovaný kvůli omezené použitelnosti mimo Java a bezpečnostním rizikům
Telnet	Vzdálená správa	Široká podpora	Velmi slabá bezpečnost (nešifované)	Nepreferovaný kvůli vážným bezpečnostním rizikům

XMPP	Real-time komunikace	Široká podpora, rozšiřitelnost	Omezená škálovatelnost, bezpečnostní problémy	Nepreferovaný kvůli omezené škálovatelnosti a bezpečnostním problémům
------	----------------------	--------------------------------	---	---

Tabulka poskytuje přehled preferovaných a nepreferovaných protokolů pro integrační architekturu naší organizace, zdůvodňuje jejich použití a vyzdvihuje klíčové výhody a nevýhody. Protokoly jako REST/HTTP, SOAP, MQTT, AMQP a další jsou preferovány pro svou robustnost, flexibilitu a bezpečnost. Naopak protokoly jako FTP (nešifované), SMTP, CORBA, RMI, Telnet a XMPP jsou nepreferované kvůli jejich zastaralosti, bezpečnostním rizikům nebo omezené funkčnosti.

7 Datové formáty

V rámci organizace je klíčové zajistit efektivní, bezpečnou a interoperabilní výměnu dat mezi různými informačními systémy a platformami. Výběr vhodných datových formátů hraje zásadní roli při dosahování těchto cílů. Datový formát určuje způsob, jakým jsou informace strukturovány a jakým způsobem mohou být přenášeny a zpracovávány mezi různými systémy. V této části se zaměříme na nejčastěji používané datové formáty, jejich typické použití, výhody, nevýhody a důvody, proč jsou preferovány nebo nepreferovány v naší organizaci, se zvláštním důrazem na bezpečnostní aspekty. Kromě toho uvádíme níže v tabulce i formáty, které jsou z bezpečnostních nebo jiných důvodů nevhodné a v podstatě zakázané.

Tabulka datových formátů

Formát	Použití	Výhody	Nevýhody	Důvod Preference/Nepreference
REST/HTTPS	Aplikační, datové	Jednoduchost, široká podpora, škálovatelnost	Omezená bezpečnost ve srovnání s jinými protokoly	Preferovaný pro svou jednoduchost a širokou podporu
JSON (JavaScript Object Notation)	Webové API, konfigurace, mobilní aplikace	Jednoduchost, čitelnost, podpora v moderních programovacích jazycích	Není vhodný pro složité datové struktury, bez schématu	Preferován pro svou jednoduchost a širokou podporu, bezpečnostní riziko lze mitigovat validací a šifrováním
XML (eXtensible Markup Language)	Webové služby, dokumenty, datová výměna mezi systémy	Flexibilita, podporuje složité datové struktury, možnost validace pomocí XSD	Verbóznost, vyšší nároky na výkon	Preferován pro komplexní strukturovaná data, bezpečnost lze zlepšit pomocí šifrování a podpisů
CSV (Comma-Separated Values)	Export/import dat, tabulkové aplikace	Jednoduchost, široká podpora v aplikacích	Omezená strukturovanost, citlivost na formátování	Preferován pro jednoduchou tabulkovou data, nepreferován pro složité struktury, bezpečnostní riziko při přenosu nešifrovaných dat
YAML (YAML Ain't Markup Language)	Konfigurace, data pro DevOps nástroje	Čitelnost, jednoduchost, podpora komplexních datových struktur	Méně robustní než XML, obtížnější validace	Preferován pro konfigurace a čitelnost, nepreferován pro kritická data kvůli chybějícímu schématu a validaci
EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport)	EDI v obchodních a státních systémech	Standardizace, spolehlivost, široká akceptace v EDI	Složitost, náročná implementace	Preferován pro standardizované obchodní procesy, bezpečnostní riziko lze řešit šifrováním EDI zpráv
Plain Text (neformátovaný text)	Základní komunikace, logy	Jednoduchost, univerzální čitelnost	Žádná strukturovanost, vysoké riziko chyb	Zakázán pro přenos citlivých dat, protože postrádá jakoukoliv formu zabezpečení a struktury

HTML (HyperText Markup Language)	Webové stránky, obsah dokumentů	Flexibilita, široká podpora v prohlížečích	Neefektivní pro strukturovaná data, riziko XSS útoků	Zakázán pro datovou výměnu kvůli bezpečnostním rizikům a nevhodnosti pro strukturovaná data
Proprietární Formáty (např. specifické formáty určitého softwaru)	Specifické aplikace	Optimalizace pro konkrétní software	Omezená interoperabilita, závislost na konkrétním dodavateli	Zakázány kvůli uzamčení na jednoho dodavatele a nízké interoperabilitě, což zvyšuje riziko vendor lock-in

Tabulka níže poskytuje přehled jednotlivých datových formátů, jejich specifické použití, výhody a nevýhody, a důvody preference či nepreference v kontextu naší organizace.

8 Metody

Metody integrací se liší v závislosti na povaze dat, četnosti výměny, úrovni transformace dat a typu architektury integrace dat. Metody primárně využívané naší organizací lze rozdělit na tyto čtyři základní:

- **ETL - extract, transform, load** – je běžnou metodou pro dávkové/hromadné zpracování velkých objemů strukturovaných nebo částečně strukturovaných dat
- **ELT extract, load, transform** – je podobná ETL, ale transformace se provádí až po načtení do cílového místa určení
- **CDC - change data capture** – zachycuje a přenáší pouze změny ve zdrojových datech a je užitečná pro integraci v reálném čase nebo téměř v reálném čase
- **Virtualizace dat** – vytváří virtuální vrstvu, která integruje data z různých zdrojů, aniž by je fyzicky přesouvala nebo ukládala, tato metoda poskytuje jednotný pohled na data a je vhodná pro komplexní a heterogenní datová prostředí

9 Dokumentace integračních scénářů

V naší organizaci je dokumentace integračních scénářů klíčovým nástrojem pro zajištění přehlednosti a konzistence v rámci všech integračních aktivit. Pro tento účel používáme standardizovaný dokument s názvem Integrační specifikace, který obsahuje veškeré potřebné informace k pochopení, implementaci a konfiguraci konkrétního integračního scénáře. Tento dokument slouží jako detailní blueprint pro všechny zúčastněné strany.

9.1.1.1 Integrační specifikace zahrnuje primárně:

- Stručný popis integračního scénáře, jeho účel a přínosy.
- Název integračního scénáře přidělený dle katalogu Integračních scénářů a zavedené jmenné konvence, což zajišťuje konzistenci a snadnou identifikaci.
- Popis technologií, protokolů a datových formátů použitých v integraci.
- Detailní popis procesních a datových toků, které jsou součástí integračního scénáře.
- Specifikace bezpečnostních opatření, jako je šifrování, autentizace a autorizace.

Kromě textového popisu využíváme modelovací jazyky, jako je Archimate v poslední platné verzi, pro vizualizaci integračních scénářů. Tyto modely poskytují grafický přehled o architektuře, komponentách a vztazích mezi nimi, což usnadňuje pochopení komplexních integrací.

9.1.1.2 Další používané modelovací jazyky zahrnují:

- UML (Unified Modeling Language) - Pro vytváření diagramů tříd, sekvencí a aktivit, které detailně popisují jednotlivé části integračního scénáře.

- BPMN (Business Process Model and Notation) - Pro modelování procesů organizace a jejich interakcí v rámci integračních scénářů.

Integrace jsou v naší organizaci také popsány v katalogu Integračních scénářů, který obsahuje všechny aktuální a historické integrační scénáře s příslušnými metadaty. Tento katalog je pravidelně aktualizován a slouží jako centrální zdroj informací pro všechny týmy zapojené do integračních projektů.

Dokumentace integračních scénářů je důkladně verifikována a validována, aby byla zajištěna její přesnost a úplnost. To zahrnuje revize od technických odborníků, bezpečnostních specialistů a dalších relevantních stakeholderů. Tento proces zajišťuje, že všechny integrační aktivity jsou prováděny konzistentně, efektivně a bezpečně.

10 Řízení integračních scénářů

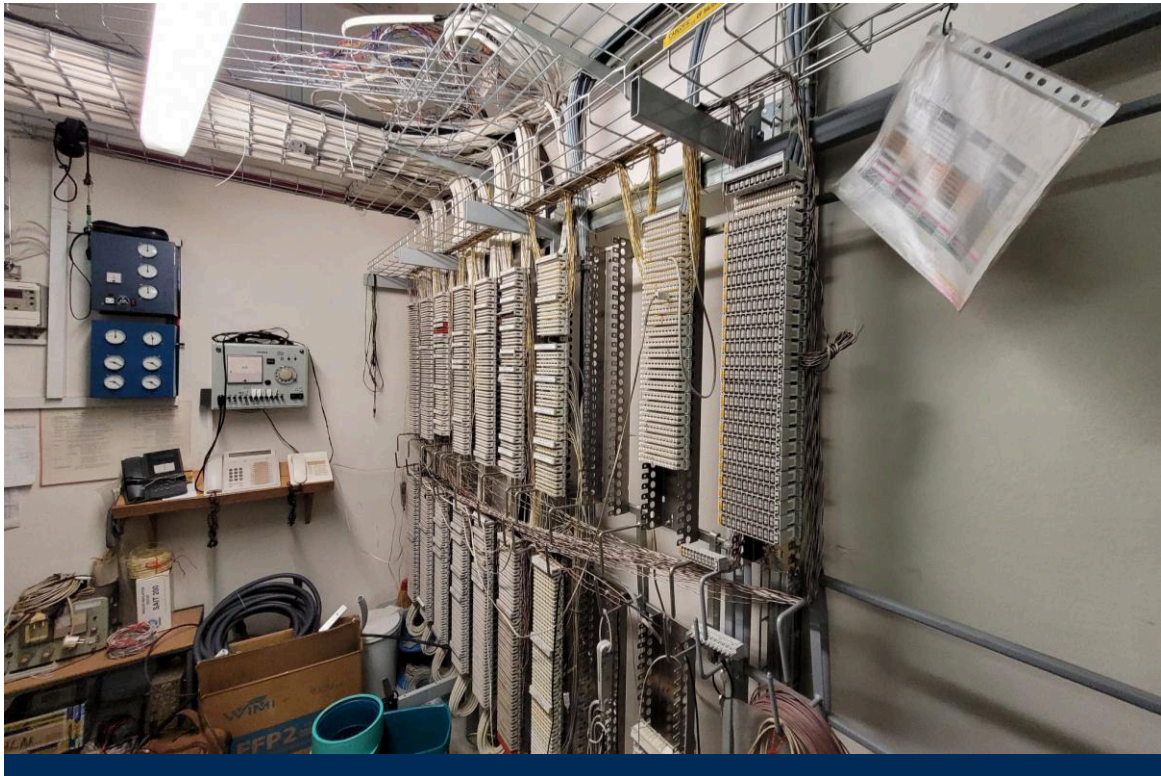
Jakékoliv nové Integrační scénáře, či změny Integračních scénářů musí projít skrze Architecture Board nebo Change management a být posouzeny v širším kontextu. Skrze jaký proces bude integrační scénář posuzován určí matice, která zahrnuje posouzení složitosti změny a její dopady. Integrační scénář následně bude nově zaevidován do katalogu Integračních scénářů nebo proběhne aktualizace u již existujícího.

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Komunikační standardsy

Červen 2025

Obsah

1	Úvod	4
2	Komunikační služby	4
3	SMS brána	4
4	Emailová komunikace.....	4
4.1	Z uživatelsko-aplikační sítě	4
4.2	Z technologických datových sítí	4
4.3	Z externích sítí Správy železnic.....	4
4.4	Mimo sítě Správy železnic	5
5	Komunikační platforma dispečerských pracovišť.....	5

Seznam zkratek

API	Komplexně definované komunikační rozhraní aplikace (<i>Application Programming Interface</i>)
APN	Virtuální vyhrazená část mobilní datové sítě. Nejedná se tak o mobilní připojení k Internetu, ale k lokální síti daného zákazníka mobilního operátora.
CPS	Centrální poštovní systém Správy železnic
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
O27	Odbor komunikace GŘ SŽ
SAP	Modulární ERP systém od německé firmy SAP AG
SMS	Krátká textová zpráva (<i>Short Message Service</i>)
SMTP	Základní síťový protokol pro přenos elektronické pošty (<i>Simple Mail Transfer Protocol</i>)
SŽ	Správa železnic, státní organizace
SŽT	Správa železničních informačních technologií
UAS	Logická uživatelsko-aplikační síť SŽ, zahrnuje VRF v MPLS sítích a lokální VLAN, běžně se nazývá také „Intranet SŽ“
VPN	Virtuální privátní síť (<i>Virtual Private Network</i>)

Seznam vysvětlivek

Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.
---------------------	--

1 Úvod

Cílem této přílohy Platformy SŽ je popsat podporovaných komunikačních služeb a technologií, které lze v rámci Platformy SŽ využít a současně definuje služby, zařízení a technologie, které není možné z důvodu duplicity v rámci navrhovaných řešení dodávat do ICT prostředí Správy železnic.

2 Komunikační služby

Platforma Správy železnic definuje základní komunikační služby, které lze v rámci aplikací a informačních systémů využívat primárně technické notifikace. Použití k jiným účelům (například pro marketingové účely nebo komunikaci s veřejností) je možná jen po předchozím schválení ze strany Správy železnic, a to minimálně ze strany SŽT a O27.

3 SMS brána

SMS je negarantovaná služba telekomunikačních operátorů. Garantován není čas doručení ani samotné doručení SMS zprávy vůbec. SMS brána je aplikace instalovaná v prostředí SŽ napojená přímo na telekomunikačního operátora. Nejedná se tedy o použití koncového zařízení přihlášeného do veřejné mobilní telefonní sítě.

SMS brána umožňuje obousměrnou komunikaci, to znamená odesílání SMS zpráv definovaným příjemcům a příjem odpovědí na odeslané zprávy. Stejně tak umožňuje evidenci (logování) doručenek zpráv. Komunikaci se SMS bránou zajišťuje jednoduché API rozhraní popsané v implementačním manuálu.

Službu SMS brány lze využít jen pro aplikace a informační systémy umístěné v ICT prostředí Správy železnic a to pouze v UAS.

4 Emailová komunikace

Pro navrhovaná řešení, pokud je součástí i emailová komunikace, poskytuje službu emailového serveru pro odchozí poštu. Je pro aplikace odpůrné služby standardně poskytované k využití pro dodávaná ICT řešení.

4.1 Z uživatelsko-aplikační sítě

Z UAS je služba odesílání emailových zpráv zprostředkována takto:

- Nešifrovaně přes CPS a jeho Open-Relay SMTP servery umístěné ve vnitřní síti
- Šifrovaně přes služby MS Exchange

4.2 Z technologických datových sítí

Z technologických datových sítí není v současné době služba odesílání elektronické pošty podporována.

4.3 Z externích sítí Správy železnic

Z externích sítí a připojení Správy železnic (VPN a APN) není služba odesílání emailových zpráv dostupná.

4.4 Mimo síť Správy železnic

Odesílání emailové komunikace z vnějších sítí mimo perimetr Správy železnic (například SAP Cloud, MS Azure atp.) není v současné době možné.

Pro tuto službu je nutné využít lokálních SMTP služeb s omezením, že z technických a bezpečnostních důvodů nelze takto odesílat emaily z domén Správy železnic.

5 Komunikační platforma dispečerských pracovišť

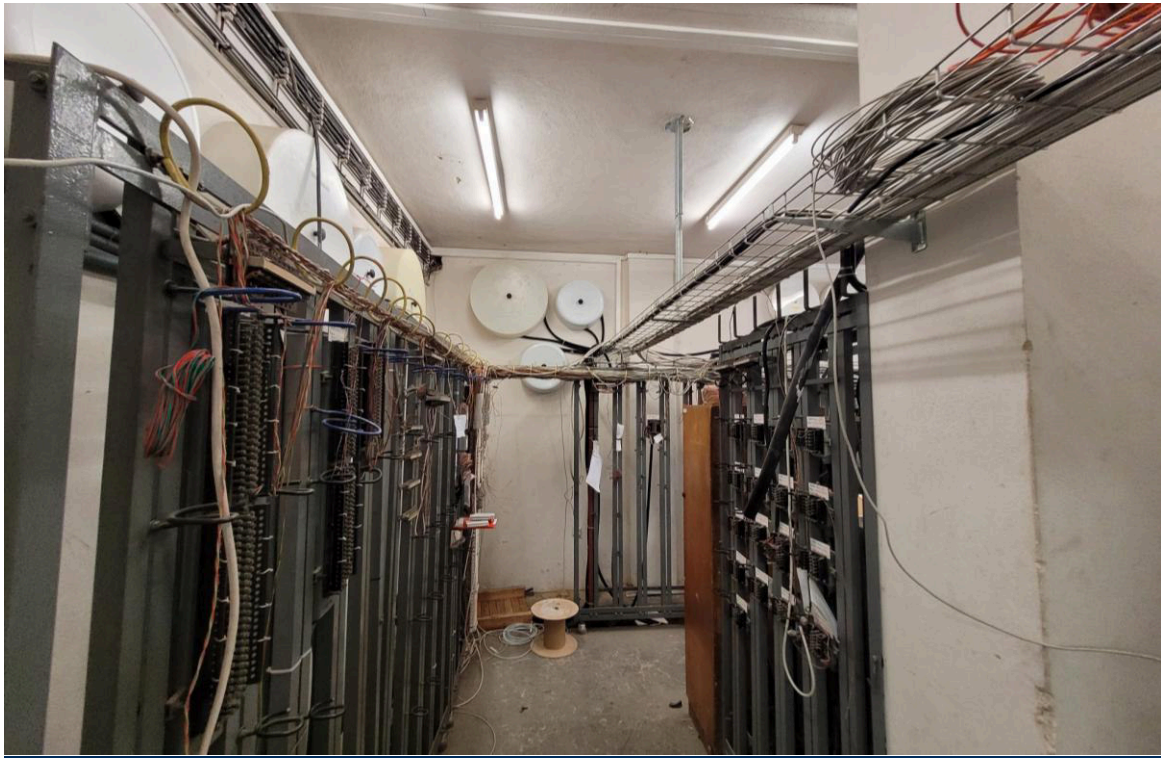
Komunikační platforma pro zajištění komunikace v rámci dispečerských pracovišť je Cisco Webex.

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Standardy zálohování a disaster recovery

Červen 2025

Obsah

1	Úvod	4
2	Služby zálohování	4
3	Řešení Disaster recovery	4

Seznam zkratek

DB	Databázová aplikace (<i>Database Engine</i>)
DR	Plán obnovy po havárii, součást kontinuity IT služeb (<i>Disaster Recovery</i>)
IBM	Americká technologická společnost (<i>International Business Machines</i>)
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
LTO	Otevřený formát magnetické pásky určené pro záznam velkých objemů dat (<i>Linear Tape Open</i>)
MSSQL	Databázový server od firmy Microsoft (<i>Microsoft SQL Server</i>)
OS	Operační systém (<i>Operating System</i>)
SQL	Standardní jazyk pro manipulaci s relačními databázemi. SQL umožňuje ukládat, manipulovat a vyhledávat data v relačních databázích. SQL je založeno na dotazech (queries) na data v databázích. Dotazy lze pak definovat a modifikovat strukturu databází, vytvářet a upravovat tabulky, indexy a další prvky, vkládat a aktualizovat data, mazat data a další operace. SQL je nezávislý na platformě, což znamená, že může být použit na různých operačních systémech a s různými databázovými systémy, avšak každá databázová platforma může mít různé změny v sintaxi (<i>Structured Query Language</i>)
SŽ	Správa železnic, státní organizace
TSM	Nástroj pro zálohování, v současné době již nese název IBM Storage Protect (<i>Tivoli Storage Manager</i>)
UAS	Logická uživatelsko-aplikační síť SŽ, zahrnuje VRF v MPLS sítích a lokální VLAN, běžně se nazývá také „Intranet SŽ“

Seznam vysvětlivek

Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů se standardy a technologiemi v ICT prostředí SŽ.
---------------------	--

1 Úvod

Cílem této části Platformy SŽ je popis podporovaných služeb, technologií, a architektonických principů v oblasti zálohování a disaster recovery v ICT prostředí Správy železnic.

2 Služby zálohování

Služba zálohování ICT prostředí Správy železnic je zajištěna technologií IBM Storage Protect (dříve známý jako IBM Spectrum Protect nebo TSM). Jedná se o komplexní řešení pro fyzické fileservery, virtualizovaná prostředí a širokou škálu aplikací. IBM Storage Protect zálohuje data především s využitím technologie VMware Snapshot. Služba zálohování je dostupná v současné době jen v UAS.

Služba zálohování umožňuje 3 základní typy zálohování:

- Snapshot disku pro dosažení rychlé obnovy celého OS v Crash Consistent stavu včetně aplikační konfigurace. Zpravidla je takto zálohován pouze systémový oddíl virtualizovaného serveru. Záloha probíhá jednou denně a retence je nastavena na 30 posledních verzí.
- Záloha datových svazků připojených k jednotlivým serverům, pro dosažení maximální možné odolnosti proti náhodnému smazání či poškození apod. Záloha probíhá jednou denně, kdy se uchovává 90 posledních verzí souborů a poslední smazaná verze souboru je uchovávána 365 dní.
- Zálohy databází Oracle nebo MSSQL pomocí agentů. Záloha probíhá dvakrát denně. Přes den jsou zálohovány transakční logy databází, v noci pak vlastní databáze. Retence je nastavena na 60 posledních verzí.

Zálohy jsou řešeny lokálním backup serverem u každé virtualizační farmy, odkud jsou poté přenášeny do DR lokality a v rámci řešení offline záloh (pro další zvýšení odolnosti proti ztrátě dat) jsou zálohy dále ukládány na LTO pásky v páskové knihovně umístěné v DR lokalitě.

3 Řešení Disaster recovery

V rámci UAS byla jako DR lokalita určen objekt *Praha U2*, kam jsou pravidelně přenášeny zálohy ze všech lokálních backup serverů.

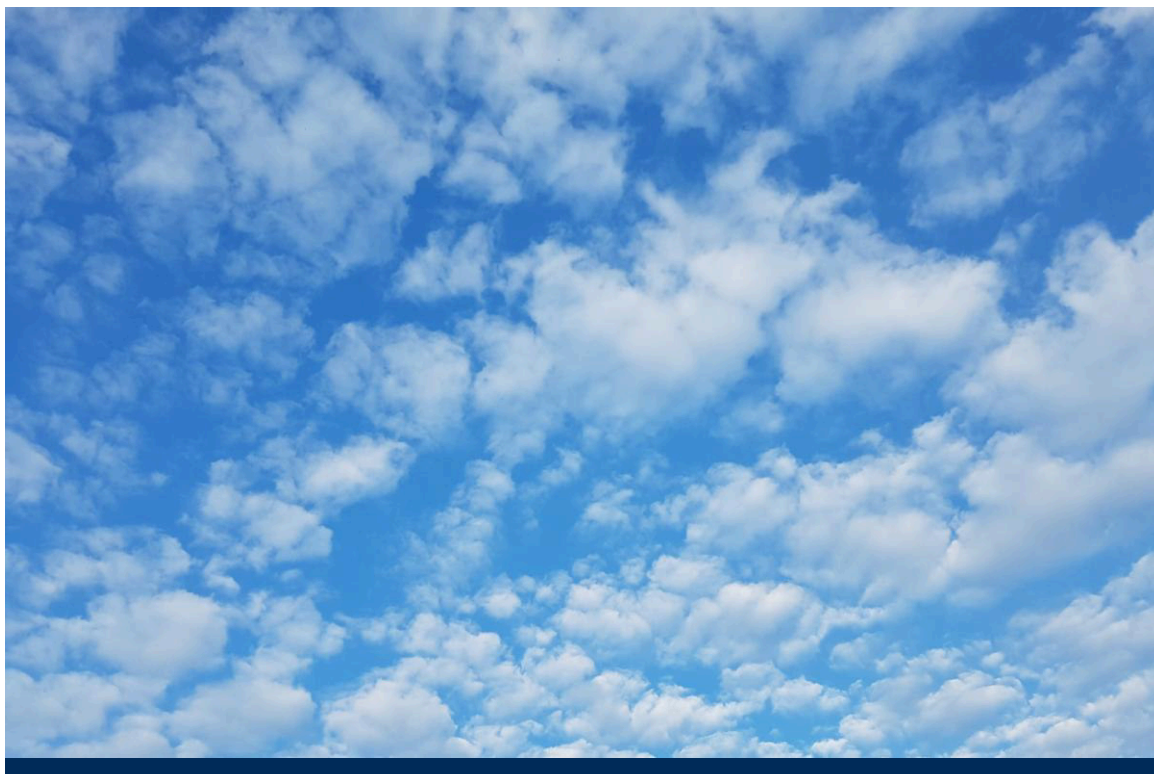
Všechny zálohy jsou pravidelně testovány a veškeré offline zálohy uložené na LTO páskách jsou pravidelně převáženy do zabezpečeného prostoru (do trezoru v jiné budově).

