

Kupní smlouva na dodávku HW a SW

Číslo smlouvy kupujícího 27843/2025-SŽ-GŘ-O8

Číslo smlouvy prodávajícího

uzavřená podle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“)

(dále jen „**Smlouva**“)

Kupující: Správa železnic, státní organizace

zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. A 48384

Praha 1 - Nové Město, Dlážďená 1003/7, PSČ 110 00

IČ 70994234, DIČ CZ70994234

zastoupená **Bc. Jiřím Svobodou, MBA**, generálním ředitelem

Prodávající: ALTEPRO solutions a.s.

zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. B 20333

Na Maninách 1092/20, Holešovice, 170 00 Praha 7

IČ 03665496, DIČ CZ03665496

Bankovní spojení: xxxxx

Číslo účtu: xxxxx

zastoupená **Ing. Martinem Vítkem**, předsedou představenstva

(Kupující a Prodávající dále tak jako „**Smluvní strany**“ nebo „**Strany**“)

Tato smlouva je uzavřena na základě výsledků výběrového řízení veřejné zakázky s názvem „**DMZ serverová farma**“, č.j. veřejné zakázky 12395/2025-SŽ-GŘ-O8 (dále jen „**Veřejná zakázka**“). Jednotlivá ustanovení této Smlouvy tak budou vykládána v souladu se zadávacími podmínkami Veřejné zakázky.

1. Předmět smlouvy

1.1. Předmětem této smlouvy je dodávka Hardware a Software včetně potřebných licencí pro obměnu DMZ farmy v lokalitě zadavatele – ČD Telematika a.s., Pod Tábořem 369/8a, 190 00 Praha 9 - Hrdlořezy dle specifikace v Příloze č. 1 *Specifikace Plnění*.

1.2. Touto Smlouvou se Prodávající zavazuje:

- (a) dodat Hardware alespoň v kvalitě a specifikacích uvedených v Příloze č. 1 *Specifikace Plnění* této Smlouvy a další drobné hmotné pomůcky či předměty jinak nezbytné pro uvedení Hardware do běžného provozu (například propojovací kabely, napájecí kabely, šrouby, koncovky apod.) v rámci IT prostředí Kupujícího;

- (b) poskytnout oprávnění užít případný Software (např. firmware, obslužné ovladače apod.), který je součástí Hardware uvedeného v Příloze č. 1 *Specifikace Plnění* této Smlouvy;
- (c) předat Kupujícímu Dokumentaci a poskytnout Kupujícímu oprávnění Dokumentaci užít;
- (d) provést dopravu Hardware do místa plnění, včetně umístění Hardware do vhodného přepravního obalu zamezujícího anebo minimalizujícího případné poškození Hardware během dopravy;
- (e) poskytnout Kupujícímu záruku za jakost k dodanému Hardware a Software;
- (f) provést fyzickou instalaci Hardware včetně případné likvidace odpadů vzniklých při instalaci v Místě plnění a poskytnout Kupujícímu záruku za jakost na provedenou Instalaci;
- (g) poskytnout oprávnění užít Software uvedený v Příloze č. 1 *Specifikace Plnění* této Smlouvy („**Software**“);
- (h) poskytovat služby k dodanému Hardware po dobu, v rozsahu a za podmínek dále stanovených v Příloze č. 1 *Specifikace plnění* („**Služby**“);

(dále jen „**Plnění**“).

1.3. Touto Smlouvou se Kupující zavazuje:

- (a) převzít dodaný Hardware a Software od Prodávajícího a zaplatit Prodávajícímu za řádně poskytnutý předmět plnění v souladu s touto Smlouvou Cenu (jak je definována níže); a
- (b) poskytnout Prodávajícímu nezbytnou součinnost pro plnění povinností dle této Smlouvy.