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz



Platforma SŽ Cloudové prostředí

Červen 2025



Obsah

1	Úvod	5
2	Cloudové prostředí.....	5
2.1	Microsoft Entra ID	5
2.2	Služby M365	5
3	Cloudové služby	5
3.1	Služba ověření proti Microsoft Entra ID	5
3.2	Integrace s M365	5

Seznam zkratek

AAD	Služba AD provozovaná v cloudovém prostředí MS Azure. Nový název služby je „MS EntraID“ (<i>Azure Active Directory</i>)
AD	Rozšiřitelná a škálovatelná adresářová služba, která umožňuje efektivně uspořádat síťové prostředky. Kromě informací o objektech v počítačové síti (uživatelské účty, počítače, tiskárny) umožňuje používat stromovou strukturu objektů, nastavovat globálně systémové politiky, instalovat programy na počítače nebo aplikovat kritické aktualizace v celé organizační struktuře. Má úzkou vazbu na DNS (<i>Active Directory</i>)
AWS	Cloudové prostředí firmy Amazon (<i>Amazon Web Services</i>)
DNS	Distribuovaný hierarchický jmenný systém používaný v síti Internet. Překládá názvy domén na číselné IP adresy a zpět, obsahuje informace o tom, které stroje poskytují příslušnou službu (<i>Domain Name System</i>)
ERP	Informační systém pro řízení podniku, který integruje různé oblasti podnikání, jako je například finanční řízení, řízení zásob, výroby, prodeje, nákupu a personálního řízení. Cílem je poskytovat podnikovým uživatelům přehled o celkových aktivitách a umožňovat efektivní a koordinované řízení všech procesů v rámci podniku (<i>Enterprise Resource Planning</i>)
IaaS	Typ cloudové služby, který poskytuje zákazníkům základní IT infrastrukturu jako službu, včetně serverů, úložiště, sítě a virtuálních počítačů. Tyto služby se často poskytují prostřednictvím Internetu a umožňují zákazníkům snadno a rychle využívat IT infrastrukturu bez nutnosti jejího nákupu, instalace a správy. Mezi nejznámější poskytovatele IaaS patří Amazon Web Services, Microsoft Azure a Google Cloud Platform (<i>Infrastructure as a Service</i>)
ICT	Informační a komunikační technologie (<i>Information and Communication Technology</i>)
IP	Jeden ze základních komunikačních protokolů používaných v počítačových sítích (<i>Internet Protocol</i>)
IT	Informační technologie (<i>Information Technology</i>)
M365	Globální označení služeb společnosti Microsoft, umožňující licencování jejich produktů a provoz aplikací, a to ať už jako on-premise řešení, či v cloudovém prostředí (<i>Microsoft 365</i>)
MS	Microsoft Corporation, americký výrobce především SW a provozovatel cloudového prostředí MS Azure
PaaS	Typ cloudové služby, která poskytuje vývojářům a IT týmům platformu pro vývoj, nasazení a správu aplikací bez nutnosti starat se o správu hardwaru a infrastruktury. Poskytovatelé PaaS nabízejí vývojové nástroje, databáze, síťové služby a další nástroje jako služby, což umožňuje vývojářům se soustředit pouze na vývoj aplikace (<i>Platform as a Service</i>)
SaaS	Model poskytování software, kdy je software hostován v cloudovém prostředí a poskytován uživatelům přes Internet. Tyto služby jsou poskytovány vývojáři software jako služby a účtovány jsou za používání (<i>pay-as-you-go</i>). To umožňuje uživatelům využívat software bez nutnosti investovat do hardware a IT infrastruktury (<i>Software as a Service</i>)
SAP	Modulární ERP systém od německé firmy SAP AG
SSO	Metoda jednotného přihlášení (<i>Single Sign-On</i>)
SW	Software je sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost
SŽ	Správa železnic, státní organizace
SŽT	Správa železničních informačních technologií

Seznam vysvětlivek

MS Azure	Cloudové prostředí firmy Microsoft.
MS EntraID	Služba AD provozovaná v cloudovém prostředí MS Azure.
Platforma SŽ	Soubor dokumentů, rozdělený na veřejnou, interní a metodickou část, určený pro seznámení dodavatelů s ICT prostředím SŽ a současně s používanými standardy a technologiemi.
Tenant	Dedikovaný virtuální prostor v cloudovém prostředí MS Azure

1 Úvod

Cílem této části Platformy SŽ je popis podporovaných cloudových služeb, technologií, a architektonických principů v rámci tenantu provozovaného Správou železnic v cloudovém prostředí.

Důvodem je zajistit ve fázích přípravy poptávky, návrhu ICT řešení a realizace dodávky kompatibilitu se stávajícím cloudovým prostředím Správy železnic a umožnit využití pro aplikace, které splňují podmínky pro umístění v cloudovém prostředí.

2 Cloudové prostředí

U aplikací a informačních systémů, kde je to z technických a bezpečnostních důvodů možné, adoptuje Správa železnic moderní technologie včetně cloudového prostředí. S ohledem na vysoké zastoupení kritické informační infrastruktury v portfoliu Správy železnic je tento proces řízen přísnou metodikou.

V současnosti využívá Správa železnic cloudová prostředí na platformách Microsoft Azure, Amazon AWS, SAP HANA Cloud a Oracle Cloud Infrastructure, která podporují různé typy cloudových služeb:

- IaaS – infrastruktura jako služba
- PaaS – platforma jako služba
- SaaS – software jako služba

V rámci Platformy SŽ pak nabízí výhradně SaaS na platformě MS Azure, jelikož ostatní cloudová prostředí jsou v případě SŽ úzce svázána s konkrétními informačními systémy.

2.1 Microsoft Entra ID

Správa železnic provozuje ve svém ICT prostředí službu Active Directory a spolu s příchodem cloudového prostředí ho rozšířila i tam, dříve pod názvem Azure Active Directory, dnes Microsoft Entra ID.

2.2 Služby M365

Správa železnic využívá velkou část portfolia SaaS služeb poskytovaných na platformě MS Azure pod názvem M365.

3 Cloudové služby

V rámci svého v současnosti používaného cloudového prostředí na platformě Microsoft Azure jsou Platformou SŽ poskytovány následující služby.

3.1 Služba ověření proti Microsoft Entra ID

Zejména u aplikací jejichž uživatelé se pohybují mimo interní síť Správy železnic je k dispozici služba Microsoft Entra ID. Ověřování proti Microsoft Entra ID přináší vyšší bezpečnost a pohodlí uživatelů i pomocí jednotného přihlašování (SSO).

3.2 Integrace s M365

Pokud u informačního systému či aplikace předpokládá Dodavatel jakoukoli integraci s aplikacemi z rodiny M365, je nutné využít tenant Správy železnic.

Správa železnic, státní organizace
Správa železniční telematiky
Dlážděná 1003/7
110 00 Praha 1

© 2025

Datum tisku
2025-07-30

spravazeleznic.cz

Zvláštní obchodní podmínky pro Zakázky v oblasti ICT

OBSAH

1. VÝKLAD POJMŮ.....	2
2. DOBA A MÍSTO PLNĚNÍ	8
3. PRÁVA A POVINNOSTI OBOU STRAN.....	9
4. POVINNOSTI DODAVATELE	9
5. POVINNOSTI OBJEDNATELE.....	10
6. LICENČNÍ UJEDNÁNÍ	10
7. ZDROJOVÝ KÓD A DOKUMENTACE.....	15
8. AKCEPTAČNÍ ŘÍZENÍ.....	16
9. ŠKOLENÍ	19
10. SERVICEDESK.....	19
11. NAHLÁŠENÍ INCIDENTU	20
12. SERVISNÍ MODELY	21
13. AKTUALIZACE PLNĚNÍ.....	22
14. ÚČAST PODDODAVATELŮ	22
15. REALIZAČNÍ TÝM	23
16. KOMUNIKACE STRAN	24
17. NÁHRADA ŠKODY A SMLUVNÍ POKUTY	24
18. ZÁRUKA ZA JAKOST A PRÁVA Z VADNÉHO PLNĚNÍ.....	26
19. UKONČENÍ SMLUVNÍHO VZTAHU	28
20. ZMĚNY SMLOUVY A ZMĚNOVÉ ŘÍZENÍ	29
21. KYBERNETICKÁ BEZPEČNOST.....	29
22. OCHRANA OSOBNÍCH ÚDAJŮ	36
23. OCHRANA DŮVĚRNÝCH INFORMACÍ	37

1. VÝKLAD POJMŮ

- 1.1. **Akceptační kritéria** představují podmínku anebo vlastnost výstupu provádění Plnění dle Smlouvy, která musí být splněna, aby bylo Plnění dle Smlouvy provedeno, přičemž Akceptační kritéria jsou uvedena v Příloze Smlouvy, která obsahuje specifikaci Plnění (dále jen „**Specifikace Plnění**“).
- 1.2. **Akceptační protokol** je protokol, který jsou zavázáni podepsat Objednatel i Dodavatel po provedení všech nezbytných činností v rámci Akceptačního řízení, potvrzující provedení výstupu provádění Plnění anebo výsledek Testů výstupů provádění Plnění. Protokol je připravený ze strany Dodavatele a následně upravený a vyplněný Objednatelem. Akceptační protokol obsahuje:
 - a. Specifikaci provedeného Plnění;
 - b. Akceptační kritéria;
 - c. informace o průběhu Testů, jsou-li prováděny;
 - d. další informace a dokumenty nezbytné pro provedení Akceptačního řízení provedeného Plnění.
- 1.3. **Akceptační řízení** je postupné provedení akceptačních procesů a podepsání Akceptačního/ch protokolu/ů pro Plnění dle Smlouvy.
- 1.4. **Aktualizace** je dílčí změna verze Softwaru, zpravidla odstraňující zranitelnosti či drobné nedostatky Softwaru většinou neprojevující se navenek uživatelům, v IT obvykle označovaná jako „patch“ nebo „security update“ (v rámci IT se také často označuje jako změna třetí číslice v čísle verze Softwaru, tedy např. 4.1.1. na 4.1.2.). Aktualizace představuje takovou změnu Softwaru, která není Modernizací ani Zásadní modernizací.
- 1.5. **Autorské dílo** znamená dílo ve smyslu § 2 Autorského zákona; zejména Software, Databáze a jakékoliv výstupy předávané Objednateli na základě Smlouvy, které splňují podmínky stanovené v § 2 Autorského zákona.
- 1.6. **Autorský zákon** znamená zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.
- 1.7. **Cena** je celková cena za Plnění bez DPH dle Smlouvy. V případě:
 - a. Smlouvy na dobu neurčitou, jejímž předmětem jsou výhradně pravidelně se opakující či trvající služby či činnosti, se cenou Plnění bez DPH rozumí cena bez DPH za 12 měsíců poskytování takových služeb či činností.
 - b. Smlouvy na dobu neurčitou, součástí jejíhož předmětu jsou mj. pravidelně se opakující či trvající služby či činnosti, které je Dodavatel povinen poskytovat na dobu neurčitou, se cenou Plnění bez DPH rozumí souhrn cen bez DPH ostatních částí Předmětu Smlouvy a ceny bez DPH za 12 měsíců poskytování takových služeb či činností.
 - c. Smlouvy, která je rámcovou dohodou, se cenou za Plnění bez DPH této Smlouvy rozumí limit stanovený v této Smlouvě jako maximální souhrnná hodnota bez DPH všech dílčích smluv uzavřených na základě této Smlouvy.
 - d. Smlouvy, která je zčásti rámcovou dohodou, se cenou za Plnění bez DPH této Smlouvy rozumí souhrn cen bez DPH ostatních částí Předmětu Smlouvy a limitu stanoveného v této Smlouvě jako maximální souhrnná hodnota bez DPH všech dílčích smluv uzavřených na základě této Smlouvy.
- 1.8. **Čas nahlášení Incidentu** představuje časový údaj, vyjadřující datum a čas, kdy byl Incident nahlášen Dodavateli způsobem stanoveným ve Smlouvě a ZOP, tj. vytvořením ticketu v Servicedesku, vytěžením e-mailu z e-mailového serveru Objednatele a jeho vložení do Servicedesku jako ticketu anebo ukončením telefonátu.
- 1.9. **Data** jsou záznamy jednání, skutečností nebo informací a soubory takových jednání, skutečností nebo informací, včetně provozních údajů a metadat, zejména v podobě textu, čísel, grafů, obrazů, zvuku a videa.

- 1.10. **Databáze** znamená databázi splňující požadavky na Autorská díla, databázi ve smyslu § 88 Autorského zákona a jakoukoliv jinou Autorským zákonem neupravenou databázi.
- 1.11. **Doba vyřešení** je pro každou kategorii Incidentů uvedena ve Smlouvě a ZOP a znamená rozdíl mezi časem nahlášení Incidentu a dodáním řešení. Do Doby vyřešení Incidentu se nezapočítává doba, po kterou nemůže Dodavatel řešit Incident z důvodu:
- neobdržení podkladů a informací vyžádaných Dodavatelem, které jsou nezbytně nutné pro lokalizaci nebo replikaci Incidentu, od Objednatele;
 - řešení Incidentu u třetí osoby (vyjma Poddodavatele), jejíž součinnost je dle Smlouvy povinen zajistit Objednatel (např. poskytovatele služeb podpory IT prostředí Objednatele anebo systémů, na které je Software napojen);
 - neposkytnutí jiné nezbytně nutné součinnosti Objednatele vyžádané Dodavatelem v souladu s těmito ZOP či Smlouvou a souvisejícími přílohami.
- 1.12. **Doba zpracování či Reakční doba** je doba, ve které Dodavatel musí reagovat prostředkem odpovídajícím způsobu nahlášení Incidentu či Požadavku o přijetí takového nahlášení a o zahájení činností směřujících k vyřešení Incidentu či Požadavku.
- 1.13. **Dodavatel** označuje rovněž Poskytovatele, Zhotovitele či Prodávajícího v závislosti na typu uzavřené Smlouvy.
- 1.14. **Dodavatel strategicky významné služby** je Dodavatel, který se podílí na poskytování Strategicky významné služby.
- 1.15. **Dohledové centrum kybernetické bezpečnosti SŽ (SOC SŽ)** je specializovaný útvar SŽ, který ve režimu 24/7 zajišťuje činnosti související se zajištěním kybernetické bezpečnosti. Kontaktní údaje: soc@spravazeleznic.cz nebo +420 972 235 333.
- 1.16. **Dokumentace** znamená část specifikace Předmětu Smlouvy, která představuje jednotlivé dokumenty popisující Předmět Smlouvy a zacházení s ním, jako jsou uživatelská dokumentace, administrátorská dokumentace, bezpečnostní dokumentace, a také jakoukoliv jinou dokumentaci vytvářenou anebo poskytovanou Dodavatelem v rámci provádění Plnění. Dokumentace musí být vždy vyhotovena a předána Objednateli v elektronické podobě (pokud je vyhotovována v listinné podobě, pak Dodavatel předá Objednateli elektronickou kopii takové Dokumentace).
- 1.17. **Dostupnost** znamená stav Software či Hardware, v průběhu kterého je, anebo by v případě poskytování řádné a včasné součinnosti ze strany Objednatele za podmínek dle Smlouvy byl, možný řádný provoz Softwaru či Hardware v celém jeho rozsahu, přičemž Software se považuje za Dostupný, je-li přístupný a použitelný pro všechny uživatele Softwaru ve sjednaném rozsahu minimálně dle příslušného Servisního modelu dle ZOP.
- 1.18. **Důvěrné informace** znamenají informace, které jsou zpracovávány, ukládány nebo poskytovány v IT prostředí Objednatele, včetně Dat Objednatele, veškeré údaje a informace související s těmito informacemi, s technickým vybavením, komunikačními prostředky a programovým vybavením IT prostředí Objednatele a s objekty, ve kterých jsou tyto systémy umístěny, zaměstnanci nebo dodavateli podílejícími se na provozu, rozvoji, správě nebo bezpečnosti IT prostředí Objednatele. Mezi Důvěrné informace nepatří informace, které jsou veřejně přístupné.
- 1.19. **FOSS licence** znamená Free Open Source Software licence.
- 1.20. **GDPR** znamená nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
- 1.21. **GUI** znamená grafické uživatelské rozhraní.
- 1.22. **Hands-on** se rozumí školení vymezené v rámci Smlouvy či jejích příloh (je-li takové), zpravidla jde o školení, jehož součástí je komentované provedení části Plnění za účasti zástupců Objednatele
- 1.23. **Hardware** znamená veškeré hmotné součásti počítačových systémů a veškeré související vybavení hmotné povahy spolu se vším příslušenstvím, a včetně veškeré související dokumentace.
- 1.24. **Servicedesk** je Software provozovaný Dodavatelem nebo Objednatelem sloužící ke komunikaci Stran v průběhu provádění Plnění dle Smlouvy a zároveň bude sloužit jako kontaktní místo

Dodavatele pro nahlásování Incidentů a Požadavků, vznášení dotazů k Plnění, získávání odpovědí ve vztahu k Plnění a další zaznamenávání průběhu provádění Plnění dle Smlouvy.

- 1.25. **Informační či komunikační systém** znamená informační či komunikační systém kritické informační infrastruktury Objednatele nebo jiný informační či komunikační systém, který souvisí s poskytováním regulované služby Objednatelem.
- 1.26. **Incident** představuje neplánované přerušení fungování Předmětu Smlouvy, jakékoliv jeho části anebo Plnění dle Smlouvy, omezení kvality fungování Předmětu Smlouvy a souvisejícího Plnění, anebo jakoukoliv prokazatelnou nefunkčnost Předmětu Smlouvy a souvisejícího Plnění. Incident se projevuje zejména selháním oproti funkčnosti a funkcionalitě specifikované v Příloze Smlouvy *Specifikace Plnění*, anebo obvyklé pro Předmět Smlouvy. Vada je vždy Incidentem a jde tak o podmnožinu pojmu Incident. Za dobu trvání Incidentu se považuje doba od Času nahlášení Incidentu Ohlašovatelem do vyřešení Incidentu, které bude Ohlašovatelem nebo jeho nadřízeným uživatelem potvrzeno vhodným způsobem v Servicedesku, byl-li Incident vyřešen.

Kategorizace Incidentů dle důležitosti, zohledňující naléhavost a dopad Incidentu:

- A) Vysoká – ohrožení kritických procesů a činností na straně Objednatele
- B) Střední – Zásadní vliv na důležité procesy a činnosti Objednatele
- C) Nízká – standardní řešení v efektivním režimu.

Mezi Incidenty dále patří také všechny Kybernetické bezpečnostní incidenty, které jsou podmnožinou pojmu Incident.

- 1.27. **Instalace** znamená provedení veškerých činností nezbytných ke zprovoznění Hardwaru nebo Softwaru vč. jeho Aktualizací, Modernizací či Zásadních modernizací poskytnutých v rámci Plnění dle Smlouvy v IT prostředí Objednatele, a to na platformě určené Objednatelem.
- 1.28. **ISDS** znamená informační systém datových schránek ve smyslu zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů.
- 1.29. **Interní předpisy** znamenají interní předpisy Objednatele, jejichž seznam včetně znění daných interních předpisů, jsou-li relevantní z hlediska Plnění, je uveden v Příloze Smlouvy *Seznam interních předpisů*.
- 1.30. **Insolvenční zákon** znamená zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.
- 1.31. **IT prostředí Objednatele** znamená veškerý Hardware a Software, který Objednatel oprávněně užívá. Jedná se zejména o servery, diskové pole a stanice, aplikace třetích osob, pasivní a aktivní datová infrastruktura (kabeláže, switche, VPN linky apod.). Podrobná specifikace IT prostředí Objednatele je uvedena v Příloze Smlouvy *Platforma Správy železnic* a v Příloze Smlouvy *Specifikace Plnění*.
- 1.32. **Kvalifikovaná osoba** je člen Realizačního týmu, kterým Dodavatel prokazoval splnění kvalifikačních předpokladů v rámci Veřejné zakázky.
- 1.33. **Kybernetický bezpečnostní incident** je narušení bezpečnosti informací v Kybernetickém prostoru SŽ.
- 1.34. **Kybernetická bezpečností událost** je událost podle ZoKB, která může vyústit v Kybernetický bezpečnostní incident.
- 1.35. **Kybernetický prostor SŽ** je soubor sítí elektronických komunikací a dalších technologií, ve kterém dochází ke zpracování informací a dat v elektronické podobě.
- 1.36. **MD** znamená manday/člověkoden. Nestanoví-li Smlouva jinak, odpovídá jeden MD 8 MH.
- 1.37. **MH** znamená manhour/člověkohodinu. Nestanoví-li Smlouva jinak, odpovídá jedna MH 60 minutám práce.
- 1.38. **Modernizace** je změna verze Softwaru, která zpravidla představuje výraznější zásah do dílčí funkcionality Softwaru, přepracováním jeho vybrané funkcionality či doplnění funkcionality nové, zvýšení kompatibility Softwaru s jinými prvky informačních a komunikačních technologií, či jinou optimalizací funkce Softwaru nad rámec Aktualizace, zpravidla v IT označovaná jako „update“ (v

rámci IT se také často označuje jako změna druhé číslice v čísle verze Softwaru, tedy např. 4.1. na 4.2.).