2. Další podmínky plnění

- 2.1. Prodávající dodá Hardware a Software v konfiguracích podle jejich specifikace, jež tvoří Přílohu č. 1 *Specifikace Plnění* této Smlouvy. Je-li součástí Veřejné zakázky a byl-li Kupujícímu před podpisem této Smlouvy doručen návrh řešení nebo obdobný dokument, který má v souladu se Zadávací dokumentací k Veřejné zakázce sloužit jako specifikace kvality Plnění anebo podklad pro Plnění, pak je Prodávající povinen provádět Plnění v kvalitě dle takového dokumentu, pokud takový dokument stanoví kvalitu vyšší, než je kvalita specifikovaná v Příloze č. 1 *Specifikace Plnění*.
- 2.2. Prodávající je povinen dodat Hardware do místa plnění na vlastní nebezpečí a na vlastní náklady.
- 2.3. Prodávající je povinen dodat Kupujícímu požadovaný Hardware a Software nejdéle do data dle pravidel článku 4.1. této Smlouvy.
- 2.4. Dodací list musí obsahovat:
 - (a) identifikační (sériové, tovární) číslo každého Hardware nebo Software licencí a typové označení Hardware nebo Software licencí;
 - (b) počet kusů (souprav) dodaného Hardware nebo Software licencí;
 - (c) jednotkovou a celkovou cenu bez DPH za dodaný Hardware nebo Software licenci;
 - (d) místo dodání Hardware nebo Software licencí; a
 - (e) podpis zástupce Prodávajícího.

(„**Dodací list**“)

- 2.5. Podpisem Dodacího listu Kupující přebírá Hardware a Software k provedení akceptačního řízení v místě plnění. Pokud Kupující daný Hardware a Software převezme, potvrdí toto převzetí Prodávajícímu podpisem na Dodacím listu. Prodávající současně doplní na Dodací list datum a čas předání a převzetí Hardware a Software k akceptačnímu řízení. Hardware a Software se považuje za dodaný až okamžikem skončení Akceptačního řízení.
- 2.6. Dodací list bude vyhotoven Prodávajícím ve dvou (2) vyhotoveních. Jedno (1) vyhotovení Dodacího listu obdrží Kupující a jedno (1) vyhotovení Dodacího listu obdrží Prodávající.
- 2.7. Kupující není povinen převzít Hardware nebo Software neodpovídající specifikaci sjednané v této Smlouvě anebo zjevně vykazující vady či vady zabezpečení pro dopravu. V takovém případě Kupující vystaví Prodávajícímu či dopravci potvrzení, které bude obsahovat zejména následující údaje:
- (a) prohlášení, že Kupující odmítá převzít Hardware nebo Software;
 - (b) důvody pro odmítnutí převzetí Hardware nebo Software včetně označení zjištěných vad;
 - (c) datum a čas; a
 - (d) podpis zástupce Kupujícího.
- 2.8. V případě, že převzetí Hardware nebo Software bylo Kupujícím odmítnuto, je Prodávající povinen zjištěné vady na vlastní náklady neprodleně odstranit a vyzvat Kupujícího k opětovnému převzetí Hardware a Software.
- 2.9. V rámci akceptace dodaného Plnění Kupující ověřuje:
- a) parametry, vlastnosti a funkcionality uvedené v Příloze č. 1 *Specifikace plnění* této Smlouvy, a dále vlastnosti a funkcionality uvedené ve specifikaci plnění Prodávajícího (je-li taková), která je součástí Smlouvy;
 - b) příslušenství a dokumentaci, jež mělo být dodáno spolu s Hardware.

3. Kontaktní osoby

- 3.1. Kontaktními osobami za účelem plnění této Smlouvy jsou za Prodávajícího xxxxx, xxxxx, +420 xxxxx.
- 3.2. Kontaktními osobami za účelem plnění této Smlouvy jsou za Kupujícího: xxxxx, +420 xxxxx, xxxxx.
- 3.3. Kontaktní osobou Kupujícího pro oblast kybernetické bezpečnosti je: xxxxx, +420 xxxxx, xxxxx.

4. Doba a místo plnění

- 4.1. Prodávající dodá veškerý požadovaný Hardware a Software nejpozději do 60 dnů ode dne nabytí účinnosti Smlouvy.
- 4.2. Místo dodání plnění je ČD Telematika a.s., Pod Táborem 369/8a, 190 00 Praha 9 - Hrdlořezy.