- 1.39. **NÚKIB** znamená Národní úřad pro kybernetickou a informační bezpečnost.
- 1.40. **Občanský zákoník** znamená zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
- 1.41. **Obchodní podmínky** znamenají obchodní podmínky Objednatele v posledním znění ke dni podání nabídky do Veřejné zakázky či aktualizace těchto Obchodních podmínek provedené v souladu se Smlouvou po dobu jejího trvání.
- 1.42. **Objednatel** je Správa železnic, státní organizace, IČO 70994234, se sídlem Praha 1 – Nové Město, Dlážďená 1003/7, PSČ 110 00, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. Zn. A 48384.
- 1.43. **Ohlašovatel** znamená osobu určenou Objednatelem, zpravidla uživatele Předmětu Smlouvy.
- 1.44. **Opční právo** představuje vyhrazenou změnu závazku v souladu s ustanovením § 100 odst. 3 ZZVZ ze Smlouvy spočívající v pořízení dalšího obdobného Plnění od vybraného uchazeče v rámci zadávacího řízení Veřejné zakázky, tj. od Dodavatele dle Smlouvy.
- 1.45. **Osobní údaje** znamenají osobní údaje ve smyslu GDPR, včetně zvláštních kategorií osobních údajů ve smyslu článku 9 a rozsudků ve smyslu článku 10 GDPR.
- 1.46. **Pracovní den (PD)** znamená kterýkoliv den, kromě soboty a neděle a dnů, na něž připadá státní svátek nebo ostatní svátek podle platných a účinných právních předpisů České republiky.
- 1.47. **Paušální služby** jsou služby definované ve Smlouvě, jsou-li takové, zpravidla trvajících či opakujících se charakteru.
- 1.48. **Platforma Správy železnic/Platforma SŽ** je dokument, který definuje prostředí, které standardizuje a podporuje návrh, implementaci a provozování veškerého ICT řešení pro Správu železnic. Popisuje infrastrukturní a platformní služby, podporované technologie a upravuje pravidla jejich použití i rozšiřování. Primárním cílem Platformy SŽ je poskytnout potenciálním dodavatelům základní přehled o ICT prostředí SŽ a současně umožnit organizaci SŽ zajištění efektivního vytváření a provozování ICT řešení při dodržení vysoké kvality a bezpečnosti služeb.
- 1.49. **Plnění (též Předmět Smlouvy)** představuje plnění, které je Dodavatel povinen dle Smlouvy poskytovat. Plněním se rozumí jak činnost Dodavatele, tak její výsledek, je-li takový; tímto výsledkem je zejména HW, SW či jiný výstup plnění dle Smlouvy. Plnění je blíže specifikováno ve Smlouvě nebo v její příloze.
- 1.50. **Poddodavatel** znamená kteroukoli třetí osobu realizující poddodávky pro Dodavatele v souvislosti s Předmětem Smlouvy. Poddodavatelé mohou být výslovně uvedeni v Příloze Smlouvy *Poddodavatelé*.
- 1.51. **Požadavek** znamená žádost ze strany Objednatele o službu nebo její podporu předanou v souladu se Smlouvou Dodavateli, která nemá příčinu v chybovém stavu, tj. není Incidentem.

Kategorizace Požadavků dle důležitosti:
A) Vysoká – řešení je pro Objednatele kritické
B) Střední – řešení neovlivňuje využívání hlavních funkcí služby
C) Nízká – řešení výrazně neovlivňuje procesy Objednatele
- 1.52. **Produkční prostředí** znamená IT prostředí Objednatele v ostrém provozu běžně přípustnou uživatelům Software, vyjma Testovacího prostředí.
- 1.53. **Převzetí poskytování plnění** je předání znalostí Dodavateli a praktické seznámení se Dodavatele s podmínkami poskytování služeb. Pokud dochází k převzetí poskytování podpory, jsou podmínky pro Převzetí poskytování plnění uvedeny ve Smlouvě a v Příloze Smlouvy *Specifikace Plnění*.
- 1.54. **Příloha Smlouvy** je dokument, který tvoří nedílnou součást Smlouvy a obsahuje bližší specifikaci smluvních podmínek.

- 1.55. **Reakce** znamená kvalifikovanou a konkrétní odpověď na nahlášení Incidentu nebo na jiný požadavek, ve formě a způsobem dále definovanými v Příloze Smlouvy *Specifikace Plnění*.
- 1.56. **Reakční doba** je pro každou kategorii Incidentů uvedena v Příloze *Specifikace Plnění* a představuje dobu od Času nahlášení Incidentu do doručení Reakce Objednateli nebo Ohlašovatelí.
- 1.57. **Realizační tým** znamená osoby uvedené v příloze Smlouvy *Realizační tým*, kterými Dodavatel prokazoval splnění kvalifikačních předpokladů v rámci Veřejné zakázky a další osoby (zaměstnanci Dodavatele či Poddodavatele), prostřednictvím nichž Dodavatel provádí Plnění dle Smlouvy.
- 1.58. **Recovery Point Objective (RPO)** je parametr, který vyjadřuje maximální ztrátu dat uživatelů při havárii systému a následné obnově.
- 1.59. **Recovery Time Objective (RTO)** je parametr, který vyjadřuje dobu nutnou k obnově chodu služby do akceptované úrovně provozu.
- 1.60. **Servisní model** je standardizovaný model provozu a podpory aplikace, systému nebo instance služby.
- 1.61. **SLA** znamená úroveň kvality Plnění představující dohodu o úrovni poskytovaných ICT služeb dle Smlouvy.
- 1.62. **Služby** jsou služby definované ve Smlouvě, jsou-li takové.
- 1.63. **Smluvní strany či Strany** jsou strany Smlouvy, tj. Objednatel a Dodavatel či jinak označené strany Smlouvy, jejíž součástí jsou tyto ZOP.
- 1.64. **Software** znamená veškeré programové vybavení a další Autorská díla, stejně jako další věci či jiné majetkové hodnoty, které s programovým vybavením souvisí a jsou určeny ke společnému užívání s tímto programovým vybavením, tj. zejména Databáze, GUI, zvukové nahrávky, videa, obrázky, fotografie apod., včetně veškeré související dokumentace a updatů a upgradů tohoto programového vybavení, avšak s výjimkou Hardwaru a Databází.
- 1.65. **Standardní Software** znamená Software, který je distribuován pod standardními licenčními podmínkami více třetím osobám. Mezi Standardní software patří:
- Software renomovaných výrobců, jenž je na trhu běžně dostupný, tj. nabízený na území České republiky alespoň dvěma (2) na sobě nezávislými a vzájemně se neovládajícími subjekty, a který je v době uzavření Smlouvy prokazatelně užíván v produkčním prostředí nejméně u pěti (5) na sobě nezávislých a vzájemně nepropojených subjektů.
 - Software, u kterého je s ohledem na jeho (i) marginální význam, (ii) nekomplikovanou propojitelnost či (iii) oddělitelnost a nahraditelnost v IT prostředí bez nutnosti vynakládání větších prostředků (více než 50.000 Kč/rok) zajištěno, že další rozvoj Softwaru jinou osobou než tvůrcem/distributorem takového Softwaru je možné provádět bez toho, aby tím byla dotčena práva autorů takového Softwaru, neboť nebude nutné zasahovat do Zdrojových kódů takového Softwaru anebo proto, že případné nahrazení takového Softwaru nebude představovat výraznější komplikaci a náklad na straně Objednatele.
 - Software, jehož API („Application Programming Interface“) pokrývá všechny moduly a funkcionality Softwaru, je dobře dokumentované, umožňuje zapouzdření Softwaru a jeho adaptaci v rámci měnících se podmínek IT prostředí Objednatele a Softwaru bez nutnosti zásahu do Zdrojových kódů Softwaru, a Dodavatel poskytne Objednateli právo užít toto rozhraní pro programování aplikací ve stejném rozsahu jako Software.
 - Software, o kterém to stanoví Smlouva.
- 1.66. **Strategicky významná služba (SVS)** je regulovaná služba, jejíž narušení by mohlo mít závažný dopad na bezpečnost České republiky nebo vnitřní pořádek a která je určena obecně závazným právním aktem – nařízením vlády ČR.
- 1.67. **Smlouva** uzavřená na základě zadávacího řízení Veřejné zakázky vztahující se k ICT, která se řídí těmito ZOP. Smlouvou se rovněž rozumí rámcová dohoda a dílčí smlouva uzavřená na základě takové rámcové dohody.

- 1.68. **Systém** znamená ucelený soubor technických, programových a datových prvků, včetně jejich konfigurace, rozhraní a vzájemných vazeb, který je provozován samostatně nebo jako součást IT infrastruktury a slouží k zajištění určité funkce, služby nebo procesu, zejména ke zpracování, ukládání, přenosu nebo poskytování informací.
- 1.69. **Testy** se rozumí provádění testovacího užívání Předmětu Smlouvy v Testovacím prostředí prostřednictvím simulace ostrého provozu v Produkčním prostředí a reálných situací a Testovacích scénářů.
- 1.70. **Testovací prostředí** znamená virtuální či fyzickou kopii Předmětu Smlouvy anebo IT prostředí Objednatele určenou Objednatelem k provádění Testů.
- 1.71. **Vada kategorie A** znamená kritickou vadu, která má zásadní dopad na základní funkce Plnění, má jakýkoli vliv na kvalitu a bezpečnost dat a výsledky jejich zpracování anebo způsobuje výpadky Plnění.
- 1.72. **Vada kategorie B** znamená vadu umožňující provoz základních funkcí Plnění, zároveň nemá vliv na kvalitu ani na bezpečnost dat a výsledky zpracování anebo hrozí, že by mohla způsobit výpadek Plnění.
- 1.73. **Vada kategorie C** znamená vadu, která není Vadou kategorie A anebo B (např. špatná grafická úprava aplikace, špatný pravopis u nápovědy apod.).
- 1.74. **Veřejná zakázka** je zakázka realizovaná na základě smlouvy mezi Objednatelem a Dodavatelem, jež byla uzavřena na základě zadávacího řízení dle ZZVZ nebo výběrového řízení dle vnitřních předpisů Objednatele.
- 1.75. **VoKB** znamená vyhlášku č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.
- 1.76. **Výkaz** znamená dokument obsahující souhrnnou evidenci poskytnutého Plnění za období vymezené ve Smlouvě nebo v Příloze Smlouvy *Specifikace Plnění*. Výkaz je vystavován zpětně za vymezené období.
- 1.77. **Výpadek** znamená neplánované přerušení provozu Předmětu smlouvy či jakékoliv jeho podstatné části, při kterém je tento celek či příslušná část nedostupná pro uživatele (není dostupný). Za Výpadek se pro účely této Smlouvy nepovažuje Výpadek způsobený z důvodů způsobených třetími osobami, jejichž součinnost anebo bezvadné poskytování služeb je povinen zajistit Objednatel (poskytovatel služeb podpory IT prostředí Objednatele a informačních systémů, na které je Software napojen).
- 1.78. **Újma** znamená vždy újmu na jmění (škodu) ve smyslu § 2894 odst. 1 Občanského zákoníku a dále vždy i nemajetkovou újmu ve smyslu § 2894 odst. 2 Občanského zákoníku. Toto ustanovení je výslovným ujednáním o povinnosti stran odčinit nemajetkovou újmu v případech porušení povinností dle těchto ZOP a Smlouvy.
- 1.79. **Významný dodavatel** je ten, kdo SŽ poskytuje plnění, které je významné z hlediska zajištění kybernetické bezpečnosti regulované služby. Významní dodavatelé jsou evidováni v souladu s VoKB.
- 1.80. **Významná změna** znamená změnu Softwaru, Systému, Služby, IT prostředí Objednatele, nebo procesu, která může podstatným způsobem ovlivnit bezpečnost, dostupnost, integritu nebo funkčnost Předmětu plnění, plnění závazků vyplývajících ze Smlouvy nebo může mít významný dopad na plynulost či kontinuitu provozu Objednatele. Za Významnou změnu se považuje zejména změna, která zahrnuje podstatnou úpravu architektury, funkčnosti nebo způsobu provozu systému, zavádí novou technologii nebo zásadně mění technické řešení, může změnit úroveň rizik nebo vyžaduje provedení bezpečnostní analýzy či bezpečnostních testů, a dále změna, která může mít dopad na plnění povinností podle obecně závazných právních předpisů, zejména předpisů v oblasti kybernetické bezpečnosti. Významné změny podléhají předchozímu písemnému schválení Objednatele a musí být realizovány v souladu s procesy řízení změn Objednatele, včetně požadovaného bezpečnostního posouzení, testování nebo auditu, pokud tak stanoví Smlouva, Interní předpisy Objednatele nebo příslušná právní úprava.
- 1.81. **Zadávací dokumentace** je souborem dokumentů obsahujících zadávací podmínky, sdělované nebo zpřístupňované účastníkům zadávacího řízení na Veřejnou zakázku.

- 1.82. **Zásadní modernizace** je podstatná změna/rozšíření funkčnosti nebo změna koncepce Softwaru, přinášející podstatné změny pro chování Softwaru vůči uživatelům, zpravidla v IT označovaná jako „upgrade“ (v rámci IT se také často označuje jako změna v čísle verze Software, tedy např. 4 na 5).
- 1.83. **Zdrojový kód** znamená zápis kódu počítačového programu (Softwaru) v programovacím jazyce, který je uložen v jednom nebo více editovatelných souborech, čitelný, opatřený komentáři vysvětlujícími jeho jednotlivé části alespoň ve standardu obvyklém pro open source projekty a procesy, ve spustitelném formátu odpovídajícím programovacímu jazyku a Produkčnímu prostředí, včetně ověřeného a podrobného postupu nezbytného pro sestavení plně funkčního strojového kódu, a v podobě, aby jej bylo možné zkompileovat do strojového kódu bez nutnosti provedení jiných úprav než kompilace v souladu s postupem k sestavení.
- 1.84. **ZoKB** znamená zákon č. 264/2025 Sb., o kybernetické bezpečnosti.
- 1.85. **ZOP** znamená tento dokument, tedy zvláštní obchodní podmínky, které definují další parametry a upřesňují konkrétní podmínky a specifické požadavky Objednatele.
- 1.86. **ZZVZ** znamená zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.
- 1.87. Není-li výslovně uvedeno jinak nebo nevyplývá-li něco jiného z povahy věci, mají pojmy, které nejsou definovány v těchto ZOP, význam uvedený v Obchodních podmínkách či Smlouvě a jejich přílohách.
- 1.88. Ustanovení ZOP mají přednost před ustanoveními Obchodních podmínek, pokud jsou ustanovení těchto dokumentů v rozporu, uplatní se ustanovení uvedené v ZOP. Ustanovení Smlouvy mají přednost před ustanoveními Obchodních podmínek i ZOP.
- 1.89. Pokud je uveden v ZOP čas, jedná se o čas SEČ.
- 1.90. Dodavatel je povinen se seznámit s Platformou Správy železnic, a to bez ohledu na to, zda plnění probíhá v IT prostředí Objednatele, a to minimálně v rozsahu, v kterém je pro Plnění relevantní.

2. DOBA A MÍSTO PLNĚNÍ

- 2.1. Provádění Plnění bude zahájeno ode dne nabytí účinnosti Smlouvy, není-li ve Smlouvě stanoveno jinak.
- 2.2. Plnění nebo dílčí části Plnění bude Dodavatel provádět v termínech sjednaných ve Smlouvě či definovaných v Příloze Smlouvy *Specifikace Plnění* nebo *Harmonogram*.
- 2.3. Místem provádění Plnění jsou místa umístění IT prostředí Objednatele (tj. Testovací prostředí a Produkční prostředí), není-li ve Smlouvě anebo Příloze Smlouvy *Specifikace Plnění* výslovně stanoveno jinak. Popis IT prostředí Objednatele obsahuje Příloha Smlouvy *Platforma Správy železnic*.
- 2.4. Služby budou poskytovány formou vzdáleného přístupu k IT prostředí Objednatele, není-li ve Smlouvě stanoveno jinak. Objednatel se zavazuje umožnit Dodavateli vzdálený přístup k IT prostředí Objednatele. Objednatel je oprávněn monitorovat a logovat přístupy Dodavatele do IT prostředí Objednatele, jakož i veškerou další aktivitu Dodavatele významnou z hlediska bezpečnosti Informačního či komunikačního systému za účelem posouzení souladu Plnění Smlouvy s pravidly uvedenými v těchto ZOP, zejm. pak v čl. 21. ZOP, a Dodavatel se zavazuje Objednateli za tímto účelem poskytnout veškerou nutnou součinnost. Vzdálený přístup k IT prostředí Objednatele může být Objednatelem okamžitě odepřen v případě Kybernetické bezpečnostní události ve smyslu § 2 ZoKB či porušení povinností stanovených v Interních předpisech.
- 2.5. Dodavatel bere na vědomí, že přístup k IT prostředí Objednatele:
 - a. je udělován fyzickým osobám Dodavatele, jakož i pro konkrétní zařízení, na základě výslovného požadavku Dodavatele a Objednatel je oprávněn dle svého uvážení přístup neudělit či kdykoli odebrat;
 - b. je poskytován na základě principů „need to know“ a „deny by default“; a
 - c. je poskytován za podmínky dodržování veškerých bezpečnostních opatření a požadavků Objednatele.

3. PRÁVA A POVINNOSTI OBOU STRAN

- 3.1. Strany se zavazují postupovat v souladu s veškerými obecně závaznými právními předpisy a prohlašují, že Smlouva je v souladu s těmito právními předpisy. Pokud se v průběhu trvání Smlouvy některé její ustanovení dostane do rozporu s kogentním ustanovením obecně závazného právního předpisu, platí příslušné ustanovení právního předpisu s tím, že zbývající ustanovení Smlouvy zůstávají v platnosti.
- 3.2. Strany jsou v průběhu Plnění povinny postupovat v souladu s Interními předpisy Objednatele, pokud jsou jednoznačně specifikovány v Příloze Smlouvy *Seznam Interních předpisů*. Objednatel je oprávněn přiměřeným způsobem jednostranně měnit nebo doplňovat Interní předpisy uvedené v Příloze Smlouvy, pokud je to nezbytné pro zajištění souladu s právními předpisy, bezpečnostními požadavky nebo provozními standardy. Objednatel je povinen o každé takové změně informovat Dodavatele tak, aby měl Dodavatel reálnou možnost změny implementovat, není-li z povahy věci nutné jednat bezodkladně (např. při hrozbě Kybernetického bezpečnostního incidentu). Dodavatel je povinen změny implementovat v rozsahu, v jakém je to po něm lze spravedlivě požadovat, s ohledem na charakter plnění, technické možnosti a přiměřené náklady. Pokud Dodavatel prokazatelně doloží, že změna má podstatný dopad na cenu nebo termíny plnění, Strany sjednají odpovídající úpravu Smlouvy.

4. POVINNOSTI DODAVATELE

- 4.1. Dodavatel se zavazuje provádět pro Objednatele Plnění osobně, tj. prostřednictvím svých zaměstnanců, členů Realizačního týmu a prostřednictvím svých Poddodavatelů za podmínek stanovených ve Smlouvě a těchto ZOP. V případě, že je požadavek na složení Realizačního týmu uveden ve Smlouvě, je Dodavatel povinen provádět Plnění výhradně prostřednictvím členů Realizačního týmu, kterými prokázal splnění kvalifikace v průběhu zadávacího řízení na Veřejnou zakázku.
- 4.2. Dodavatel se během poskytování Plnění pro Objednatele zavazuje informovat Objednatele o Významné změně ovlivnění nebo ovládání Dodavatele podle ust. § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů (dále jen „ZOK“), nebo změně vlastnictví zásadních aktiv, využívaných Dodavatelem k Plnění Smlouvy, jakož i o změně oprávnění nakládat s těmito aktivy.
- 4.3. Dodavatel se zavazuje poskytovat v rámci Plnění veškerou součinnost nezbytnou k provádění Plnění, zejména:
 - 4.3.1. poskytovat Plnění dle Smlouvy ve vysoké kvalitě s odbornou péčí odpovídající podmínkám sjednaným ve Smlouvě;
 - 4.3.2. poskytovat Plnění dle Smlouvy alespoň v závazných parametrech kvality dle Smlouvy a SLA, a to zejména dodržování stanoveného Servisního modelu dle odst. 12.2. ZOP;
 - 4.3.3. upozorňovat Objednatele včas na všechny hrozící vady svého Plnění či potenciální Výpadky či jiné výpadky Plnění, jakož i poskytovat Objednateli veškeré informace, které jsou pro Plnění potřebné;
 - 4.3.4. zajistit v souladu s podmínkami Smlouvy poskytnutí Dokumentace, a to rovněž vždy při každé Aktualizaci nebo jiné změně Předmětu smlouvy, nestanoví-li Objednatel jinak;
 - 4.3.5. počínat si při provedení Plnění tak, aby nedošlo k infekci Softwaru, Standardního Softwaru nebo IT prostředí Objednatele virem či jiným škodlivým kódem (malware apod.) způsobujícím narušení zabezpečení Softwaru a Standardního Softwaru za účelem jeho poškození či jiného narušení běhu;
 - 4.3.6. bez zbytečného odkladu na výzvu Objednatele předat Data, provozní údaje a informace ve formátu předem odsouhlaseném Objednatelem (zpravidla ve formátu daného prostředí, který umožňuje jejich nasazení „as is“ do prostředí), které má k dispozici v souvislosti s Plněním Smlouvy, a poskytnout Objednateli za tímto účelem veškerou nezbytnou součinnost; tato Data musí být po dobu poskytování Plnění dle Smlouvy uložena u Dodavatele a mohou být Dodavatelem užívána v souladu se Smlouvou a příslušnými právními předpisy, avšak pouze v nezbytném rozsahu. Dodavatel se

zavazuje dodržovat přiměřená technická a organizační opatření k ochraně těchto Dat. Veškerá Data jsou vlastnictvím Objednatele, není-li ve Smlouvě výslovně stanoveno jinak. Toto ustanovení se uplatní obdobně i na jiná data poskytnutá Objednatelem Dodavateli;

4.3.7. plnit Interní předpisy Objednatele a jeho pokyny v oblasti likvidace Dat (ať už Dat na papírových médiích, Dat zpracovávaných elektronicky nebo prostřednictvím jakýchkoli dalších nosičů Dat) a případně dále na vyzvu Objednatele bez zbytečného odkladu zlikvidovat Data v souladu s těmito pravidly a pokyny. Dodavatel musí především postupovat tak, aby nebylo možné odstraněná data zneužít. Za odpovídající způsob likvidace dat je považováno odstranění, přepsání či fyzická likvidace nosiče informace v souladu se standardem US DoD 5220.22-M;

4.3.8. poskytnout při ukončení smluvního vztahu přiměřenou součinnost při Převzetí poskytování Plnění novým Dodavatelem nebo Objednatelem, a to s odbornou péčí, zodpovědně a do doby úplného Převzetí poskytování Plnění. Součinnost zahrnuje zejména, pokud je součástí Plnění:

- a. předání Dokumentace, konfiguračních informací, přístupových údajů a kryptografických klíčů;
- b. migraci dat v bezpečném, odsouhlaseném formátu;
- c. zajištění provozu služeb po přechodné období podle harmonogramu;
- d. technická a bezpečnostní opatření k zajištění kontinuity a ochrany informací;
- e. likvidaci dat a nosičů dle požadavků Objednatele po ukončení smlouvy

4.4. Dodavatel se během poskytování Plnění pro Objednatele zavazuje informovat Objednatele o žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu, vyjma situace, kdy by takové informování bylo v rozporu s právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána. V případě zpřístupnění nebo předání dat na základě žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu se Dodavatel zavazuje tato data zpřístupnit nebo předat:

- a. až po provedení přezkoumání zákonnosti žádosti,
- b. až po vynaložení úsilí o zabránění zpřístupnění nebo předání dat v rámci možností daných právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána,
- c. pouze v nezbytném rozsahu.

5. POVINNOSTI OBJEDNATELE

5.1. Objednatel je povinen zajistit Testovací a Produkční prostředí pro činnost Dodavatele v rámci IT prostředí Objednatele, pokud je to nezbytné pro provádění Plnění. Zajištění prostředí zahrnuje zajištění vzdáleného přístupu personálu Dodavatele do IT prostředí Objednatele, v přiměřeném rozsahu odpovídajícího možnostem Objednatele a Zadávací dokumentaci a při respektování bezpečnostních pravidel Objednatele, zejména bezpečnostní dokumentace, která je součástí Interních předpisů. Objednatel je povinen zajistit fungování Dodavatelem vytvořeného Testovacího prostředí, na kterém bude Software Testován, a Produkčního prostředí, na kterém Software poběží v ostrém provozu, přičemž všechna prostředí budou umístěna na IT prostředí Objednatele, není-li ve Smlouvě stanoveno jinak.

6. LICENČNÍ UJEDNÁNÍ

6.1. Smlouva stanoví, která licenční ujednání dle tohoto článku se použijí ve vztahu k Plnění. Neobsahuje-li Smlouva takový odkaz, použije se ve vztahu k Plnění vedle společných ustanovení k licenčním ujednáním dle [odst. 6.7](#) tohoto článku též [odst. 6.3](#) tohoto článku a ve vztahu k částem Plnění, která obsahují Standardní Software, též [odst. 6.5](#) tohoto článku. Je-li součástí Plnění Hardware, použijí se též pravidla dle [odst. 6.6](#) tohoto článku.

6.2. Odměna za oprávnění dle tohoto článku je zahrnuta v ceně Plnění.

6.3. Postoupení výkonu autorských majetkových práv k Software

- 6.3.1. V případě, že je Software Autorské dílo vznikající v průběhu Plnění, Dodavatel neodvolatelně postupuje na Objednatele oprávnění k výkonu majetkových práv autorských k takovému Autorskému dílu).
- 6.3.2. Dodavatel prohlašuje, že Software byl vytvořen zaměstnanci či Poddodavatelem jako zaměstnanecké dílo ve smyslu § 58 odst. 1 a 7 Autorského zákona, a že je oprávněn k postoupení výkonu majetkových práv v souladu s tímto odst. 6.3 ZOP a má k takovému postoupení náležitě souhlas, přičemž Dodavatel se zavazuje na požádání Objednatele neprodleně předložit nebo jinak vhodným způsobem zpřístupnit dokumenty prokazující rozsah oprávnění Dodavatele.
- 6.3.3. Objednatel je dále oprávněn postoupit oprávnění k výkonu majetkových práv na jakoukoli další třetí osobu dle volby Objednatele a udělovat licence a podlicence, s čímž Dodavatel výslovně souhlasí; pro zamezení pochybnostem je Dodavatel povinen podniknout veškeré kroky k získání náležitých oprávnění tak, aby mohl oprávnění k výkonu majetkového práva postoupit na Objednatele v souladu s tímto odst. 6.3 ZOP. S povinností převodu oprávnění k výkonu majetkových práv se pojí povinnost předání Zdrojového kódu dle čl. 7 ZOP.
- 6.3.4. Dodavatel dále prohlašuje, že má svolení autora/ů k zásahům do Software (včetně jeho Zdrojového a strojového kódu) ve smyslu § 58 odst. 4 Autorského zákona a tato svolení se vztahují na jakékoliv třetí osoby, jež budou vykonávat autorská majetková práva k tomuto Software.
- 6.3.5. Dodavatel dále prohlašuje, že vyloučil oprávnění autorů dle ustanovení § 58 odst. 3 Autorského zákona i vůči všem budoucím vykonavatelům autorských majetkových práv k Software.
- 6.3.6. Dodavatel dále převádí veškerá zvláštní práva pořizovatele k Databázím, jež tvoří součást Plnění. Nedojde-li z jakéhokoliv důvodu k převodu práva dle předchozí věty, uděluje Dodavatel Objednateli oprávnění k vytěžování a zužitkování celého obsahu takové Databáze nebo její kvalitativně nebo kvantitativně podstatné části a právo udělit jinému oprávnění k výkonu tohoto práva.
- 6.3.7. K ostatním majetkovým hodnotám, které spadají pod pojem Software a zároveň nespádají pod definici Autorského díla, uděluje Dodavatel Objednateli oprávnění v rozsahu dle odst. 6.3.8. ZOP. Ustanovení odst. 6.5 a 6.6 ZOP tímto nejsou dotčena.
- 6.3.8. Nevznikne-li Objednateli z jakéhokoliv důvodu ke kterékoliv části Softwaru oprávnění k výkonu autorských majetkových práv, uděluje Dodavatel Objednateli k dotčené části množstevně a územně neomezenou výhradní licenci ke všem známým způsobům užití, a to na dobu trvání autorských majetkových práv. Objednatel je oprávněn k dotčené části Softwaru udělovat licence, tyto dále postoupit a udělovat podlicence třetím osobám. Objednatel je dále oprávněn dotčené části upravovat a měnit (včetně Zdrojového a strojového kódu takové části Software), dokončovat, včetně práva takto upravené či dokončené části užívat, a dále tyto původní, upravené či dokončené části zveřejňovat, spojovat s jiným dílem či zařazovat do díla souborného, zpracovávat, překládat či jinak zasahovat, a to vše i prostřednictvím třetí osoby.

6.4. Nevýhradní licence k Software

- 6.4.1. Ve vztahu k Software Dodavatel tímto uděluje Objednateli okamžikem akceptace Plnění ve smyslu čl. 8 ZOP, nebo jinak vymezeným okamžikem akceptace Plnění Smlouvou a jejími přílohami nevýhradní oprávnění k výkonu práva užití Software v souladu s dalšími podmínkami odst. 6.4 ZOP (dále „**Licence**“). Ustanovení tohoto odstavce se nevztahují na oprávnění Objednatele k Software, který je Standardním Software; tato oprávnění jsou upravena samostatně v odst. 6.5 ZOP. V případě, že je Plnění rozděleno na části, použije se tento odstavec na každou část Plnění.
- 6.4.2. Licence se uděluje jako nevýhradní a opravňuje Objednatele k výkonu práva užití veškerá Autorská díla a k výkonu práva vytěžovat a zužítkovat Databáze, jež tvoří Plnění, a to:

- a. k jakémukoliv účelu;
 - b. na dobu trvání majetkových práv autorských;
 - c. na jakémkoliv území;
 - d. jakýmkoliv způsobem; a
 - e. bez množstevního omezení.
- 6.4.3. Dodavatel okamžikem dle odst. 6.3. ZOP uděluje rovněž oprávnění takový Software upravovat a měnit (včetně Zdrojového a strojového kódu), dokončovat, včetně práva takto upravený, změněný či dokončený Software užívat v rozsahu Licence, a dále tyto původní, upravené, změněné či dokončené části spojovat s jiným dílem či zařazovat do díla souborného, zpracovávat, překládat či jinak do nich zasahovat, a to vše i prostřednictvím třetí osoby
- 6.4.4. Objednatel má v rámci Licence právo udělit k Softwaru podlicenci třetím osobám a právo postoupit Licenci zcela či z části na třetí osoby, s čímž Dodavatel výslovně souhlasí.
- 6.4.5. Licence zahrnuje povinnost Dodavatele předat Objednateli Zdrojový kód a Dokumentaci k Software dle článku 7 ZOP.
- 6.4.6. Licence se vztahuje ve stejné míře a rozsahu jako k Software taktéž na:
- a. Dokumentaci specifikovanou ve Smlouvě nebo jejích přílohách;
 - b. jakoukoliv jinou Dokumentaci předávanou k Software nad rámec Dokumentace dle předchozího písmene;
 - c. loga či jiné předměty duševního vlastnictví, které souvisí s Plněním a jsou vhodné či nezbytné k užití spolu s Plněním;
 - d. jakákoliv jiná Autorská díla či jiné předměty duševního vlastnictví, které souvisí s Plněním.

6.5. Licence ve vztahu ke Standardnímu Software

- 6.5.1. V případech, kdy je součástí Plnění Standardní Software, Dodavatel uděluje Objednateli okamžikem akceptace Plnění ve smyslu čl. 8 ZOP, jehož součástí je Standardní Software, k veškerému takovému Standardnímu Software nevýhradní oprávnění k výkonu práva užít příslušný Standardní Software v souladu s dalšími podmínkami odst. 6.5 ZOP (dále „**Licence k Standardnímu Software**“). V případě, že je Plnění rozděleno na části, použije se tento odstavec na každou část Plnění, jehož součástí je Standardní Software či jeho část.
- 6.5.2. Licence k Standardnímu Software se uděluje jako nevýhradní a opravňuje Objednatele k výkonu práva užít veškerý Standardní Software, a to:
- a. všemi způsoby odpovídajícími účelu, pro který je takový Standardní Software určen;
 - b. na dobu trvání majetkových práv autorských, nebo alespoň na dobu trvání Smlouvy;
 - c. na jakémkoliv území; a
 - d. bez množstevního omezení.
- 6.5.3. Dodavatel je v rámci Licence k Standardnímu Software povinen zajistit poskytnutí podpory (subscription/license maintenance) k veškerému Standardnímu Software, tj. zajistit poskytování nejnovějších verzí Standardního Software Objednateli a dalších služeb v souladu se standardními licenčními podmínkami Standardního Software, a to alespoň na dobu trvání Smlouvy.
- 6.5.4. Objednatel má v rámci Licence k Standardnímu Software oprávnění udělit ke Standardnímu Software podlicenci třetím osobám a právo postoupit Licenci k

Standardnímu Software zcela či z části na třetí osoby, s čímž Dodavatel výslovně souhlasí.

- 6.5.5. Licence k Standardnímu Software se vztahuje ve stejné míře jako k Standardnímu Software taktéž na:
- a. Aktualizaci, Modernizaci a Zásadní modernizaci Standardního Software, který je součástí Plnění;
 - b. Dokumentaci k Standardnímu Software specifikovanou ve Smlouvě nebo jejích přílohách;
 - c. Dokumentaci nad rámec Dokumentace k Standardnímu Software dle předchozího písm.;
 - d. právo užívat a vytěžovat Databáze obsažené ve Standardním Software, který je součástí Plnění;
 - e. loga či jiné předměty duševního vlastnictví, které se Standardním Software, jež je součástí Plnění, souvisí a jsou vhodné či nezbytné k užití spolu s takovým Standardním Software.
- 6.5.6. V parametrech, které nejsou upraveny Smlouvou, jejími přílohami anebo jinou částí Zadávací dokumentace, se Licence k Standardnímu Software řídí příslušnými licenčními podmínkami výrobce Standardního Software.
- 6.5.7. V případě, že Dodavatel využije při plnění předmětu Smlouvy Standardní Software, je Dodavatel za účelem vyloučení vzniku proprietárního uzamčení Objednatele (tzv. vendor lock-in) povinen použít výlučně takový Standardní Software, u kterého jsou splněny podmínky dle definice Standardního Software dle odst. 1.65. písm. a., b., c. nebo d. ZOP, v době využití Standardního Software, a u kterého lze zároveň důvodně předpokládat, že tento stav zůstane zachován minimálně po dobu trvání Smlouvy.
- 6.5.8. V případě, že Dodavatel v rámci plnění Smlouvy použije Standardní Software, který v průběhu trvání Smlouvy nebude anebo přestane splňovat podmínky stanovené v odst. 6.5.7 ZOP, je Dodavatel povinen, po dohodě s Objednatelem, a v případě, že tato dohoda nebude možná, pak dle volby Dodavatele:
- a. na vlastní náklady dodat Objednateli Zdrojový kód předmětného Standardního Software a poskytnout Objednateli oprávnění užívat tento Standardní Software včetně Zdrojového kódu (včetně dalších způsobů nakládání) v rozsahu Licence dle odst. 6.4 ZOP; nebo
 - b. nahradit na vlastní náklady předmětný Standardní Software jiným Standardním Software, který bude mít alespoň srovnatelné funkcionality, kvalitu a technickou způsobilost jako nahrazovaný Standardní Software a zároveň splňovat podmínky stanovené v odst. 6.5.7 ZOP, a poskytnout k tomuto Standardnímu Software Objednateli Licenci k Standardnímu Software dle odst. 6.5 ZOP; nebo
 - c. nahradit na vlastní náklady předmětný Standardní Software vlastním Softwarem, tj. přeprogramovat část Díla představovanou předmětným Standardním Softwarem za využití vlastního Software vytvořeného na míru Objednateli, který bude mít alespoň srovnatelné funkcionality, kvalitu a technickou způsobilost jako nahrazovaný Standardní Software, a poskytnout k tomuto vlastnímu Software Objednateli Licenci dle odst. 6.4 ZOP, a to včetně Zdrojového kódu.
- 6.5.9. Postupy dle odst. 6.5.8 písm. a) až c) ZOP podléhají samostatnému Akceptačnímu řízení. Vznikla-li Dodavateli povinnost dle odst. 6.5.8 ZOP, je Dodavatel povinen splnit povinnosti dle uvedeného odstavce i po ukončení Smlouvy. Ustanovení Smlouvy a ZOP relevantní pro splnění povinností dle předchozí věty se použijí i po ukončení Smlouvy.
- 6.5.10. Pokud v rámci Akceptačního řízení dle čl. 8 ZOP vyjde najevo, že Standardní Software nesplňuje podmínky odst. 6.5.7 ZOP, je Objednatel oprávněn Akceptační řízení přerušit, dokud Dodavatel nenapraví tento nedostatek předmětného Standardního Software jedním ze způsobů uvedených v odst. 6.5.8 ZOP. Objednatel není v takovém případě v prodlení.

6.5.11. Ustanovení [odst. 6.3](#) a 6.6 ZOP se pro Standardní Software nepoužijí.

6.6. Software vztahující se k Hardware

6.6.1. V případech, kdy je k řádnému užívání dodaného Hardwaru potřebný určitý Software, je Dodavatel povinen poskytnout/zajistit Objednateli jako součást Plnění a za cenu zahrnutou v ceně Hardwaru, oprávnění užít tento Software v rozsahu, způsoby a za účelem obvyklým ve vztahu k Hardwaru, se kterým je spojen, nejméně však za podmínek dle Smlouvy a jejích příloh.

6.6.2. Ustanovení [odst. 6.3](#) a 6.4 ZOP se pro Software vztahující se k Hardwaru nepoužijí.

6.7. Společná ustanovení

6.7.1. Nestanoví-li Smlouva a její přílohy či jiné části Zadávací dokumentace jinak, je Dodavatel při plnění Smlouvy oprávněn využít programy s otevřeným kódem či jejich části distribuovanými pod FOSS licencemi. Dodavatel však není oprávněn využít programy s otevřeným kódem či jejich části, které jsou distribuovány pod FOSS licencemi, jejichž podmínky by Objednateli ukládaly povinnost sdělovat nebo jinak šířit Software či jeho části, včetně Zdrojových kódů, třetím osobám, nebo umožnit jim změny, úpravy či jiné zásahy do Softwaru nebo jeho části.

6.7.2. Dodavatel je povinen zajistit Objednateli udělení oprávnění k veškerým programům s otevřeným kódem poskytnutým Objednateli v rozsahu takových FOSS licencí, které se na konkrétní program s otevřeným kódem, který je součástí Plnění, vztahují, přičemž konkrétní rozsah licence lze určit odkazem na soubor předávaný v rámci výstupu z Plnění anebo odkazem ve Zdrojovém kódu či jiným označením takové licence ve formátu vyžadovaném takovou veřejnou licencí, včetně odkazu na kompletní znění aktuálních licenčních podmínek příslušné FOSS licence; Dodavatel je dále povinen zajistit poskytnutí podpory k veškerým programům s otevřeným kódem, které jsou součástí Plnění, tj. povinnost Dodavatele zajistit poskytování nejnovějších verzí programů s otevřeným kódem a dalších služeb v souladu se standardními licenčními podmínkami programů s otevřeným kódem, a to alespoň na dobu trvání této Smlouvy. Ustanovení čl. 7 ZOP se pro programy s otevřeným kódem či jejich části, které jsou distribuovány pod FOSS licencemi, použije obdobně.

6.7.3. Dodavatel prohlašuje, že je oprávněn udělit Objednateli veškerá oprávnění v souladu s tímto článkem ZOP, má k takovému udělení veškeré potřebné souhlasy a jejich udělením Objednateli ani užíváním Plnění Objednatelem či uživateli Objednatele nebudou porušena práva duševního vlastnictví třetí osoby. Dodavatel odpovídá Objednateli za zajištění všech nezbytných oprávnění a souhlasů autora či autorů Software či Standardního Software k oprávněním udělovaným Objednateli dle tohoto článku ZOP. Dodavatel se zavazuje na výzvu Objednatele poskytnout Objednateli o zajištění oprávnění a veškerých souhlasů dle tohoto článku ZOP písemné prohlášení a tyto skutečnosti prokázat.

6.7.4. V případě, že by třetí osoba vznesla vůči Objednateli jakékoliv nároky z porušení práv duševního vlastnictví v souvislosti s užíváním Plnění Objednatelem, se Dodavatel zavazuje přijmout taková opatření, aby Objednatel byl Plnění oprávněn nerušeně užívat, a to zejména zajistit pro Objednatele udělení oprávnění v rozsahu dle tohoto článku ZOP bez dalších nákladů a požadavků na úplatu od Objednatele.

6.7.5. V případě, že jakákoliv třetí osoba uplatní nárok z důvodu porušení práv duševního vlastnictví ve vztahu k Plnění, je Dodavatel povinen nahradit Objednateli veškerou újmu takto způsobenou, jakož i účelné náklady vynaložené na obranu práv Objednatele. Dodavatel se v takovém případě dále zavazuje na svůj náklad poskytnout Objednateli veškerou možnou součinnost k ochraně jeho práv a oprávnění dle tohoto článku ZOP, zejména mu poskytnout všechny podklady, informace a vysvětlení k prokázání neoprávněnosti nároku třetí strany.

6.7.6. V případě nároku dle předchozího [odst. 6.7.5](#) ZOP, nebo je-li důvodné předpokládat, že takový nárok bude uplatněn, zajistí Dodavatel Objednateli možnost dále příslušný výstup užívat bez nároku na úplatu nad rámec sjednaný ve Smlouvě.

- 6.7.7. Spolu se Standardním Software, je-li součástí Plnění, musí být Objednateli vždy předána kompletní Dokumentace, tj. zejména uživatelská, administrátorská, provozní dokumentace a dokumentace jeho API.

7. ZDROJOVÝ KÓD A DOKUMENTACE

- 7.1. Zdrojový kód bude předáván Objednateli na datovém nosiči společně s předáním výstupu z Plnění pro účely zahájení Akceptačního řízení, nebo za podmínek stanovených ve Smlouvě, zejména pokud bude smluvní vztah ukončen bez provedení Akceptačního řízení.
- 7.2. Na datovém nosiči dat musí být viditelně označen „Zdrojový kód“ s označením části Modifikace a jeho verze a den předání Zdrojového kódu. O předání nosiče dat bude oběma Smluvními stranami sepsán a podepsán písemný předávací protokol.
- 7.3. Povinnost Dodavatele předávat Zdrojový kód se přiměřeně použije i pro jakékoliv opravy, změny, doplnění, upgrade nebo update Zdrojového kódu v rámci následného provádění Plnění anebo v rámci záručních oprav. Zdrojový kód musí obsahovat podrobný popis a komentář každého zásahu do Zdrojového kódu.
- 7.4. Objednatel nebude v průběhu provádění Plnění sám anebo prostřednictvím jiných osob zasahovat do Zdrojového kódu nasazeného anebo fungujícího v Produkčním prostředí či Testovacím prostředí.
- 7.5. Dodavatel je povinen předat Objednateli příslušnou Dokumentaci a Zdrojový kód ve standardní podobě (to nejméně v kvalitě obvyklé pro open source projekty), vždy obsahující následující:
- a. Kompletní Zdrojové kódy celého díla.
 - b. Uživatelskou příručku obsahující konkrétní popis uživatelského prostředí, funkcí a postupů pro zaškolení zaměstnanců.
 - c. Administrátorskou příručku, popisující všechny parametry, které lze konfigurovat a popis dopadů změny konfigurace do systému.
 - d. Technickou dokumentaci systému, pakliže se jedná o vícevrstvou architekturu, popis každé vrstvy zvlášť:
 - i. Datová vrstva – popis datové vrstvy, čili tabulek v databázi včetně vazeb mezi tabulkami a včetně E-R schémat.
 - ii. Aplikační vrstva – popis jádra systému, jeho funkcí, služeb a rozhraní. Dokumentace musí obsahovat kompletní popis architektury jádra systému, výčet a podrobný popis všech jeho funkcí, přehled a popis služeb, které jádro poskytuje dalším komponentám systému, modulům a knihovnám.
 - iii. Prezentační vrstva – Dokumentace systému musí obsahovat drátové modely všech obrazovek uživatelského rozhraní včetně popisu funkcí prvků každé obrazovky.
 - e. Popis konfigurace provozního prostředí systému (serverová strana i klientská strana).
 - f. Dokumentace musí obsahovat soupis všech požadavků na nastavení hardwarových a softwarových komponent běhového prostředí jako jsou:
 - i. mapování souborových systémů;
 - ii. požadavky na operační paměť a procesory;
 - iii. konfigurační parametry jednotlivých podpůrných Softwarových prostředků (např. specifika pro nastavení databáze, aplikačního serveru, webového serveru apod.).
 - g. Objednatel požaduje, aby tato Dokumentace byla ve formátech XML DocBook (zdrojové) a PDF (export z XML zdroje pro snadnou distribuci uživatelům) nebo případně v jiném formátu, který Objednatel schválí po vzájemné dohodě s Dodavatelem. Všechny Dokumentace musí být verzované, opatřené seznamem

autorů, přehledem změn jednotlivých verzí a musí být obsahově úplné pro tu část systému, kterou popisují.

- h. Řešení musí obsahovat návod na používání systému (uživatelský manuál) a popis systému – jeho vlastností, strukturu projektu, použité technologie (technická dokumentace). Součástí řešení je i Dokumentace a automaticky generovaná dokumentace (Javadoc). Součástí Dokumentace musí být zip archiv se zdrojovými soubory řešení a programátorskou dokumentací.

7.6. V případě jakýchkoli pochybností o správnosti předání Zdrojového kódu se bude uvedené posuzovat podle svého účelu, tedy zejména následné možnosti provádět samostatně či prostřednictvím třetích osob opravy, změny, doplnění, upgrady nebo updaty Zdrojového kódu. Za nesprávné předání se přitom považuje takové předání, které v důsledku vede ke znemožnění či podstatnému ztížení práce se Zdrojovým kódem ve výše uvedeném smyslu.