5. Cena a platební podmínky

- 5.1. Cena za předmět plnění dle této Smlouvy je sjednána v souladu s nabídkovou cenou, kterou Prodávající uvedl ve své nabídce k Veřejné zakázce a je uvedena v Příloze č. 2 *Cena Plnění*.
- 5.2. Podrobný rozpis Ceny dle jednotlivých částí Plnění je rovněž uveden v Příloze č. 2 *Cena Plnění*.

- 5.3. Cena uvedená v Příloze č. 2 *Cena plnění* současně zahrnuje veškeré související náklady Prodávajícího, zejména náklady související s balením a obalovými materiály, jejich odběr, třídění a ekologickou likvidaci, jakož i náklady na dopravu, nakládku a vykládku v místě plnění a náklady na instalaci Hardware a Software.
- 5.4. Cena je výslovně sjednávána jako nejvyšší možná a nepřekročitelná.
- 5.5. Řádné dodání Hardware a Software se předává a přebírá na základě předávacího protokolu podepsaného odpovědnými zástupci smluvních stran. Právo na zaplacení ceny za Hardware a Software dle Přílohy č. 2 *Cena plnění* vzniká dnem podpisu předávacího protokolu o dodání a instalaci Hardware a Software.
- 5.6. Smluvní strany se dohodly, že splatnost daňového dokladu činí 60 dní ode dne jejího doručení Kupujícímu. V případě, že faktura nebude mít odpovídající náležitosti, je Kupující oprávněn ve lhůtě splatnosti ji vrátit Prodávajícímu s vytknutím nedostatků, aniž by se dostal do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od okamžiku doručení opraveného či doplněného daňového dokladu Kupujícímu.

6. Práva duševního vlastnictví

- 6.1. Pro Software vztahující se k Hardware platí článek 6.6. Přílohy č. 5 *Zvláštní obchodní podmínky*.
- 6.2. Pro ostatní Software platí článek 6.5. Přílohy č. 5 *Zvláštní obchodní podmínky*.

7. Helpdesk

- 7.1. Prodávající bude poskytovat Helpdesk v režimu 1 ve smyslu čl. 10.3. Přílohy č. 5 *Zvláštní obchodní podmínky*.
- 7.2. Helpdesk bude Poskytovatelem zajištěn prostřednictvím elektronické pošty, a to na adrese určené Poskytovatelem.
- 7.3. Helpdesk bude poskytován po dobu 5 let od podpisu předávacího protokolu dle čl. 4 Přílohy č. 1 *Specifikace Plnění*.

8. Servisní model

- 8.1. Prodávající bude poskytovat servisní model v režimu A4 ve smyslu čl. 12.2. Přílohy č. 5 *Zvláštní obchodní podmínky* s doručením náhradního dílu a dojezdem technika on-site do 24h od diagnostiky závady. Servisní model bude poskytován pro všechny dodaný Hardware bez nutnosti vrácení paměťových medií v případě reklamace. Vadná média zůstávají v držení zákazníka.
- 8.2. Záruka a servisní služby musí být pokryty oficiální servisní podporou výrobce tak, aby v případě závady, kterou není Poskytovatel schopen odstranit, mohl Kupující tuto závadu eskalovat přímo k technické podpoře výrobce.
- 8.3. Servisní model bude poskytován po dobu 5 let od podpisu předávacího protokolu dle čl. 4 Přílohy č. 1 *Specifikace Plnění*.

9. Kybernetická bezpečnost

- 9.1. Prodávající je povinen dodržovat ustanovení týkající se kybernetické bezpečnosti ve smyslu čl. 20 Přílohy č. 5 *Zvláštní obchodní podmínky*.

10. Ochrana osobních údajů

- 10.1. Pokud bude v rámci plnění této Smlouvy docházet ke zpracování osobních údajů, zavazuje se Prodávající dodržovat opatření dle článku 21. Přílohy č. 5 *Zvláštní obchodní podmínky*.