8. AKCEPTAČNÍ ŘÍZENÍ

8.1. Akceptační řízení Předmětu Smlouvy

- 8.1.1. Předání a převzetí Předmětu Smlouvy (tj. včetně Zdrojových kódů a Dokumentace) probíhá na základě Akceptačního řízení, tj. postupným provedením akceptačních procesů a podepsáním Akceptačního protokolu. Je-li Předmět Smlouvy rozdělen na části, použije se tento článek obdobně pro každou část, nestanoví-li Smlouva jinak. Jsou-li součástí Předmětu Smlouvy Služby nebo Paušální služby, použijí se, nestanoví-li Smlouva jinak, pro Služby ustanovení [odst. 8.2 ZOP](#) a pro Paušální služby ustanovení [odst. 8.3 ZOP](#).
- 8.1.2. Akceptační řízení zahrnuje porovnání skutečných vlastností a funkcionalit s Akceptačními kritérii.
- 8.1.3. Nestanoví-li Smlouva či její přílohy Akceptační kritéria, rozumí se jimi:
 - a. vlastnosti a funkcionality uvedené ve specifikaci plnění určené Objednatelem, která je součástí Smlouvy, a dále vlastnosti a funkcionality uvedené ve specifikaci plnění Dodavatele či návrhu řešení (jsou-li takové), která je součástí Smlouvy, a
 - b. požadavky na Zdrojové kódy a Dokumentaci dle čl. 7 ZOP.
- 8.1.4. Dodavatel je povinen písemně informovat Objednatele minimálně se sedmi denním předstihem o termínu předání Předmětu Smlouvy či její části, nedohodnou-li se strany jinak.
- 8.1.5. Dodavatel předá Objednateli Předmět Smlouvy k realizaci Akceptačního řízení. Akceptační řízení může být zahájeno pouze v případě, že Předmět Smlouvy byl Dodavatelem skutečně předán Objednateli, a ten se s ním mohl seznámit. Objednatel na žádost Dodavatele bez zbytečného odkladu potvrdí převzetí Předmětu Smlouvy k Akceptačnímu řízení v Servicedesku, e-mailem, anebo jiným dohodnutým způsobem. Potvrzením převzetí Díla k Akceptačnímu řízení ve smyslu tohoto odstavce je zahájeno Akceptační řízení.
- 8.1.6. Předmět Smlouvy je způsobilý k akceptaci Objednatelem, pokud:
 - a. splňuje Akceptační kritéria a současně nevykazuje žádnou Vadu kategorie A, B a C či jiné zjevné vady (zejména vady, pro které není vhodné dělení Vad dle ZOP - > např. Některé vady Hardware jsou-li součástí plnění), pak Objednatel vyznačí na Akceptačním protokolu „**Akceptováno**“; nebo
 - b. splňuje Akceptační kritéria a současně nevykazuje žádnou Vadu kategorie A, B a současně nemá více než:
 - i. 30 Vad kategorie C nebo drobných vad, jež nebrání řádnému užívání Předmětu Smlouvy, je-li předmětem akceptace vytvoření Software či Dokumentace či vytvoření části Software či Dokumentace
 - ii. 10 Vad kategorie C nebo drobných vad, jež nebrání řádnému užívání Předmětu Smlouvy, nejde-li o případ uvedený v [odst. 8.1.6 písm. b. i.](#)

pak Objednatel vyznačí na Akceptačním protokolu „**Akceptováno s výhradou**“.

- 8.1.7. V jiných případech než dle odst. 8.1.6 ZOP vyznačí Objednatel na Akceptačním protokolu „**Neakceptováno**“.
- 8.1.8. Nedohodnou-li se Smluvní strany jinak, připraví Dodavatel návrh Akceptačního protokolu, který musí obsahovat minimálně:
- a. označení Smluvních stran a odkaz na Smlouvu,
 - b. seznam Akceptačních kritérií společně s vedlejším sloupcem pro možnost vyznačení, zda Předmět Smlouvy splňuje příslušné Akceptační kritérium (např. ano/ne)
 - c. tabulku pro možnost vepsání zjištěných Vad včetně možnosti uvedení, o jakou Vadu se jedná (A/B/C),
 - d. tabulku pro možnost vepsání dalších zjištěných vad,
 - e. prostor pro závěrečné hodnocení (např. formou výběru z kolonek „**Akceptováno**“, „**Akceptováno s výhradou**“, „**Neakceptováno**“) a
 - f. podpisové doložky pro oprávněné osoby za Smluvní strany.
- 8.1.9. Objednatel je povinen do 30 kalendářních dnů (v případě, že lhůta pro plnění akceptované části byla kratší než 60 kalendářních dnů, pak do 14 kalendářních dnů, nikdy však déle než činí polovina lhůty pro plnění) ode dne zahájení Akceptačního řízení posoudit Předmět Smlouvy postupem dle odst. 8.1.2 ZOP a v případě dle odst. 8.1.6 ZOP podepsat Akceptační protokol a vyznačit na něm „**Akceptováno**“, nebo „**Akceptováno s výhradou**“ včetně vyznačení Vad/y či vad/y. V opačném případě je Objednatel povinen ve výše uvedené lhůtě podepsat Akceptační protokol společně s vyznačením „**Neakceptováno**“ včetně vyznačení nesplněných Akceptačních kritérií nebo vyznačení Vad/y a jejich/její kategorizace (A, B nebo C) nebo vyznačení dalších vad.
- 8.1.10. Okamžikem podpisu Akceptačního protokolu společně s vyznačením „**Akceptováno**“, nebo „**Akceptováno s výhradou**“ je Předmět Smlouvy proveden.
- 8.1.11. Podpis Akceptačního protokolu s vyznačením „**Akceptováno s výhradou**“ nezbavuje odpovědnosti Dodavatele odstranit vyznačené Vady či vady. Dodavatel je povinen takové Vady či vady odstranit ve lhůtě určené Objednatelem, jinak do třiceti (30) kalendářních dnů od podpisu Akceptačního protokolu s vyznačením „**Akceptováno s výhradou**“. Neodstranění Dodavatel Vady či vady ve lhůtě dle tohoto odstavce, jedná se porušení této Smlouvy podstatným způsobem. Do doby odstranění vyznačených Vad či vad dle tohoto odstavce nezaplatí Objednatel Dodavateli část Ceny (či ceny příslušné části Plnění, je-li plněno po částech) odpovídající její padesáti (50) procentní výši. Objednatel není v takovém případě v prodlení se zaplacením části Ceny (či ceny příslušné části Plnění, je-li plněno po částech) dle předchozí věty. Pro účely ověření splnění povinností Dodavatele dle tohoto odstavce, je Dodavatel Objednateli povinen prokázat, že Plnění již nemá Vady či vady. Povinnost odstranit Vady či vady dle tohoto odstavce není splněna, neodstranil-li Dodavatel Vady či vady nebo objeví-li se v průběhu ověření:
- a. nové Vady či vady, které vznikly v souvislosti s odstraňováním původních Vad či vad, nebo
 - b. Vady či vady, které v důsledku existence původních Vad či vad nebylo možné v Akceptačním řízení odhalit, nebo které bylo možno odhalit pouze s výraznými obtížemi.
- 8.1.12. V případě neakceptování Předmětu Smlouvy vyznačením na Akceptačním protokolu „**Neakceptováno**“ se Dodavatel zavazuje odstranit nesplněná Akceptační kritéria a Vady uvedené v Akceptačním protokolu ve lhůtách výslovně stanovených v Akceptačním protokolu Objednatelem, a pokud nejsou takové, pak lhůtách přiměřených. Do odstranění nedostatků bránících akceptování není Předmět Smlouvy

proveden. Po odstranění nedostatků uvedených v Akceptačním protokolu Dodavatel opětovně předá Předmět Smlouvy Objednateli k dalšímu kolu Akceptačního řízení a Objednatel postupuje obdobně podle [odst. 8.1.5 ZOP](#).

8.2. Akceptační řízení ve vztahu ke Službám

- 8.2.1. Řádné provedení Služeb bude Stranami písemně potvrzeno podpisem Akceptačního protokolu po ukončení Akceptačního řízení obdobně dle [odst. 8.1 ZOP](#) (s výjimkou [odst. 8.1.3 ZOP](#)). Pro účely akceptace Služeb se Předmětem Smlouvy rozumí příslušný výstup ze Služeb (např. rozvoj Software). Strany jsou oprávněny zkrátit lhůty Akceptačního řízení ve smyslu [odst. 8.1 ZOP](#) v dílčí smlouvě uzavřené na základě Smlouvy. Nestanoví-li dílčí smlouva Akceptační kritéria Služby, rozumí se jimi:
- a. vlastnosti a funkcionality uvedené ve specifikaci plnění Objednatele, která je součástí dílčí smlouvy uzavřené na základě Smlouvy, a dále vlastnosti a funkcionality uvedené ve specifikaci plnění Dodavatele (je-li taková), která je součástí dílčí smlouvy, a
 - b. požadavky na Zdrojové kódy a Dokumentaci dle čl. 7 ZOP.
- 8.2.2. Jsou-li Služby plněny po částech, použijí se ustanovení pro Akceptační řízení ve vztahu ke Službám přiměřeně vždy na každou takovou dílčí část výstupu ze Služeb, nedohodnou-li se Strany výslovně jinak.
- 8.2.3. Akceptační řízení se neprovádí u Služeb, které z povahy věci nepodléhají Akceptačnímu řízení (např. konzultace apod.). Služby musí být v souladu s dílčí smlouvou a přílohou č. 1 této Smlouvy. Uvedeným postupem nejsou dotčena práva z vadného plnění ve vztahu k takovým Službám.

8.3. Akceptační řízení ve vztahu k Paušálním službám

- 8.3.1. Řádné provádění Paušálních služeb bude každý měsíc potvrzováno podpisem výkazu Paušálních služeb za bezprostředně předcházející měsíc. Podpisem výkazu Paušálních služeb Objednatelem jsou Paušální služby za příslušný měsíc akceptovány/provedeny. Objednatel není povinen podepsat výkaz Paušálních služeb, nebyly-li jednotlivé Paušální služby v příslušném měsíci řádně provedeny (jedná se např. o Paušální služby, u nichž konec lhůty pro splnění - např. doba pro vyřešení Incidentu - spadá do příslušného měsíce).
- 8.3.2. Návrh výkazu dle předchozího odstavce připraví Dodavatel. Výkaz musí obsahovat soupis provedených Paušálních služeb za bezprostředně předcházející měsíc a soupis dosud neukončených činností Paušálních služeb. Výkaz Paušálních služeb je Dodavatel povinen doručit nejpozději do deseti (10) kalendářních dnů po skončení měsíce, ve které byly služby poskytnuty.

8.4. Akceptační řízení ve vztahu ke školení

- 8.4.1. Dokladem o řádném provedení školení je prezenční listina podepsána účastníky školení, případně vydání certifikátu, mělo-li být školení zakončené vydáním certifikátu.
- 8.4.2. Vznikají-li pro školení školící materiály, akceptují se v akceptačním řízení [odst. 8.1 ZOP](#) se použije přiměřeně. V takovém případě je školení řádně provedené dnem, v němž je akceptován poslední požadovaný výstup.
- 8.4.3. V případě, že předmětem školení je hands-on školení, je školení řádně provedeno akceptací výstupu, který byl předmětem hands-on školení dle [odst. 8.1 ZOP](#).

8.5. Akceptace ve vztahu k Hardware

- 8.5.1. Je-li předmětem Smlouvy či dílčí části, jež je určena k akceptaci pouze dodání Hardware, použije se pro akceptaci odstavec 8.5 ZOP.
- 8.5.2. Řádné dodání Hardware se předává a přebírá na základě předávacího protokolu podepsaného odpovědnými zástupci smluvních stran.
- 8.5.3. Nestanoví-li Smlouva či její přílohy jinak, Objednatel ověřuje v rámci akceptace Hardware:

- a. parametry, vlastnosti a funkcionality uvedené ve specifikaci plnění Objednatele, která je součástí Smlouvy, a dále vlastnosti a funkcionality uvedené ve specifikaci plnění Dodavatele (je-li taková), která je součástí Smlouvy;
- b. příslušenství a dokumentaci, jež mělo být dodáno spolu s Hardware.

9. ŠKOLENÍ

- 9.1. Vyplývá-li ze Smlouvy Dodavateli povinnost poskytnout školení, aniž jsou blíže určeny jeho podmínky, zavazuje se Dodavatel poskytnout školení osobám určeným Objednatelem pomocí metod výkladu (zejména popis jednotlivých prvků a funkcionalit Předmětu Smlouvy ve vztahu k jeho užívání), praktických ukázek obsluhy Předmětu Smlouvy a zodpovězení dotazů školených osob tak, aby tyto osoby byly na základě provedeného školení ve vztahu ke svým rolím nebo pracovnímu zařazení (dle sdělení Objednatele) schopné plně porozumět svým odpovědnostem při obsluze Předmětu Smlouvy, provádět obsluhu v souvislosti se svou rolí nebo pracovním zařazením samostatně, a přitom minimalizovat riziko chybné obsluhy nebo závad na Předmětu Smlouvy.
- 9.2. Dodavatel provede zaškolení příslušných osob určených Objednatelem v termínu dle Smlouvy, a pokud takový termín není, pak v termínu určeném Objednatelem po dohodě s Dodavatelem.
- 9.3. Dodavatel je dále povinen provést v přiměřeném rozsahu školení příslušných zaměstnanců Dodavatele a dalších osob podílejících se na poskytování Plnění dle Smlouvy za účelem splnění povinností dle čl. 21. ZOP. Tuto skutečnost je povinen na vyžádání Objednateli prokázat.

10. SERVICEDESK

- 10.1. Dodavatel se zavazuje:
 - 10.1.1. nejpozději v den účinnosti Smlouvy založit a po celou dobu trvání Smlouvy udržovat v provozu Servicedesk (včetně úhrady případných licenčních poplatků za aplikaci Servicedesk) a udělit náležitá oprávnění k přístupu do Servicedesku, a to v počtu přístupů pro Ohlašovatele dle určení Objednatele. Servicedesk bude fungovat prostřednictvím webové adresy;
nebo
 - 10.1.2. po celou dobu trvání Smlouvy užívat Servicedesk provozovaný Objednatelem.
- 10.2. Provozovatele Servicedesku stanoví Smlouva. Pokud Smlouva provozovatele Servicedesku nestanoví, má se za to, že provozovatelem Servicedesku je Dodavatel. V případě, že provozovatelem bude Objednatel, poskytne Dodavateli nezbytnou součinnost k řádnému užívání Servicedesku včetně případného poskytnutí licencí.
- 10.3. Dodavatel se zavazuje zajistit Servicedesk prostřednictvím přímého přístupu do Servicedesku na webové adrese určené Dodavatelem/Objednatelem dle provozních podmínek aplikace Servicedesk, případně prostřednictvím přímého datového propojení Servicedesků Objednatele a Dodavatele, a to v jednom z následujících režimů, který je vymezen ve Smlouvě:
 - a. Režim 1:
7x24, tj. dvacet čtyři (24) hodin sedm (7) dní v týdnu.
 - b. Režim 2:
7x12, tj. dvanáct (12) hodin sedm (7) dní v týdnu.
 - c. Režim 3:
5x12, tj. dvanáct (12) hodin pět (5) dní v týdnu
 - d. Režim 4:
5x8, tj. osm (8) hodin pět (5) dní v týdnu.
- 10.4. Nestanoví-li Smlouva jinak, počíná časový rozsah dle zvoleného režimu dle odst. 10.3 ZOP (s výjimkou režimu 1) shodně s časovým rozsahem dle zvoleného Servisního modelu dle odst. 12.2 ZOP (např. pokud doba Servisního modelu začíná každý pracovní den v 7:00, provoz Servicedesku v rámci příslušného režimu začíná rovněž v 7:00).

- 10.5. Servicedesk zahrnuje mimo jiné příjem a evidenci Incidentů a Požadavků, oznámení o potřebě součinnosti Objednatele a dalších zpráv, potvrzování jejich přijetí, předávání jednotlivých úkolů odpovědným osobám, sledování stavu, průběhu a procesu prací a dalších zpráv, informování o stavu řešení, vytváření přehledů a statistik, a to přes přehledné webové rozhraní. Je-li Servicedesk provozován Dodavatelem musí být zabezpečen tak, aby odpovídal požadavkům vyplývajícím ze ZoKB a Interních předpisů. Výstupem z Servicedesku je záznam o veškerých úkonech Servicedesku ve formě přehledného logu, jež umožňuje vyhledávání a uchovávání záznamů tak, aby byly naplněny požadavky ZoKB a Interních předpisů na takové záznamy.
- 10.6. Servicedesk bude dostupný pouze pro Objednatele a Ohlašovatele.
- 10.7. Nestanoví-li Smlouva jinak, je Dodavatel povinen nezávisle na Servicedesku mít nejpozději k okamžiku nabytí účinnosti Smlouvy zřízenou elektronickou adresu a telefonní linku a tuto adresu a telefonní číslo linky sdělit Objednati, a to vše pro účely min. příjmu oznámení Incidentů a Požadavků, vznášení dotazů k Plnění, získávání odpovědí ve vztahu k Plnění a pro další komunikace dle Smlouvy. Doba provozu elektronické adresy a telefonní linky bude odpovídat zvolenému režimu Servicedesku dle odst. 10.3 ZOP.

11. NAHLÁŠENÍ INCIDENTU

- 11.1. Hlášení o Incidentu Dodavateli bude provedeno Ohlašovatelem bezodkladně po zjištění Incidentu, a to přímým zadáním Incidentu do Servicedesku (vytvoření ticketu v Servicedesku, tj. okamžikem, jímž se ticket zpřístupní Dodavateli), odesláním e-mailu nebo telefonátem na kontaktní číslo dle odst. 10.7 ZOP, přičemž Ohlašovatel je povinen uvést popis Incidentu, a to v následujícím rozsahu:
 - a. krátký a rámcově výstižný název Incidentu;
 - b. identifikace části Předmětu Plnění, které se Incident týká;
 - c. určení prostředí (Testovací prostředí, Produkční prostředí);
 - d. detailní popis Incidentu, průvodních jevů a všech významných souvisejících informací;
 - e. kategorii Incidentu (A, B, C);
 - f. identifikaci Ohlašovatele.
- 11.2. V případě, že některá z náležitosti dle odst. 11.1. ZOP chybí nebo je nedostatečná, může si Dodavatel vyžádat její doplnění od Ohlašovatele; tato skutečnost však nemá vliv na určení Času nahlášení Incidentu, ledaže bez tohoto doplnění hlášení Incidentu postrádá informaci natolik podstatnou, že bez ní objektivně nelze přistoupit k řešení Incidentu a Dodavatel o této skutečnosti Objednatele vyrozuměl, a to nejpozději v době určené na zpracování Incidentu dle určeného Servisního modelu dle čl. 12 ZOP, v takovém případě je Incident dle 11.3 ZOP nahlášen okamžikem doplnění požadované informace.
- 11.3. Je-li Incident nahlášován prostřednictvím Servicedesku, pak se za Čas nahlášení Incidentu považuje čas vytvoření ticketu v Servicedesku. Je-li Incident nahlášován písemně na e-mailovou adresu, pak se za Čas nahlášení Incidentu považuje čas odeslání e-mailu z e-mailového serveru Ohlašovatele, nebo v případě hlášení Incidentu telefonicky čas ukončení telefonického hovoru. Dodavatel je povinen prokazatelným způsobem bezodkladně potvrdit přijetí nahlášení Incidentu, a to vždy prostřednictvím Servicedesku. Nepotvrdí-li Dodavatel přijetí Incidentu, nemá to vliv na Čas nahlášení Incidentu.
- 11.4. Je-li je Incident nahlášen mimo časový rozsah Servisního modelu, avšak v rámci časového rozsahu Servicedesku dle zvoleného režimu dle odst. 10.3 ZOP, považuje se za Čas nahlášení Incidentu okamžik začátku nejbližšího následujícího časového rozsahu Servisního modelu.
- 11.5. Dodavatel se zavazuje po dobu poskytování Plnění evidovat všechny nahlášené Incidenty a způsob jejich řešení, včetně časových údajů o průběhu řešení jednotlivých Incidentů ve Výkazech.
- 11.6. Není-li v Servisní smlouvě, jejích přílohách jinak, ustanovení článku 11. ZOP se použijí přiměřeně i na nahlášení a evidování Požadavků.
- 11.7. Ustanovení článku 21 o Kybernetických bezpečnostních incidentech a Kybernetických bezpečnostních událostech se považují za speciální vůči tomuto článku 11 ZOP.

12. SERVISNÍ MODELY

- 12.1. Servisní model představuje standardizovaný model provozu a podpory aplikace, systému nebo instance služby.
- 12.2. Pokud je součástí Smlouvy zajištění provozu a podpory Softwaru nebo Hardwaru, je ve Smlouvě vymezen jeden z níže uvedených Servisních modelů:

Servisní model	Dostupnost	Doba provozu		Doba zpracování Incidentu	Doba vyřešení Incidentů kategorie A	Doba vyřešení Incidentů kategorie B	RTO	RPO	Doba zpracování Požadavku	Doba vyřešení Požadavku kategorie A	Doba vyřešení Požadavku kategorie B
A1 Kritický	99.5%	7x24	(0-24)	1 hod	2 hod	2 hod	4 hod	< 5 min	1 PD	1 PD	3 PD
A2 Kritický	99.5%	7x12	(6-18)	1 hod	2 hod	2 hod	4 hod	< 5 min	1 PD	1 PD	3 PD
A3 Kritický	99.5%	5x8	(7-15)	1 hod	2 hod	2 hod	4 hod	< 5 min	1 PD	1 PD	3 PD
A4 Kritický	99.5%	7x24	(0-24)	1 hod	4 hod	12 hod	4 hod	< 5 min	1 PD	2 PD	5 PD
A5 Kritický	99.5%	5x8	(7-15)	1 hod	4 hod	12 hod	4 hod	< 5 min	1 PD	2 PD	5 PD
B1 Závažný	98.0%	7x24	(0-24)	1 PD	2 PD	3 PD	48 hod	30 min	2 PD	3 PD	5 PD
B2 Závažný	98.0%	7x12	(6-18)	1 PD	2 PD	3 PD	48 hod	30 min	2 PD	3 PD	5 PD
B3 Závažný	98.0%	5x8	(7-15)	1 PD	2 PD	3 PD	48 hod	30 min	2 PD	3 PD	5 PD
C1 Normální	97.0%	5x12	(6-18)	1 PD	3 PD	6 PD	96 hod	24 hod	3 PD	7 PD	10 PD
C2 Normální	97.0%	5x8	(7-15)	1 PD	3 PD	6 PD	96 hod	24 hod	3 PD	7 PD	10 PD
D Minoritní	94.0%	5x8	(7-15)	2 PD	10 PD	14 PD	96 hod	24 hod	5 PD	10 PD	14 PD
E1 Customizovaný											
E2 Customizovaný											

12.3. Doba řešení Incidentu a Požadavku kategorie C je pro veškeré Servisní modely stanovena na 15 PD.

12.4. Do měření úrovně Dostupnosti (Software) nejsou započítávány:

- dočasné vyřazení Softwaru z provozu na základě předchozí dohody Objednatele a Dodavatele (odstávka),
- pravidelná vyřazení Softwaru z provozu Dodavatelem v časech sjednaných ve Smlouvě nebo její příloze (servisní okna),
- smluvními stranami předem dohodnutý časový úsek za účelem instalace upgradu,
- výpadky Softwaru způsobené Objednatelem přímo v důsledku jím provedených zásahů do Softwaru, které nebyly Dodavatelem předem schváleny,
- skutečnosti ve vztahu k Hardware dle odst. 12.9 ZOP za podmínek, že je takový Hardware součástí Plnění a současně je nezbytný pro fungování Software.

12.5. Nedostupnost Softwaru dle odst. 12.4. ZOP se nepovažuje za nedosažení sjednaných parametrů Dostupnosti dle Smlouvy a nebude započítána do výpočtu dle odst. 12.6. a 12.7. ZOP.

12.6. Nestanoví-li Smlouva jinak, bude Dostupnost Software měřena na základě následujícího vzorce:

$$Dostupnost (\%) = \frac{Doba\ provozu - Doba\ výpadku}{Doba\ provozu} \times 100$$

- 12.7. Doba výpadku Softwaru je časový úsek z Doby provozu v hodinách, kdy je služba nedostupná, a počítá se podle následujícího vzorce:

$$Doba\ výpadku = \sum_i^n T_i$$

kde:

Σ je celková doba všech výpadků Softwaru za vyhodnocované období

T_i je doba jednotlivého výpadku Softwaru

n je počet všech výpadků

- 12.8. Doba Provozu Softwaru definovaná pro účely tohoto článku je celková doba provozu Softwaru v hodinách za vyhodnocované období, kterým je kalendářní měsíc.

- 12.9. Do měření úrovně Dostupnosti (Hardware) nejsou započítávány:

- a. dočasná vyřazení Hardware z provozu na základě předchozí dohody Objednatele a Dodavatele (odstávka),
- b. pravidelná vyřazení Hardware z provozu Dodavatelem v časech sjednaných ve Smlouvě nebo její příloze (servisní okna)
- c. výpadky Hardware způsobené Objednatelem přímo v důsledku jím provedených zásahů do Hardware, které nebyly Dodavatelem předem schváleny

- 12.10. Ustanovení odst. 12.5. až 12.8 ZOP se použijí obdobně s tím, že odkaz v odst. 12.5 ZOP na odst. 12.4 ZOP se nahrazuje odkazem na odst. 12.9 ZOP a slovo Software se nahrazují slovem Hardware.

13. AKTUALIZACE PLNĚNÍ

- 13.1. Pokud bude Dodavatel v rámci provozu Plnění provádět jeho aktualizaci, bude postupovat podle:

13.1.1. hardeningových bezpečnostních politik, které jsou určeny standardem Center for Internet Security (CIS) level (group) 1, dostupné z <https://www.cisecurity.org>.

13.1.2. v souladu s Interními předpisy Objednatele a

13.1.3. v souladu s dokumentem v příloze – Platforma SŽ.

- 13.2. Dodavatel odpovídá za to, že systémy dodávané do Plnění budou obsahovat nejnovější, stabilní, bezpečné a řádně odzkoušené bezpečnostní aktualizace (patche).

- 13.3. Veškerý software musí splňovat požadavek na podporu od výrobce (podporovaný build).

- 13.4. Dodavatel je povinen za součinnosti oprávněných osob na straně Objednatele:

13.4.1. provádět analýzy topologie sítě či skenování aktivních částí Plnění;

13.4.2. realizovat bezpečnostní opatření pro odstranění nebo blokování síťových spojení, která neodpovídají požadavkům na ochranu integrity komunikační sítě a

13.4.3. zajistit řízení komunikace v rámci komunikační sítě a integritu dat při vzdáleném přístupu nebo při přístupu do komunikační sítě pomocí bezdrátových technologií.

14. ÚČAST PODDODAVATELŮ

- 14.1. Poddodavatele, jejichž prostřednictvím Dodavatel prokazoval kvalifikaci ve Veřejné zakázce, je Dodavatel povinen využívat při Plnění Smlouvy po celou dobu jejího trvání v rozsahu, v jakém jimi prokazoval kvalifikaci. Poddodavatele, jimiž Dodavatel prokazoval kvalifikaci ve Veřejné zakázce, lze vyměnit pouze s předchozím listinným souhlasem Objednatele, který může být dán výlučně za

předpokladu, že tyto osoby budou nahrazeny osobami splňujícími kvalifikaci požadovanou ve Veřejné zakázce ve stejném rozsahu jako nahrazované osoby.

- 14.2. Dodavatel se zavazuje, že při poskytování Plnění pro Objednatele budou všichni Poddodavatelé, které Dodavatel využívá k poskytnutí Plnění dle Smlouvy, dodržovat veškeré požadavky vyplývající ze Smlouvy a Příloh Smlouvy. Dodavatel odpovídá za to, že jeho Poddodavatelé budou k tomuto závázání a nebudou jednat v rozporu s ujednáními Smlouvy a jejími Přílohami, kterou mezi sebou uzavřeli Dodavatel a Objednatel.
- 14.3. Významný dodavatel je oprávněn využit k Plnění dle Smlouvy Poddodavatele neuvedené ve Smlouvě jen v případě, že to Smlouva výslovně připouští, a to za podmínek v ní uvedených. Nestanoví-li Smlouva jinak, podléhají jednotliví Poddodavatelé Významného dodavatele předchozímu písemnému schválení ze strany Objednatele. Dodavatel může ke schválení navrhnout nebo do Plnění Smlouvy zapojit pouze takové Poddodavatele, kteří nejsou v rozporu s požadavky Objednatele na Významného dodavatele.
- 14.4. Dodavatel nesmí zapojit k Plnění dle Smlouvy Poddodavatele, bylo-li by tím porušeno opatření obecné povahy vydané ze strany NÚKIB.
- 14.5. Dodavatel je povinen informovat Objednatele předem o zapojení Poddodavatelů a poskytnout mu veškeré potřebné údaje, zejm. identifikační údaje Poddodavatelů, aby Objednatel mohl splnit svoje povinnosti stanovené právními předpisy v souvislosti s prověřováním dodavatelského řetězce, zejm. povinnost zjišťovat a evidovat informace o dodavatelích bezpečnostně významných dodávek a informační povinnost vůči NÚKIB.

15. REALIZAČNÍ TÝM

- 15.1. Pokud je takový požadavek součástí Zadávací dokumentace, je Dodavatel povinen předat Objednateli seznam osob, které budou členy Realizačního týmu, který se bude podílet na Plnění dle Smlouvy. Členy Realizačního týmu lze měnit pouze s předchozím listinným souhlasem Objednatele, který může být dán výlučně za předpokladu, že tyto osoby budou nahrazeny osobami splňujícími kvalifikaci požadovanou ve Veřejné zakázce ve stejném rozsahu jako nahrazované osoby. V případě, že dochází ke změně člena realizačního týmu, který byl v zadávacím řízení hodnocen, je nezbytné, aby takového člena realizačního týmu nahradila osoba, jež by dosáhla v rámci hodnocení stejného či lepšího výsledku než osoba nahrazovaná. Při změně Realizačního týmu není nutné uzavírat listinný dodatek ke Smlouvě a Dodavatel je povinen vypracovat a předat Objednateli v listinné podobě aktualizované znění seznamu členů Realizačního týmu. Tento článek se týká pouze Veřejných zakázek, které požadují provádění Plnění prostřednictvím Realizačního týmu.
- 15.2. Dodavatel se zavazuje provádět Plnění prostřednictvím členů Realizačního týmu uvedených v Příloze Smlouvy *Realizační tým* tak, aby jednotliví členové Realizačního týmu, kteří jsou Kvalifikovanými osobami, prováděli činnosti na pozici dle jejich odbornosti (kvalifikace), které odpovídají tomu, pro jakou pozici prokazovali kvalifikaci v rámci Veřejné zakázky, a v rozsahu, který takové pozici běžně odpovídá.
- 15.3. Každá Kvalifikovaná osoba musí po celou dobu provádění Plnění splňovat kvalifikaci uvedenou v nabídce Dodavatele a zároveň minimální technické kvalifikační předpoklady kladené na pozici, kterou daná osoba zastává dle Zadávací dokumentace.
- 15.4. Nebude-li se Kvalifikovaná osoba řádně podílet na provádění Plnění v rozsahu stanoveném Smlouvou, např. v důsledku ukončení její spolupráce s Dodavatelem nebo její dlouhodobé absence (zejména dlouhodobá nemoc pravděpodobně překračující délku jednoho měsíce), je Dodavatel povinen neprodleně namísto Kvalifikované osoby zahájit provádění Plnění Náhradní Kvalifikovanou osobou a nejpozději do tří (3) Pracovních dnů ode dne, kdy taková situace nastala, informovat Objednatele o této skutečnosti.
- 15.5. Pokud Objednatel nesouhlasí s osobou Náhradní Kvalifikované osoby, je oprávněn žádat Dodavatele o její výměnu za jinou osobu se stejnou kvalifikací navrženou Dodavatelem, čemuž je Dodavatel povinen vyhovět.

16. KOMUNIKACE STRAN

- 16.1. Objednatel a Dodavatel si pro vzájemnou komunikaci ohledně Smlouvy zvolí kontaktní osoby, jejichž seznam uvedou ve Smlouvě.
- 16.2. Jsou-li naplněny podmínky 21.1 ZOP, vykonává kontaktní osoba na straně Dodavatele povinnosti kontaktní osoby pro kybernetickou bezpečnost vyplývající z článku 21. ZOP, nebo je pro plnění takových povinností Dodavatel povinen určit zvláštní kontaktní osobu ve Smlouvě (v takovém případě obě Strany zvolí kontaktní osobu pro kybernetickou bezpečnost, která má na starosti komunikaci týkající se článku 21. ZOP).
- 16.3. Strany si navzájem oznámí jakékoliv změny v kontaktních osobách, přičemž taková změna je účinná uplynutím sedmého (7.) dne po jejím doručení.
- 16.4. Není-li ve Smlouvě výslovně stanovena jiná forma pro doručování dokumentů anebo jiných právních jednání, lze takové dokumenty a jednání doručit v elektronické formě na e-mailovou adresu příslušné kontaktní osoby, prostřednictvím datové zprávy zaslané v rámci ISDS, anebo v listinné podobě.

17. NÁHRADA ŠKODY A SMLUVNÍ POKUTY

- 17.1. Poruší-li Dodavatel některé ze svých povinností stanovených ve Smlouvě či jejích přílohách, zejména pak pokud poruší SLA, resp. stanovený Servisní model dle odst. 12.2 ZOP, je Objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši stanovené v odst. 17.11. ZOP, pokud nejsou ve Smlouvě výslovně zakotveny jiné sankce, které vylučují aplikaci odst. 17.11. ZOP.
- 17.2. Uplatněním smluvní pokuty není dotčeno právo druhé Smluvní strany na náhradu škody v plné výši.
- 17.3. Uplatněním nároku na zaplacení smluvní pokuty ani jejím uhrazením nezaniká povinnost Smluvní strany splnit utvrzenou povinnost.
- 17.4. Dopadají-li na jedno skutkově stejnorodé porušení povinnosti dvě a více ustanovení o smluvní pokutě, uplatní se pouze jedna smluvní pokuta, a to ta, která je v nejvyšší částce. Není vyloučen souběh smluvní pokuty za porušení smluvní povinnosti a smluvní pokuty za prodlení s odstraněním následku téže smluvní povinnosti, jelikož se nejedná o skutkově stejnorodé porušení smluvní povinnosti.
- 17.5. Smluvní pokuty se uplatňují bez DPH. Je-li základem pro výpočet smluvních pokut Cena či její část, je rozhodná Cena či její část bez DPH stanovená k okamžiku uzavření Smlouvy; k případným jejím následným úpravám po uzavření Smlouvy se nepřihlíží.
- 17.6. Smluvní pokuta je splatná do třiceti (30) dnů ode dne vystavení daňového dokladu – sankční faktury. Je-li povinná Smluvní strana v prodlení s uhrazením smluvní pokuty, musí uhradit druhé Smluvní straně zákonný úrok z prodlení z dlužné částky smluvní pokuty za každý započatý den prodlení.
- 17.7. Maximální celková výše všech uplatněných smluvních pokut v důsledku porušení Smlouvy je stanovena ve výši 30 % Ceny.
- 17.8. Dosažení maximální celkové výše veškerých uplatněných smluvních pokut podle předchozího odstavce představuje podstatné porušení Smlouvy, na základě, kterého je Objednatel oprávněn odstoupit od Smlouvy.
- 17.9. Objednatel je ze zákona povinen uplatnit a vymáhat veškeré smluvní pokuty, na které mu vznikl nárok, a to v plné výši bez možnosti její úpravy.
- 17.10. Jsou-li smluvní pokuty stanoveny formou procentního vyjádření vůči Ceně či její části za každý den (či kratší časový úsek) prodlení, platí, že maximální denní výše každé jednotlivé smluvní pokuty činí:
 - a. v případě Ceny do 10 mil. Kč maximálně 10.000 Kč,
 - b. v případě Ceny do 100 mil. Kč maximálně 50.000 Kč
 - c. v případě Ceny do 1 mld. Kč maximálně 100.000 Kč a
 - d. v případě Ceny nad 1 mld. Kč maximálně 200 000 Kč.

17.11. Objednateli vzniká vůči Dodavateli právo na zaplacení smluvní pokuty:

- a. poruší-li Dodavatel svoji povinnost řádně a včas provést Plnění, nebo jeho část (je-li Plnění prováděno po částech) ve výši 0,2 % z Ceny, nebo ceny části Plnění za každý započatý den prodlení až do řádného splnění této povinnosti. Plnění se považuje pro účely této smluvní pokuty za řádně a včas provedené i v případě, že bylo akceptováno s výhradou;
- b. poruší-li Dodavatel svoji povinnost dle odst. 8.1.11 ZOP ve výši 0,2 % z výše zadržené části Ceny dle odst. 8.1.11 ZOP za každý započatý den prodlení až do řádného odstranění poslední vytýkané vady ve smyslu odst. 8.1.11 ZOP ;
- c. poruší-li Dodavatel povinnost udělit nebo zajistit Objednateli ze strany třetí osoby/třetích osob udělovaná oprávnění v rozsahu práv duševního vlastnictví ve výši 5 % z Ceny za každé jednotlivé porušení;
- d. poruší-li Dodavatel povinnost řádně a včas předat Objednateli Zdrojový kód a veškerou související Dokumentaci, ve výši 0,05 % z Ceny za každý započatý den prodlení;
- e. poruší-li Dodavatel některou z povinností týkající se účasti Poddodavatelů anebo Realizačního týmu, ve výši 10 % z Ceny za každé jednotlivé porušení povinnosti;
- f. poruší-li Dodavatel svoji povinnost dodržet sjednanou Dobu vyřešení Incidentu, ve výši:
 - i. 0,01 % z Ceny v případě každé započaté hodiny/den prodlení nad rámec sjednané Doby vyřešení v případě každého Incidentu kategorie A;
 - ii. 0,01 % z Ceny v případě každé započaté hodiny/den prodlení nad rámec sjednané Doby vyřešení v případě každého Incidentu kategorie B;
 - iii. 0,005 % z Ceny v případě každé započaté hodiny/den prodlení nad rámec sjednané Doby vyřešení v případě každého Incidentu kategorie C;
- g. v případě prodlení nad rámec sjednané lhůty pro odstranění vad v Produkčním prostředí:
 - i. Vada kategorie A ve výši 0,01 % z Ceny za každou započatou hodinu/den v případě každé Vady;
 - ii. Vada kategorie B ve výši 0,01 % z Ceny za každou započatou hodinu/den v případě každé Vady;
 - iii. Vada kategorie C ve výši 0,005 % z Ceny za každou započatou hodinu/den v případě každé Vady;
- h. v případě prodlení nad rámec sjednané lhůty pro odstranění vad v Testovacím prostředí:
 - i. Vada kategorie A ve výši 0,05 % z Ceny za každý započatý Pracovní den v případě každé Vady; a
 - ii. Vada kategorie B ve výši 0,01 % z Ceny za každý započatý Pracovní den v případě každé Vady;
- i. V případě, že Dodavatel nedodrží Dostupnost stanovenou Servisním modelem dle odst. 12.2. ZOP, ve výši dle tabulky uvedené níže v závislosti na míře nedodržení požadované Dostupnosti:

Výše poklesu Dostupnosti oproti stanovené Dostupnosti Servisním modelem je	Výše smluvní pokuty
--	---------------------

Do 2 %	10 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle <u>odst. 12.8 ZOP</u>
Od 2 (včetně) do 5 %	15 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle <u>odst. 12.8 ZOP</u>
Od 5 (včetně) do 10 %	25 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle <u>odst. 12.8 ZOP</u>
Od 10 % (včetně) a více	50 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle <u>odst. 12.8 ZOP</u>

- j. v případě prodloužení Dodavatele reagovat na Požadavek Objednatele v době řešení Incidentu uvedeného v odst. 12.2. ZOP ve výši z 0,02 % z Ceny za každý jednotlivý případ;
- k. ve výši a za podmínek dle článku 21. ZOP v oblasti kybernetické bezpečnosti;
- l. ve výši a za podmínek dle článku 22. ZOP v oblasti ochrany osobních údajů;
- m. ve výši a za podmínek dle článku 23. ZOP v oblasti ochrany Důvěrných informací; nebo
- n. poruší-li Dodavatel svoji povinnost dle odst. 14.2. ZOP nebo 14.3. ZOP, ve výši 2 % z Ceny za každé jednotlivé porušení.

17.12. Pro smluvní pokuty stanovené v odst. 17.11. písm. 17.11.f. a 17.11.g. ZOP platí, že je-li lhůta pro splnění stanovena v hodinách, je smluvní pokuta počítána za každou započatou hodinu, je-li lhůta pro splnění stanovena ve dnech či Pracovních dnech, je smluvní pokuta počítána za každý započatý den.

17.13. Objednatel je oprávněn započít nárok na zaplacení smluvní pokuty, i pokud ještě není splatný, proti jakémukoliv nároku Dodavatele na peněžité plnění vyplývajícímu ze Smlouvy.

17.14. Za každý den prodloužení s úhradou Smluvní pokuty je Objednatel oprávněn požadovat po Dodavateli úhradu úroků z prodloužení ve výši stanovené obecně závaznými právními předpisy.

18. ZÁRUKA ZA JAKOST A PRÁVA Z VADNÉHO PLNĚNÍ

18.1. Společná ustanovení

- 18.1.1. Dodavatel uděluje Objednateli záruku za jakost Plnění a všech jeho částí na dobu dvou (2) let ode dne akceptace výstupu Plnění.
- 18.1.2. Objednatel je oprávněn Vady, které se vyskytnou v průběhu záruční doby, nahlásit Dodavateli bez zbytečného odkladu od okamžiku, kdy je zjistil. Lhůta bez zbytečného odkladu činí vždy nejméně devadesát (90) dnů.
- 18.1.3. Dodavatel odpovídá za vady zjevné, skryté i právní, které měl výstup provádění Plnění v době akceptace Objednatelem, a dále za ty, které se na něm vyskytnou v záruční době, a zavazuje se, vedle dalších nároků Objednatele, je bezplatně odstranit.
- 18.1.4. Dodavatel neodpovídá za vady, pokud byly způsobeny zásahem do takových výstupů Plnění ze strany Objednatele nebo jím pověřené osoby, případně jiných dodavatelů Objednatele.
- 18.1.5. Objednatel je povinen oznámit vady Plnění Dodavateli prostřednictvím Servicedesku, nebude-li Stranami dohodnuto jinak.
- 18.1.6. Dodavatel neodpovídá za vady Plnění vzniklé:
 - a. provozováním Díla Objednatelem v rozporu s Dokumentací;

- b. neoprávněným nebo neodborným zásahem či nesprávným užitím Díla Objednatel;
 - c. vadami IT prostředí Objednatele.

18.2. Záruka vztahující se k Softwaru

- 18.2.1. Pokud výrobce Standardního Software poskytuje záruku za jakost, pak Dodavatel postupuje takovou záruku za jakost Objednateli. To nezabavuje Dodavatele povinnosti poskytnout Objednateli vlastní záruku za jakost ve smyslu tohoto článku.
- 18.2.2. V době trvání záruční doby je Dodavatel povinen odstraňovat vady ve lhůtách uvedených v tabulce níže. Lhůty stanovené v hodinách běží pouze v Pracovní dny osm (8) hodin denně v době od 9:00 do 17:00 hodin (režim 5x8). Lhůty stanovené v hodinách se mimo dobu uvedenou v předchozí větě staví a pokračují dále v běhu během další bezprostředně následující doby počítání. Strany pro zamezení pochybnostem prohlašují, že toto se netýká lhůt stanovených v Pracovních dnech ani počítání doby prodlení v rámci výpočtu smluvních pokut.

Produkční prostředí

Kategorie vady	Lhůta k odstranění počítaná od nahlášení vady Objednatel
Vada kategorie A – kritická	do 4 hodin ¹
Vada kategorie B – střední	do 17:00 hod. třetího Pracovního dne od nahlášení vady ²
Vada kategorie C – nízká	do 17:00 hod. pátého Pracovního dne od nahlášení vady ³

Testovací prostředí

Kategorie vady	Lhůta k odstranění počítaná od nahlášení vady Objednatel
Vada kategorie A – kritická	do 17:00 hod. druhého Pracovního dne od nahlášení vady ⁴
Vada kategorie B – střední	do 17:00 hod. pátého Pracovního dne od nahlášení vady ⁵
Vada kategorie C – nízká	do 17:00 hod. desátého Pracovního dne od nahlášení vady ⁶

18.3. Záruka vztahující se k Hardwaru

- 18.3.1. Poskytuje-li výrobce anebo Dodavatel kterékoliv části Hardwaru na své výrobky anebo služby záruku za jakost delší, než je záruka za jakost dle tohoto článku, zavazuje se Dodavatel udělit Objednateli nebo na Objednatele postoupit danou záruku za jakost tak, aby Objednatel byl oprávněn po skončení záruky za jakost uplatnit nároky ze záruky za jakost bez nutnosti součinnosti ze strany Dodavatele.
- 18.3.2. Zjevné vady Hardware a dalších hmotných věcí je Objednatel povinen u Dodavatele reklamovat v rámci Akceptačního řízení. V případě, že Objednatel zjistí vady hmotných věcí po akceptaci, je povinen tyto vady bez zbytečného odkladu reklamovat u Dodavatele.
- 18.3.3. V případě, že odstranění reklamovaných vad bude trvat déle než dva (2) Pracovní dny, zavazuje se Dodavatel poskytnout Objednateli náhradní Hardware či jinou náhradní

¹ Lhůta je stanovena v hodinách.

² Lhůta je stanovena ve dnech.

³ Lhůta je stanovena ve dnech.

⁴ Lhůta je stanovena v hodinách.

⁵ Lhůta je stanovena ve dnech.

⁶ Lhůta je stanovena ve dnech.

hmotnou věc po dobu trvání odstranění reklamované vady, nedohodnou-li se Strany jinak.

19. UKONČENÍ SMLUVNÍHO VZTAHU

19.1. Obecně k odstoupení od Smlouvy:

- a. Strany sjednávají, že vznikne-li Objednateli nárok na odstoupení od Smlouvy, může podle své volby odstoupit od Smlouvy v celém rozsahu či jen od některé části Plnění určené Objednatelem.
- b. Strany se dohodly na vyloučení použití § 1978 odst. 2 Občanského zákoníku, který stanoví, že marné uplynutí dodatečné lhůty stanovené k plnění může mít za následek odstoupení od této Smlouvy bez dalšího.
- c. Dodavatel nemá právo odstoupit od Smlouvy v případě nevhodných příkazů Objednatele či poskytnutí nevhodné věci Objednatelem dle § 2595 Občanského zákoníku.

19.2. Objednatel je oprávněn odstoupit od Smlouvy, v případě, že:

- a. Dodavatel je v prodlení s plněním dle Smlouvy či jakékoliv části Plnění déle než 30 dnů a nezjedná nápravu ani do 15 dnů od doručení písemného oznámení Objednatele o takovém prodlení.
- b. Dodavatel je v prodlení s Plněním dle Smlouvy déle než 60 dnů, a to i bez nutnosti zaslání předchozího upozornění.
- c. Nastane některý ze zákonem stanovených případů a zejména v případech podstatného porušení povinností Dodavatele stanovených ve Smlouvě. Za podstatné porušení povinností Dodavatele se považuje zejména:
 - i. Dodavatel je opakovaně v prodlení s prováděním Plnění dle Smlouvy;
 - ii. prohlášení Dodavatele učiněné na základě Smlouvy se ukáže jako nepravdivé;
 - iii. Dodavatel bez upozornění a relevantního odůvodnění nepoužil k Plnění člena Realizačního týmu, ač k tomu byl povinen; nebo
 - iv. Dodavatel poruší některou z povinností uvedenou v čl. 21. ZOP opakovaně nebo závažným způsobem.
- d. Dodavatel poruší kteroukoliv svoji povinnost dle Smlouvy jiným než podstatným způsobem a ve lhůtě 15 dnů od doručení písemného oznámení Objednatele toto své porušení nenapraví.
- e. Dodavatel poruší svou povinnost dle odst. 14.2. ZOP nebo odst. 14.3. ZOP nebo Poddodavatel Dodavatele poruší některou z povinností vyplývajících z požadavků dle odst. 14.2. ZOP.
- f. Dodavatel podá insolvenční návrh jako dlužník ve smyslu § 98 Insolvenčního zákona nebo insolvenční soud nerozhodne o insolvenčním návrhu na Dodavatele do šesti (6) měsíců od zahájení insolvenčního řízení, nebo insolvenční soud vydá rozhodnutí o úpadku Dodavatele ve smyslu § 136 Insolvenčního zákona.
- g. Je přijato rozhodnutí o povinném nebo dobrovolném zrušení Dodavatele (vyjma případů sloučení nebo splnutí).
- h. Okolnost vylučující povinnost k náhradě Újmy kterékoli ze Stran trvá déle než 30 dnů;
- i. dojde k Významné změně dle odst. 4.2. ZOP.
- j. Dojde k Významné změně kontroly nad Dodavatelem nebo změny kontroly nad zásadními aktivy využívanými Dodavatelem k plnění Smlouvy, přičemž kontrolou se zde rozumí vliv, ovládání či řízení dle ust. § 71 a násl. ZOK, či ekvivalentní postavení.