11. Střet zájmů, povinnosti Prodávajícího v souvislosti s konfliktem na Ukrajině

- 11.1. Prodávající 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 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.
- 11.2. Prodávající prohlašuje, že on, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost byla využita ve smyslu evropských směrnic o zadávání veřejných zakázek, nejsou osobami:
- a. 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, 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,
 - b. 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 (dále jen „**Sankční seznamy**“).
- 11.3. Je-li Prodávajícím sdružení více osob, platí podmínky dle odstavce 11.1 a 11.2 této Smlouvy také jednotlivě pro všechny osoby v rámci Prodávajícího sdružené, a to bez ohledu na právní formu tohoto sdružení.
- 11.4. Přestane-li Prodávající 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 Smlouvy, oznámí tuto skutečnost bez zbytečného odkladu, nejpozději však do 3 pracovních dnů ode dne, kdy přestal splňovat výše uvedené podmínky, Kupujícímu.
- 11.5. Prodávající se dále zavazuje postupovat při plnění této Smlouvy 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, a dalších prováděcích předpisů k tomuto nařízení Rady (EU) č. 269/2014.
- 11.6. Prodávající se dále ve smyslu 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, zavazuje, že finanční prostředky ani hospodářské zdroje, které obdrží od Kupujícího na základě této Smlouvy a jejích případných dodatků, nepřístupní přímo ani nepřímo fyzickým nebo právnickým osobám, subjektům či orgánům s nimi spojeným uvedeným v Sankčních seznamech, nebo v jejich prospěch.
- 11.7. Ukáží-li se prohlášení Prodávajícího dle odstavce 11.1 a 11.2 této Smlouvy jako nepravdivá nebo poruší-li Prodávající svou oznamovací povinnost dle odstavce 11.4 nebo povinnosti dle odstavců 11.5 nebo 11.6 této Smlouvy, je Kupující oprávněn odstoupit od této Smlouvy. Prodávající je dále povinen zaplatit za každé jednotlivé porušení povinností dle předchozí věty smluvní pokutu ve výši 5 % procent z Ceny.

Ustanovení § 2004 odst. 2 Občanského zákoníku a § 2050 Občanského zákoníku se nepoužijí.

12. Závěrečná ustanovení

- 12.1. Prodávající je povinen při plnění svých povinností dle této Smlouvy postupovat v souladu s Přílohou č. 3 *Platforma SŽ* (včetně jejích příloh); v případě rozporu ustanovení Přílohy č. 3 *Platforma SŽ* (včetně jejích příloh) a kteréhokoli dokumentů dle čl. 2.1. této Smlouvy se uplatní ustanovení uvedená v dokumentech dle čl. 2.1. této Smlouvy. Ustanovení dokumentů dle předchozí věty tohoto odstavce mají přednost před ustanoveními obchodních podmínek uvedených v odst. 12.2. tohoto článku.
- 12.2. Smlouva se řídí Obchodními podmínkami Kupujícího a Zvláštními obchodními podmínkami Kupujícího. 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.
- 12.3. Odchylná ujednání v této Smlouvě mají přednost před ustanoveními Obchodních podmínek a Zvláštních obchodních podmínek.
- 12.4. Tuto Smlouvu lze měnit pouze písemnými dodatky.
- 12.5. Tato Smlouva nabývá platnosti okamžikem podpisu poslední ze Stran. Je-li Smlouva uveřejňována v registru smluv, nabývá účinnosti dnem uveřejnění v registru smluv, jinak je účinná od okamžiku uzavření.
- 12.6. Tato Smlouva je vyhotovena v elektronické podobě, přičemž obě Smluvní strany obdrží její elektronický originál opatřený elektronickými podpisy. V případě, že tato Smlouva z jakéhokoli důvodu nebude vyhotovena v elektronické podobě, bude sepsána ve třech vyhotoveních, ve dvou vyhotoveních pro Kupujícího a jedno obdrží Prodávající.
- 12.7. Smluvní strany berou na vědomí, že tato Smlouva 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 Smlouvy, jeho ceně či hodnotě a datu uzavření této Smlouvy.
- 12.8. Zaslání Smlouvy správci registru smluv k uveřejnění v registru smluv zajišťuje obvykle Kupující. Nebude-li tato 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.
- 12.9. Smluvní strany výslovně prohlašují, že údaje a další skutečnosti uvedené v této Smlouvě, vyjma částí označených ve smyslu následujícího odstavce této Smlouvy, nepovažují za obchodní tajemství ve smyslu ustanovení § 504 Občanského zákoníku (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.
- 12.10. Jestliže Smluvní strana označí za své obchodní tajemství část obsahu Smlouvy, která v důsledku toho bude pro účely uveřejnění Smlouvy v registru smluv znečitelněna, nese tato Smluvní strana odpovědnost, pokud by Smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, která ze stran Smlouvu v registru smluv uveřejnila. S částmi Smlouvy, které druhá Smluvní strana neoznačí za své obchodní tajemství před uzavřením této Smlouvy, nebude Kupující 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 doručení písemného oznámení druhé Smluvní strany Kupujícímu obsahujícího přesnou identifikaci dotčených částí 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 Kupujícímu skutečnost, že takto označené informace přestaly naplňovat znaky obchodního tajemství.