- k. Dojde k Významné změně ovlivnění nebo ovládání Dodavatele podle ust. § 71 a násl. ZOK nebo změně vlastnictví zásadních aktiv, využívaných Dodavatelem k plnění Smlouvy a změně oprávnění nakládat s těmito aktivy, či dojde ke změně ekvivalentní těmto změnám a tato změna bude Objednatelem vyhodnocena jako riziko bezpečnosti informací, které nelze odstranit jiným opatřením; toto ustanovení se uplatní i pro případ, že Dodavatel o takových změnách dopředu a včas neinformuje Objednatele.
- 19.3. Dodavatel je oprávněn odstoupit od Smlouvy pouze v případech jejího podstatného porušení, jestliže:
- a. Objednatel nezaplatil jakoukoli dlužnou částku za Plnění dle Smlouvy řádně a včas a toto porušení nenapravit ani do 60 dnů ode dne obdržení písemné výzvy k nápravě; nebo
 - b. Objednatel poruší jinou povinnost dle Smlouvy podstatným způsobem a ve lhůtě 60 dnů ode dne obdržení písemné výzvy k nápravě toto své porušení nenapravit.
- 19.4. Dodavatel není oprávněn odstoupit od Smlouvy ve vztahu k části Plnění, za kterou mu již bylo Objednatelem zapláceno.
- 19.4.1. Objednatel je oprávněn Smlouvu vypovědět bez výpovědní doby, nelze-li v jejím plnění pokračovat, aniž by bylo porušeno opatření obecné povahy vydané ze strany NÚKIB.

20. ZMĚNY SMLOUVY A ZMĚNOVÉ ŘÍZENÍ

- 20.1. Není-li ve Smlouvě nebo jejích Přílohách stanoveno jinak, může být Smlouva měněna nebo zrušena pouze v listinné podobě, a to v případě změn Smlouvy číslovanými dodatky, který musí být podepsány oběma Stranami a uzavřeny v souladu se ZZVZ.
- 20.2. Pokud je ve Smlouvě upraveno Opční právo, vyhrazuje si Objednatel v souladu s ustanovením § 100 odst. 3 ZZVZ vyhrazenou změnu závazku z této Smlouvy spočívající v pořízení dalšího obdobného Plnění od vybraného účastníka v rámci zadávacího řízení Veřejné zakázky, tj. od Dodavatele dle Smlouvy. Předmětem plnění Opčního práva je poskytnutí dalšího obdobného Plnění dle Smlouvy tak, jak bylo podrobně vymezeno včetně dalších zákonných náležitostí vyhrazené změny závazku dle § 100 odst. 3 ZZVZ v Zadávací dokumentaci předmětné Veřejné zakázky.
- 20.3. Objednatel je oprávněn do uplynutí tří (3) let od nabytí účinnosti Smlouvy kdykoliv uplatnit toto Opční právo, a to i opakovaně do vyčerpání limitů Opčního práva definovaných v Zadávací dokumentaci. Vyhrazená změna závazku ze Smlouvy bude Stranami projednána v rámci jednacího řízení bez uveřejnění dle § 66 ZZVZ, které bude zahájeno Objednatelem v souladu s tímto ustanovením, a jehož výsledkem bude uzavření listinného dodatku k této Smlouvě či uzavření nové smlouvy mezi Objednatelem nebo Dodavatelem.

21. KYBERNETICKÁ BEZPEČNOST

- 21.1. Tento článek se uplatní v případě, kdy je Smlouva uzavřena s Významným dodavatelem, pokud je Dodavatel Dodavatelem Strategicky významné služby, jakož i v dalších případech, kdy tak výslovně stanoví Smlouva.
- 21.2. Zda je Dodavatel Významným dodavatelem, stanoví Smlouva. Pokud se Dodavatel stane Významným dodavatelem v průběhu plnění Smlouvy, bude o této skutečnosti Objednatelem neprodleně informován a povinnosti dle čl. 21. se na něj uplatní v rozsahu v jakém to po něm lze spravedlivě požadovat.
- 21.3. Zda je Dodavatel Dodavatelem Strategicky významné služby, stanoví Smlouva. Pokud se Dodavatel stane Dodavatelem Strategicky významné služby v průběhu plnění Smlouvy, bude o této skutečnosti Objednatelem neprodleně informován a čl. 21. se na něj uplatní v rozsahu, v jakém to po něm lze spravedlivě požadovat.
- 21.4. Dodavatel se při plnění Smlouvy zavazuje postupovat v souladu se ZoKB, VoKB a souvisejícími právními předpisy, příp. vč. právních předpisů tyto předpisy provádějící, upravující či nahrazující, dodržovat zásady bezpečnosti informací, Interní předpisy Objednatele a z nich vyplývající povinnosti týkající se bezpečnostních opatření, provozní řády prostor Objednatele, rozhodnutí, protioopatření, opatření obecné povahy, či jiný správní akt NÚKIB či jiného správního orgánu anebo

závazné podmínky pro Objednatele stanovené orgánem veřejné moci ukládající Objednateli další povinnosti ve smyslu ZoKB a VoKB, včetně upozorňování a zajištění hlášení Kybernetických bezpečnostních incidentů Objednateli, jakož i další bezpečnostní politiky, metodiky a postupy, se kterými byl Objednatelem seznámen.

- 21.5. Dodavatel je povinen seznámit se s bezpečnostními požadavky Objednatele uvedenými ve Smlouvě, jejích přílohách, těchto ZOP, Interních předpisech Objednatele a seznámit s nimi osoby podílející se na plnění Smlouvy dle potřeby s ohledem na charakter jejich plnění s přihlédnutím k zajištění bezpečnosti informací. Pokud je to potřebné, je Dodavatel povinen provést školení bezpečnostních požadavků dle tohoto odstavce a dále je provádět v pravidelných intervalech, nejméně 1x ročně. Dodavatel je také povinen aktivně vynucovat dodržování takových bezpečnostních požadavků dotčenými osobami na straně Dodavatele. Za porušení těchto pravidel osobami uvedenými v tomto odstavci odpovídá Dodavatel tak, jako by je porušil sám.
- 21.6. Není-li ve Smlouvě ujednáno jinak, je Dodavatel povinen vytvořit, pravidelně aktualizovat a vynucovat vůči osobám podílejícím se, byť i nepřímo, na Předmětu Smlouvy:
 - 21.6.1. politiku řízení přístupu, na základě které, není-li ve Smlouvě ujednáno jinak, je Dodavatel dále povinen průběžně monitorovat a zaznamenávat přístupy všech osob účastnících se na Plnění dle Smlouvy, a to v rozsahu, aby bylo možné jednoznačně určit uživatele, čas a provedenou činnost, jakož i vyhodnocovat oprávněnost těchto přístupů (logování přístupů) a tuto svou povinnost v politice řízení přístupu zohlednit a Dodavatel musí umožnit a poskytnout součinnost na jejich integraci do systému bezpečnostního monitoringu (SIEM), systému pro správu logů a centrální úložiště logů Objednatele;
 - 21.6.2. politiku zvládnání Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů obsahující činnosti, role, odpovědnosti a pravomoci k rychlému a účinnému zvládnání Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů.
- 21.7. Nestanoví-li Smlouva jinak, Plnění musí využívat nástroj Objednatele pro centrální správu přístupových účtů, který zajišťuje přidělení oprávnění k výkonu činností jednotlivým rolím jednoznačně identifikovaných fyzických osob, které se podílejí na plnění Smlouvy, a to v nejmenším možném a nutném rozsahu tak, aby měly přístup k aktivům Objednatele pouze ty osoby, které takový přístup skutečně potřebují k výkonu činností týkajících se předmětu Plnění dle Smlouvy.
- 21.8. Dodavatel je povinen při nakládání s veškerými aktivy (dotčenými aktivy Dodavatele a Objednatele) postupovat tak, aby chránil jejich důvěrnost, dostupnost a integritu a zavést přiměřená opatření na jejich ochranu.
- 21.9. Dodavatel je povinen řídit rizika spojená s Plněním dle Smlouvy minimálně dle standardů požadovaných ZoKB pro regulované služby v režimu vyšších povinností a případně dle Interních předpisů, pokud obsahují závazná pravidla pro řízení rizik.
- 21.10. Dodavatel je povinen, na vyžádání, v pravidelných minimálně ročních intervalech předkládat Zprávu o přezkoumání stavu ISMS k relevantním aktivům související s Plněním.
- 21.11. Dodavatel je povinen zaslat některým z níže uvedených způsobů hlášení o událostech, které mají charakter Kybernetického bezpečnostního incidentu, včetně případů porušení zabezpečení Osobních údajů, vždy bez zbytečného odkladu, nejpozději však do tří (3) hodin po jejich zjištění, a sdělit Objednateli opatření, která již provedl ve vztahu k tomuto Kybernetickému bezpečnostnímu incidentu, případně zvolí jinou formu dohodnutou mezi Objednatelem a Dodavatelem určenou ke včasnému hlášení Kybernetického bezpečnostního incidentu a/nebo již učiněných opatření. Dodavatel je povinen veškeré Kybernetické bezpečnostní incidenty zaznamenávat a po nezbytně dlouhou dobu uchovávat. Dodavatel je povinen bez zbytečného odkladu poskytnout Objednateli veškerou nezbytnou součinnost k detekci, vyhodnocení či řešení Kybernetického bezpečnostního incidentu, a to včetně případné realizace nutných opatření dle pokynů Objednatele, a dále k tomu, aby Objednatel mohl ve lhůtě dle ZoKB předložit NÚKIB tzv. prvotní hlášení. Zapříčinil-li Dodavatel Kybernetický bezpečnostní incident nebo podílel-li se na jeho vzniku, provede analýzu příčin Kybernetického bezpečnostního incidentu a navrhne opatření za účelem zamezení jeho opakování v budoucnu. Dodavatel je povinen ohlásit každou událost,

kteřá má charakter Kybernetického bezpečnostního incidentu, včetně případů porušení zabezpečení osobních údajů, jedním z následujících způsobů:

- a. e-mailem nebo telefonicky Dohledovému centru kybernetické bezpečnosti SŽ (viz odst. 1.15 ZOP); nebo
 - b. ohlášením do Servicedesku Objednatele.
- 21.12. Dodavatel je povinen bez zbytečného odkladu informovat Objednatele o každém Kybernetickém bezpečnostním incidentu s významným dopadem, který může negativně ovlivnit poskytování služby nebo aktiva Objednatele, a poskytnout mu veškeré informace nezbytné k tomu, aby Objednatel mohl splnit povinnosti podle § 19 ZoKB. Dodavatel je dále povinen řídit se pokyny Objednatele týkajícími se rozsahu a obsahu poskytovaných informací, zejména v případech, kdy NÚKIB uloží Objednateli povinnost nebo zákaz informovat uživatele regulované služby.
- 21.13. Bude-li se jednat o Kybernetický bezpečnostní incident s významným dopadem ve smyslu § 16 odst. 3 ZoKB, zavazuje se dále Dodavatel poskytnout Objednateli veškerou potřebnou součinnost, aby Objednatel mohl předložit příslušným orgánům:
- a. oznámení, v němž aktualizuje informace z prvotního hlášení, předloží prvotní posouzení Kybernetického bezpečnostního incidentu a uvede dopad a indikátory kompromitace, pokud jsou k dispozici, přičemž tuto součinnost Dodavatel poskytne bez zbytečného odkladu, nejpozději však do 48 hodin po zjištění Kybernetického bezpečnostního incidentu;
 - b. na výzvu NÚKIB nebo Národního CERT průběžnou zprávu o podstatných změnách stavu zvládání Kybernetického bezpečnostního incidentu, a
 - c. závěrečnou zprávu o vyřešení Kybernetického bezpečnostního incidentu, přičemž tuto součinnost Dodavatel poskytne bez zbytečného odkladu, nejpozději však do 25 dnů ode dne předložení oznámení podle písmene a); nebo aby, v případě, že i po uplynutí 30 dnů ode dne předložení oznámení podle písmene a) Kybernetický bezpečnostní incident stále trvá, mohl Objednatel předložit bez zbytečného odkladu průběžnou zprávu o aktuálním stavu zvládání Kybernetického bezpečnostního incidentu, a poté nejpozději do 30 dnů ode dne, kdy došlo k vyřešení Kybernetického bezpečnostního incidentu, závěrečnou zprávu o vyřešení Kybernetického bezpečnostního incidentu.
- 21.14. Dodavatel je povinen pravidelně alespoň jednou ročně Objednateli zprávu o počtu a druhu útoků a Kybernetických bezpečnostních incidentů, které zaznamenal ve spojení s Plněním a/nebo Předmětem Smlouvy.
- 21.15. Dodavatel se zavazuje poskytnout Objednateli veškerou součinnost nezbytnou k tomu, aby Objednatel řádně naplňoval právní povinnosti stanovené ZoKB, VoKB a dalšími souvisejícími právními předpisy a normami. Zejména se Dodavatel zavazuje poskytnout Objednateli součinnost směřující k zavedení a provádění bezpečnostních protopatření podle ZoKB, VoKB a Kybernetických bezpečnostních incidentů.
- 21.16. Pokud Dodavatel při plnění Smlouvy zjistí či jako odborník mohl a měl zjistit rozpor ustanovení Interních předpisů se ZoKB, VoKB anebo rozhodnutím či jiným pokynem NÚKIB, je povinen takový rozpor Objednateli neprodleně ohlásit a poskytnout Objednateli součinnost k jeho odstranění.
- 21.17. Dodavatel je povinen udržovat a pravidelně aktualizovat vlastní plán kontinuity činností (BCP) a plán obnovy po havárii (DRP), které pokrývají služby, aktiva a procesy poskytované v souladu se Smlouvou. Na žádost Objednatele je Dodavatel povinen poskytnout k nahlédnutí relevantní části těchto plánů.
- 21.18. Dodavatel se zavazuje provádět pravidelné testování BCP/DRP nejméně jednou za dva roky, o provedeném testování vést záznamy a na žádost objednatel poskytnout souhrnnou zprávu o výsledcích testů, zjištěných nedostatcích a přijatých nápravných opatřeních.
- 21.19. V případě, že dojde k jakémukoliv rozporu mezi Dodavatelem a třetí osobou, která není jeho Poddodavatelem a je dodavatelem Softwaru nebo jiných technologií dotčených plněním povinností Dodavatele dle této Smlouvy, je Dodavatel povinen tuto skutečnost bez zbytečného odkladu oznámit Objednateli. Dodavatel je dále povinen poskytovat Objednateli nutnou součinnost pro

jednání s těmito třetími osobami a sám se těchto jednání účastnit, nebo na základě žádosti Objednatele jednat s těmito třetími osobami napřímo.

- 21.20. Objednatel má právo v souladu s ustanoveními § 2593 Občanského zákoníku prostřednictvím určených osob kdykoli kontrolovat plnění Smlouvy u Dodavatele a jeho případných Poddodavatelů, a to i prostřednictvím třetí osoby; předchozí věta se uplatní obdobně v případě kontroly některé ze Stran ze strany kontrolního orgánu ve smyslu zákona č. 255/2012 Sb., kontrolní řád, ve znění pozdějších předpisů.
- 21.21. Objednatel má právo prostřednictvím určených osob provádět v pravidelných intervalech (1x za dva roky, není-li ve Smlouvě ujednáno jinak), jakož i v případě důvodného podezření na závažné porušení povinností Dodavatele dle těchto ZOP, v případě Kybernetických bezpečnostních incidentů a/nebo v jiných případech vyžadovaných ZoKB a/nebo VoKB, audit kybernetické bezpečnosti, tj. dodržování bezpečnosti informací dle Interních předpisů, ZoKB a VoKB u Dodavatele a jeho případných Poddodavatelů, a to i prostřednictvím třetí osoby. V rámci auditu kybernetické bezpečnosti je Objednatel oprávněn zejména porovnávat zjištěné skutečnosti s bezpečnostní dokumentací Objednatele a nad rámec obvyklý u auditu kybernetické bezpečnosti dále provádět následující činnosti:
- 21.21.1. pravidelné konzultace, jimž bude předcházet minimálně týdenní ohlašovací povinnost (e-mail, telefonní kontakt). Tyto konzultace nebudou častější než jednou za tři měsíce;
 - 21.21.2. nehlášený telefonát od Kontaktní osoby Objednatele s členem Realizačního týmu, který má přístup do Informačního či komunikačního systému, zahrnující konkrétní dotazy na zabezpečení a jiné aspekty informační bezpečnosti dotčeného Informačního či komunikačního systému.
 - 21.21.3. Dodavatel je povinen umožnit Objednateli provedení kontroly a auditu kybernetické bezpečnosti a zajistit (i smluvně) právo na provedení této kontroly a auditu kybernetické bezpečnosti u svých případných Poddodavatelů, jakož i veškerou další součinnost nezbytnou pro provedení auditu. Kontrolu a audit kybernetické bezpečnosti může rovněž provést i třetí osoba pověřená Objednatelem. Průběh takového auditu je doložen např. auditní zprávou či jiným obdobným dokumentem. Případné náklady na straně Dodavatele na provedení auditu jsou součástí Ceny za Plnění dle Smlouvy. Dodavatel je oprávněn rozporovat výsledky auditu kybernetické bezpečnosti do 7 Pracovních dnů od oznámení výsledku auditu kybernetické bezpečnosti. Dodavatel může rozporovat a) existenci vyčteného porušení či hrozby; b) že porušení či hrozba byla Dodavatelem již odstraněna. V obou případech uvede skutečnosti a důkazy k podpoře svých tvrzení. Objednatel je v takovém případě povinen takové připomínky vypořádat. V případě, že Objednatel na svém zjištění setrvá, je Dodavatel povinen se tímto auditem řídit.
 - 21.21.4. Pokud audit kybernetické bezpečnosti odhalí jakékoliv podstatné porušení či hrozbu takového porušení, je Dodavatel povinen napravit nedostatky vč. přijetí případných dalších bezpečnostních opatření a o tomto informovat Objednatele, pokud se jedná o Významného dodavatele, je povinen napravit nedostatky bezodkladně a informovat Objednatele nejpozději do 7 dnů.
- 21.22. Je-li součástí Plnění přenos Dat a informací, je Dodavatel povinen jej za součinnosti oprávněných osob na straně Objednatele zabezpečit odolnými kryptografickými algoritmy v souladu s aktuálními doporučeními a metodikami NÚKIB a požadavky příslušných právních předpisů, zejména VoKB. Dodavatel je povinen zejména:
- 21.22.1. používat pouze aktuálně odolné kryptografické algoritmy, klíče a certifikáty,
 - 21.22.2. zajistit bezpečnou komunikaci všech forem datového přenosu souvisejícího s Plněním,
 - 21.22.3. bezpečně nakládat s kryptografickými algoritmy, jejich implementacemi a parametry,
 - 21.22.4. používat nástroje pro bezpečnou správu kryptografických klíčů a certifikátů,
 - 21.22.5. zajistit možnost kontroly a auditu nakládání s kryptografickými klíči,
 - 21.22.6. zajistit důvěrnost a integritu kryptografických klíčů a souvisejících procesů,

- 21.22.7. bezodkladně provést potřebné změny, pokud NÚKIB nebo jiný orgán upozorní na zranitelnost či nedostatečnou odolnost používaných kryptografických prostředků.
- 21.23. Je-li součástí Předmětu Plnění správa síťové infrastruktury a/nebo jejích prvků (aktivních či pasivních), je Dodavatel povinen za součinnosti oprávněných osob na straně Objednatele:
- 21.23.1. provádět analýzy topologie sítě či skenování aktivních částí Předmětu Plnění; a
- 21.23.2. realizovat bezpečnostní opatření pro odstranění nebo blokování síťových spojení, která neodpovídají požadavkům na ochranu integrity komunikační sítě.
- 21.24. Dodavatel je dále povinen:
- 21.24.1. provádět pravidelné zálohy dat, konfigurací a nastavení technických aktiv vztahujících se k Plnění dle Smlouvy, zabezpečit je vhodnými prostředky proti neoprávněným přístupům, ztrátě nebo narušení integrity, a to včetně šifrování záloh v souladu s požadavky VoKB. Dodavatel je povinen: provádět testování integrity, dostupnosti a obnovitelnosti záloh nejméně jedenkrát za měsíc, dokumentovat výsledky těchto testů a uchovávat je po dobu trvání Smlouvy, oddělit zálohovací prostředí od produkčního prostředí, zajistit bezpečnou správu konfigurací a nastavení technických aktiv;
- 21.24.2. zajistit, aby dodávaná aplikace, je-li součástí Plnění, poskytovala auditní záznamy (logy) o činnostech v ní provedených, v rozsahu stanoveném VoKB, které umožní jednoznačně určit uživatele, čas a provedenou činnost, a aby tyto záznamy byly uchovávány po dobu stanovenou právními předpisy a Interními předpisy Objednatele. Dodavatel je povinen umožnit jejich integraci do systému bezpečnostního monitoringu Objednatele, pokud to Objednatel vyžaduje.
- 21.25. Pokud Objednatel zjistí, že Dodavatel postupuje v rozporu s tímto článkem 21 ZOP, je Objednatel v takovém případě oprávněn dožadovat se toho, aby Dodavatel odstranil vady vzniklé vadným postupem Dodavatele, zdržel se provádění postupů, které jsou v rozporu s tímto článkem, nebo konal, jak je od něj vyžadováno tímto článkem, a dále Smlouvu plnil řádným způsobem. Strany se dohodnou na podmínkách a lhůtě k odstranění nedostatků plnění Smlouvy ve smyslu tohoto odstavce, přičemž nedohodnou-li se Strany na konkrétní lhůtě, pak je Dodavatel povinen odstranit nedostatky do třiceti (30) dnů. V případě, že Dodavatel postupuje v rozporu s tímto článkem 21 ZOP, jakož i v případech, kdy Dodavatel včas neodstraní nedostatky ve smyslu předchozí věty tohoto odstavce, je Objednatel oprávněn od Smlouvy odstoupit.
- 21.26. Kontaktní osoby Stran vzájemně komunikují v průběhu plnění Smlouvy za účelem dosažení standardů pro bezpečnost informací. V případě ohrožení anebo porušení bezpečnosti informací, zejména v případě výskytu Kybernetického bezpečnostního incidentu, jsou kontaktní osoby povinny vzájemně komunikovat, ihned po zjištění takových skutečností hlásit jejich výskyt druhé Straně a společně podnikat kroky k zajištění obnovení bezpečnosti informací.
- 21.27. Objednatel si vyhrazuje možnost provedení pravidelného penetračního testování nebo testování zranitelností v průběhu trvání Smlouvy.
- 21.27.1. Dodavatel je povinen neprodleně přijmout dodatečná, účinná nápravná opatření k odstranění kritických zranitelností, které byly zjištěny v průběhu penetračního testování aplikace (a to na úrovni hardwaru i softwaru).
- 21.27.2. Pro odstranění případných pochybností, penetračním testováním je myšleno jakékoliv zkoumání informačního/počítačového systému s cílem najít slabá místa (zranitelnosti) Plnění. S výsledky penetračního testování mohou být seznámeny výhradně pověřené osoby Dodavatele a Objednatele.
- 21.27.3. Při realizaci penetračního testování nebo testování zranitelností řešení, poskytne Dodavatel Objednateli veškerou potřebnou součinnost.
- 21.27.4. V případě, že výsledkem penetračního testování nebo testování zranitelností jsou kritická zjištění zranitelností, je Dodavatel povinen neprodleně přijmout dodatečná, účinná nápravná opatření k odstranění těchto zranitelností.
- 21.27.5. V případě, že opakované penetrační testování, i přes ujištění Dodavatele o přijetí nápravných opatření k odstranění zranitelností, bude obsahovat totožné zranitelnosti, bude se Dodavatel podílet na finančních nákladech testování.

21.28. Dodavateli nenáleží za plnění povinností souvisejících s bezpečností informací ve smyslu článku 21. ZOP jakákoliv další odměna, resp. taková odměna je součástí Ceny.

21.29. Významný dodavatel

21.29.1. Je-li Dodavatel identifikován jako Významný dodavatel, je dále nad rámec povinností uvedených v odst. 21.1 až 21.28 ZOP povinen:

- a. průběžně detekovat známé zranitelnosti dotčených aktiv Objednatele a bezodkladně na ně upozorňovat Objednatele;
- b. umožnit přístup k auditním údajům aplikace Objednatele, a to v takové podobě, která je v souladu zejména s CEF, CEE či LEEF / Windows event log formát/databázové VIEW tak, aby je bylo možné strojově zpracovávat pomocí nástroje SIEM Objednatele;
- c. na vyžádání Objednatele předat veškerá Data, provozní údaje a informace v otevřeném nebo standardizovaném formátu dostupném bez nutnosti pořízení proprietárního softwaru (zejména ve formátech CSV, XML, JSON, PDF/A, XLSX nebo jiném standardizovaném formátu příslušného prostředí), který umožňuje jejich okamžité využití v prostředí Objednatele „as is“. Dodavatel je povinen předat tato Data spolu s nezbytnými metadaty, popisy datových struktur, technickou dokumentací a informacemi o integračních rozhraních, aby byla Data plně čitelná, interpretovatelná a použitelná bez závislosti na Dodavateli. Dodavatel zajistí, aby tyto podmínky předání Dat splňovaly požadavky VoKB na specifikaci podmínek pro formát předání dat a informací po vyžádání povinnou osobou.
- d. poskytnout potřebnou součinnost na integraci auditních záznamů do systému bezpečnostního monitoringu (SIEM), systému pro správu logů a do centrálního úložiště logů Objednatele;
- e. zajistit, aby Plnění využívalo procesy pro ověřování identity uživatelů a administrátorů, které jsou založeny na autentizačním mechanismu využívajícím multifaktorovou autentizaci (MFA) s nejméně dvěma různými typy faktorů. Procesy pro využívání identity uživatelů musí být kompatibilní se systémem řízení identit Objednatele;
- f. poskytnout potřebnou součinnost na integraci procesů pro ověřování identity do systému řízení identit Objednatele;
- g. zajistit, aby zaměstnanci Dodavatele s administrátorskými oprávněním využívali k přístupu do Kybernetického prostoru SŽ, výhradně bezpečný přístup založený na řešení PAM (Privileged Access Management);
- h. poskytnout Objednateli veškeré potřebné informace a součinnost v procesu řízení a změn a jeho dokumentace v souladu s § 11 VoKB dle potřeb Objednatele (zejm. při posouzení, zda je změna Významnou změnou, analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní a provozní dokumentace, souvisejícím testováním, zajištění možnosti navrácení do původního stavu a provedení dalších činností dle VoKB), a současně zajistit, aby veškeré navrhované změny byly posuzovány, řízeny a dokumentovány v souladu s požadavky VoKB, zejména pravidly systému řízení bezpečnosti informací, řízení rizik, prováděním bezpečnostních opatření, vedením evidence změn, záznamů o testování a ověřování, kontrolou účinnosti přijatých opatření a pravidelnou aktualizací související dokumentace;
- i. bezodkladně odstranit všechny relevantní zranitelnosti, které se vztahují k aplikaci a které mají hodnocení zranitelností založené na systému CVSS (Common Vulnerability Scoring System) vyšší než 8.0, a to včetně 8.0, který je zobrazován pomocí standardu CVE (Common Vulnerabilities and Exposures);
- j. zpracovat a pravidelně aktualizovat bezpečnostní a provozní dokumentaci v rozsahu stanoveném ve Smlouvě;

- k. neprovést žádnou Významnou změnu bez předchozího písemného schválení Objednatele. Dodavatel je dále povinen informovat Objednatele o každé změně, která může mít dopad na kybernetickou bezpečnost, před jejím provedením, a poskytnout podklady pro posouzení dopadů a hodnocení rizik;
 - l. průběžně detekovat známé zranitelnosti dotčených aktiv Objednatele a bezodkladně na ně upozorňovat Objednatele;
 - m. vést v elektronické formě provozní deník obsahující veškeré podstatné okolnosti související s plněním povinností Dodavatele ZOP a/nebo Plněním, provozní události důležitých aktiv a zpřístupnit jej Objednateli prostřednictvím zabezpečeného vzdáleného přístupu, není-li ve Smlouvě ujednáno jiný způsob;
 - n. na vyžádání předložit Objednateli provozní deník a výstup z monitoringu dostupnosti, důvěrnosti a integrity aktiv Objednatele, se kterými pracuje v rámci plnění Smlouvy;
 - o. dodržovat pravidla a standardy bezpečného vývoje, a to v souladu s požadavky ZoKB a VoKB, přičemž je nezbytné, aby veškeré činnosti spojené s návrhem, vývojem, úpravami a implementací aplikace probíhaly na základě principů „security by design“ a „security by default“. Významný dodavatel je povinen používat uznávané bezpečnostní standardy bezpečného vývoje (např. OWASP, secure coding guidelines (standardizované postupy pro bezpečné programování), bezpečný životní cyklus vývoje aplikací - SDLC), zavádět kontrolní mechanismy pro předcházení vzniku zranitelností, provádět bezpečnostní revize kódu a testování zaměřené na bezpečnost, zajistit průběžné sledování rizik spojených s použitými komponentami a knihovnami a odstranit zjištěné nedostatky před předáním Objednateli. Současně je povinen vést a udržovat dokumentaci potvrzující splnění požadavků bezpečného vývoje tak, aby Objednatel mohl prokázat naplnění povinností podle ZoKB a navazujících prováděcích předpisů;
 - p. vést v elektronické formě přehled vykonávaných činností (výkaz) obsahující veškeré podstatné okolnosti související s plněním povinností Dodavatele z oblasti plnění Kybernetických požadavků a provozem aplikace, provozní události důležitých aktiv a relevantní záznamy o plnění povinností Dodavatele, a tyto předávat v rámci měsíčního vyúčtování služeb.
- 21.29.2. Pokud je v rámci Plnění dodávána aplikace, musí Významný dodavatel využívat nástroj pro centrální správu přístupových účtů. A dále musí Aplikace dodávaná Významným dodavatelem:
- a. přidělit každému uživateli a administrátorovi přistupujícímu k informačnímu systému Objednatele přístupová práva a oprávnění a jedinečný identifikátor;
 - b. zajistit přístup na základě přidělených rolí a oprávnění;
 - c. zajistit, že přístupová oprávnění jsou šifrována pomocí odolných kryptografických algoritmů v souladu s aktuálními doporučeními NÚKIB.

21.30. Dodavatel strategicky významné služby

- 21.30.1. Je-li Dodavatel Dodavatelem strategicky významné služby, je dále nad rámec povinností uvedených v odst. 21.1 až 21.28 ZOP povinen:
- a. poskytovat Objednateli veškerou potřebnou součinnost za účelem splnění jeho povinností coby poskytovatele Strategicky významné služby;
 - b. postupovat při plnění Smlouvy tak, aby byla zajištěna dostupnost Strategicky významné služby v nezbytném rozsahu, ve stanoveném čase a kvalitě z území České republiky;
 - c. v případě potřeby poskytnout Objednateli potřebnou součinnost při shromažďování dat za účelem prověřování rizik spojených s Dodavatelem strategicky významné služby;

- d. strpět povinnosti, které na Objednatele klade ZoKB, spojené s prověřováním bezpečnosti dodavatelského řetězce;
- e. zajišťovat Strategicky významnou službu v nezbytném rozsahu mimo území České republiky, kterou musí pravidelně testovat. Zprávu o výsledcích takových testování předloží Dodavatel Strategicky významné služby Objednateli.

21.31. Objednatel je oprávněn požadovat na **Dodavatel** zaplacení smluvní pokuty:

- a. za každý den prodlení při zavedení bezpečnostních opatření podle ZoKB, VoKB, těchto ZOP a Interních předpisů:
 - i. ve výši 0,05 % z Ceny po dobu prvních pěti (5) dnů prodlení;
 - ii. ve výši 0,1 % z Ceny po dobu od šestého (6.) dne prodlení do desátého (10.) dne prodlení; a
 - iii. ve výši 0,2 % z Ceny po dobu od jedenáctého (11.) dne prodlení;
- b. za každý den Objednatelem zjištěného soustavného porušování bezpečnostních opatření podle ZoKB, VoKB, těchto ZOP a Interních předpisů:
 - i. ve výši 0,05 % z Ceny do šestého (6.) dne soustavného porušování; a
 - ii. ve výši 0,1 % z Ceny od šestého (6.) dne soustavného porušování;
- c. ve výši 2 % z Ceny za každý případ porušení povinnosti hlášení událostí, které mají charakter Kybernetického bezpečnostního incidentu;
- d. ve výši 2 % z Ceny za každý případ neumožnění nebo odepření provedení kontroly a auditu kybernetické bezpečnosti ve smyslu článku 21. ZOP;
- e. ve výši 5 % z Ceny za každý případ porušení článku 21. ZOP, přičemž toto porušení vedlo ke Kybernetickému bezpečnostnímu incidentu;
- f. ve výši 0,1 % z Ceny za každý započatý den trvání porušení povinností Významného dodavatele dle článku 21. ZOP, kdy dané porušení nebylo odstraněno a negativní následek porušení povinnosti stále trvá;
- g. ve výši 1 % z Ceny za každý případ jiného porušení článku 21. ZOP neuvedeného výše.

22. OCHRANA OSOBNÍCH ÚDAJŮ

- 22.1. Budou-li údaje, ke kterým Dodavatel získá přístup v souvislosti s Plněním dle Smlouvy, mít povahu Osobních údajů, je Dodavatel povinen přijmout veškerá opatření k tomu, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k těmto Osobním údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům či jinému zneužití, a zajistit nakládání s Osobními údaji v souladu s GDPR.
- 22.2. Pokud bude v rámci provádění Plnění docházet ke zpracování Osobních údajů, je rozsah zpracovávaných Osobních údajů uveden ve Smlouvě. Pokud dojde v rámci poskytování Plnění ke zpracování Osobních údajů, které Smlouva výslovně neuvádí, budou tato nová zpracování Osobních údajů prováděna za stejných podmínek.
- 22.3. Dodavatel bude zpracovávat Osobní údaje pro Objednatele výhradně za účelem poskytování služeb v rozsahu ujednaném podle Smlouvy. Dodavatel bude pro Objednatele zpracovávat Osobní údaje výhradně za uvedeným účelem, způsobem a na základě doložených pokynů a podmínek Objednatele a v souladu s nimi tak, jak vyplývají ze Smlouvy. Dodavatel neprodleně informuje Objednatele, pokud jsou podle jeho názoru určité pokyny Objednatele v rozporu s účinnými právními předpisy.
- 22.4. Dodavatel se zavazuje přijmout vhodná technická a organizační opatření podle GDPR, které se na něj jako na zpracovatele vztahují, a plnění těchto povinností na vyžádání doložit Objednateli.
- 22.5. Dodavatel může předávat Osobní údaje do třetí země nebo mezinárodní organizaci ve smyslu GDPR pouze na základě zvláštního pokynu Objednatele. Je-li takovéto předání založeno na povinnosti vyplývající z práva Unie nebo členského státu, které se na Objednatele vztahuje,

informuje Dodavatel Objednatele o tomto právním požadavku před předáním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu.

- 22.6. Dodavatel je povinen zajistit, aby se osoby oprávněné zpracovávat osobní údaje zavázaly zachovávat mlčenlivost ve vztahu ke všem Osobním údajům, které zpracovává na základě Smlouvy, a rovněž tak o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů.
- 22.7. Dodavatel je povinen přijmout všechna opatření dle čl. 32 GDPR tak, aby byla zajištěna odpovídající bezpečnost Osobních údajů. Dodavatel může do zpracování zapojit Poddodavatele pouze na základě předchozího písemného souhlasu Objednatele. Dodavatel se zavazuje s těmito Poddodavateli uzavřít smlouvu v souladu s GDPR zajišťující dodržování práv a povinností stanovených Smlouvou a/nebo těmito ZOP, zvláště pak povinnosti mlčenlivosti a zajištění bezpečnosti Osobních údajů a poskytnutí dostatečných záruk pro zavedení stejných technických a organizačních opatření Poddodavatelem, jakož i v souladu s dalšími aplikovatelnými právními předpisy. Dodavatel je dále povinen zohlednit povahu zpracování, být Objednateli nápomocen prostřednictvím vhodných technických a organizačních opatření pro splnění povinnosti Objednatele reagovat na žádost o výkon práv subjektu údajů dle GDPR.
- 22.8. Dodavatel je povinen být Objednateli nápomocen při zajišťování souladu s povinnostmi podle článku 32 až 36 GDPR, a to při zohlednění povahy zpracování informací, jež má Dodavatel k dispozici. V případech, kdy povaha věci vyžaduje informování Objednatele ze strany Dodavatele, informuje Dodavatel Objednatele bez zbytečného odkladu.
- 22.9. Dodavatel je povinen umožnit Objednateli a jím pověřené osobě během běžné pracovní doby Dodavatele provést v sídle Dodavatele kontrolu dodržování povinností týkajících se zpracování Osobních údajů vyplývajících ze Smlouvy, a to i po ukončení stanovené doby zpracování, tj. po ukončení této Smlouvy, a to do 3 měsíců od jejího ukončení.
- 22.10. Po ukončení zpracování Osobních údajů podle Smlouvy je Dodavatel povinen poskytnout Objednateli všechna Zařízení obsahující Osobní údaje, pokud je to možné, a vymazat všechny zpracovávané Osobní údaje ze všech svých systémů nebo databází, včetně vymazání všech záložních kopií, s výjimkou, kdy uchovávání vyžadují právní předpisy, nebo k tomu dal písemný souhlas Objednatel.
- 22.11. V případě, že Dodavatel zpracuje osobní údaje nad rámec vymezený Smlouvou/doloženými pokyny Objednatele, považuje se ve vztahu k takovému zpracování za správce. Pokud tímto zpracováním nad rámec vymezený Smlouvou/doloženými pokyny Objednatele vznikne Objednateli škoda, je Dodavatel povinen škodu uhradit.
- 22.12. Pokud Dodavatel poruší povinnost chránit Osobní údaje v souladu s tímto článkem, vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši částky sankce případně uložené z tohoto důvodu Objednateli ze strany Úřadu pro ochranu osobních údajů či jiným správním orgánem, který bude v budoucnu vykonávat působnost Úřadu pro ochranu osobních údajů. Objednatel je však za předpokladu, že mu k tomu Dodavatel poskytne nezbytnou součinnost, povinen uplatnit v příslušných řízeních veškeré přiměřené námitky, které mohl uplatnit ve svém zájmu, a v rámci řízení je povinen řádně hájit svá práva.

23. OCHRANA DŮVĚRNÝCH INFORMACÍ

- 23.1. Dodavatel se zavazuje zachovávat mlčenlivost o všech Důvěrných informacích, které získal nebo mu byly poskytnuty či zpřístupněny v souvislosti s plněním povinnosti dle Smlouvy, a uchovávat je v tajnosti.
- 23.2. Dodavatel se zavazuje použít Důvěrné informace pouze k plnění svých povinností vyplývajících ze Smlouvy. Dodavatel nesmí použít Důvěrné informace k jinému účelu.
- 23.3. Dodavatel nesmí bez předchozího písemného souhlasu Objednatele zpřístupnit Důvěrné informace žádné třetí osobě, a to v jakékoli formě. To neplatí u Důvěrných informací, ohledně kterých byla Dodavateli pravomocným rozhodnutím soudu, správního orgánu, či jiného příslušného státního orgánu v konkrétním případě uložena povinnost Důvěrnou informaci poskytnout nebo plyne-li taková povinnost Dodavateli z právního předpisu.

- 23.4. Dodavatel nesmí Důvěrné informace bez předchozího písemného souhlasu Objednatele rozmnožovat, kopírovat či jakýmkoliv jiným způsobem reprodukovat. Dodavatel dále nesmí Důvěrné informace bez předchozího písemného souhlasu Objednatele uchovávat v jakékoliv databázi, počítačovém programu, úložišti či na datovém nosiči, vyjma případů, kdy je takové uchování Důvěrných informací nezbytné pro účel vyplývající ze Smlouvy.
- 23.5. Dodavatel se zavazuje provést technická, organizační, právní a personální opatření, kterými zajistí dodržování povinnosti zachovat mlčenlivost o Důvěrných informacích a uchovat Důvěrné informace v tajnosti v rozsahu podle tohoto článku i ze strany svých zaměstnanců, Poddodavatelů, jakož i dalších osob, kterým budou Důvěrné informace poskytnuty či zpřístupněny.
- 23.6. Objednatel je oprávněn kdykoliv kontrolovat řádné plnění povinností Dodavatele uvedených v tomto článku, k čemuž se Dodavatel zavazuje bez zbytečného odkladu poskytnout Objednateli veškerou součinnost, zejména je Objednatel oprávněn kontrolovat řízení bezpečnosti Důvěrných informací Dodavatelem. V případě, že Objednatel vyzve Dodavatele na základě kontroly k nápravě, je Dodavatel povinen takové výzvě vyhovět v Objednatelem stanovené přiměřené lhůtě.
- 23.7. Dodavatel se během poskytování Plnění pro Objednatele zavazuje informovat Objednatele o fyzických osobách přicházejících do kontaktu s Důvěrnými informacemi Objednatele (jedná se například o osoby zastávající bezpečnostní role, penetrační testery a administrátory apod.).
- 23.8. Objednatel je oprávněn požadovat na Dodavateli zaplacení smluvní pokuty:
- a. ve výši 500 000 Kč za každé jednotlivé jednání, které představuje porušení jakékoli z povinností Dodavatele dle tohoto článku, vyjma povinností stanovených v odst. 23.6. ZOP
 - b. ve výši 100 000 Kč za každé jednotlivé jednání, které představuje porušení jakékoli z povinností stanovených v odst. 23.6. ZOP.

Příloha č. 4 Výzvy

Vzor profesního životopisu

Předpokládaná **pozice** ze seznamu realizačního týmu dodavatele: **[VYBERE DODAVATEL: „Vedoucí týmu“ / „Penetrační tester“]**

- a. Příjmení: **[DOPLNÍ DODAVATEL]**
- b. Jméno: **[DOPLNÍ DODAVATEL]**
- c. Titul: **[DOPLNÍ DODAVATEL]**
- d. Kontaktní pracovní adresa (včetně pracovního tel/e-mail): **[DOPLNÍ DODAVATEL]**
- e. Současná funkce/pracovní pozice včetně uvedení osoby zaměstnavatele a vztahu k zaměstnavateli, příp. uvést OSVČ či jinak dle skutečného stavu: **[DOPLNÍ DODAVATEL]**

Pozn.: Dodavatel uvede některou z následujících alternativ: pracovní poměr na plný úvazek, pracovní poměr na částečný úvazek, dohoda o pracovní činnosti, dohoda o provedení práce, člen statutárního orgánu, OSVČ, příp. další možnost. Pro vyloučení pochybností zadavatel uvádí, že pokud je dokládána osoba OSVČ a zároveň není současně dodavatelem nebo není vůči dodavateli v pracovním či obdobném poměru, bude považována za jinou osobu ve smyslu § 83 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, se všemi důsledky z toho vyplývajícími, nikoliv za zaměstnance či za osobu v obdobném postavení.

- f. Osoba **je / není** **[DOPLNÍ DODAVATEL]** zaměstnancem dodavatele.
- g. Osoba **je / není** **[DOPLNÍ DODAVATEL]** současně zaměstnancem zadavatele.
- h. **Praxe** pro účely prokázání kvalifikace čl. 9.5.3. Zadávací dokumentace:

Počet celých let odborné praxe celkem	[DOPLNÍ DODAVATEL]
Kdy (MM/RRRR - MM/RRRR) a na jakých pozicích a u jakých zaměstnavatelů (či jako OSVČ) člen realizačního týmu praxi získal?	[DOPLNÍ DODAVATEL]

- i. **Zkušenosti** pro účely prokázání kvalifikace čl. 9.5.3. Zadávací dokumentace:

1) Název služby (činnosti/zakázky)	[DOPLNÍ DODAVATEL]
------------------------------------	---------------------------

Objednatel zakázky (obch. firma/název a sídlo a kontaktní osoba objednatele - jméno, tel., email)	[DOPLNÍ DODAVATEL]
Datum realizace projektu (MM/RRRR – MM/RRRR)	[DOPLNÍ DODAVATEL]
Popis předmětu projektu	[DOPLNÍ DODAVATEL]
Popis role/pozice, kterou člen týmu zastával v rámci projektu	[DOPLNÍ DODAVATEL]

2) Název služby (činnosti/zakázky)	[DOPLNÍ DODAVATEL]
Objednatel zakázky (obch. firma/název a sídlo a kontaktní osoba objednatele - jméno, tel., email)	[DOPLNÍ DODAVATEL]
Datum realizace projektu (MM/RRRR – MM/RRRR)	[DOPLNÍ DODAVATEL]
Popis předmětu projektu	[DOPLNÍ DODAVATEL]
Popis role/pozice, kterou člen týmu zastával v rámci projektu	[DOPLNÍ DODAVATEL]

3) Název služby (činnosti/zakázky)	[DOPLNÍ DODAVATEL]
Objednatel zakázky (obch. firma/název a sídlo a kontaktní osoba objednatele - jméno, tel., email)	[DOPLNÍ DODAVATEL]
Datum realizace projektu (MM/RRRR – MM/RRRR)	[DOPLNÍ DODAVATEL]
Popis předmětu projektu	[DOPLNÍ DODAVATEL]
Popis role/pozice, kterou člen týmu zastával v rámci projektu	[DOPLNÍ DODAVATEL]

V případě dalších zkušeností použije dodavatel tabulku opakovaně dle potřeby.

Přílohy:

- kopie certifikátů požadovaných v čl. 9.5.3. zadávací dokumentace