12.11. Osoby uzavírající tuto Smlouvu za Smluvní strany souhlasí s uveřejněním svých osobních údajů, které jsou uvedeny v této Smlouvě, spolu se Smlouvou v registru smluv. Tento souhlas je udělen na dobu neurčitou.

12.12. Nedílnou součástí této Smlouvy jsou její přílohy:

Příloha č. 1 – Specifikace Plnění

Příloha č. 2 – Cena Plnění

Příloha č. 3 – Platforma SŽ (včetně jejích příloh)

Příloha č. 4 – Poddodavatelé

Příloha č. 5 – Zvláštní obchodní podmínky

Příloha č. 6 – Obchodní podmínky

Za Kupujícího:

Za Prodávajícího:

podepsáno elektronicky 28. 4. 2025

podepsáno elektronicky 30. 4. 2025

.....
Bc. Jiří Svoboda, MBA
generální ředitel

.....
Ing. Martin Vitek
předseda představenstva

Příloha č. 1 Smlouvy

Specifikace plnění

1. SPECIFIKACE HARDWARE

Na základě této Smlouvy dodá Prodávající Hardware dle následujících požadavků Kupujícího:

a) Konfigurace – čtyři serverové nody pro DMZ Farmu

ThinkAgile HX630 V3

Požadavek	Nabízené řešení
4 serverové nody se shodnou konfigurací	ThinkAgile HX630 V3
Provedení serverového nodu pro instalaci do rackové skříně o hloubce 100 cm	ANO nabízené servery ThinkAgile HX630 V3 jsou instalovatelné do rackové skříně o hloubce 100 cm
Velikost skříně serveru o maximální výšce 1 RU (44,5 mm)	ANO nabízené servery ThinkAgile HX630 V3 jsou 1U vysoké
2x CPU, každý minimálně 16 fyzických jader (32 vláken) se základní frekvencí minimálně 2.0 GHz se spotřebou maximálně 270 W TDP, výkon dle www.spec.org ve sloupci baseline minimálně 323 bodů pro CPU2017 Integer Rates a 431 pro CPU2017 Floating Point Rates	ANO nabízené servery obsahují 2x Intel Xeon Gold 6526Y 16C 195W 2.8GHz Processor, výkon dle www.spec.org ve sloupci baseline minimálně 340 bodů pro CPU2017 Integer Rates a 480 pro CPU2017 Floating Point Rates
Operační paměť minimálně 768 GB	ANO 768 GB TruDDR5
Minimálně 4x 10/25 Gbps SFP28 LAN adapter včetně SFP+ modulů	ANO 2x Lenovo Dual Rate 10G/25G SR SFP28
Dedikovaný 1 Gbps RJ45 port pro HW management	ANO xCC kontroller obsahuje 1 Gbps RJ45 port
Trusted Platform Module 2.0	ANO TPM 2.0 modul je součástí nabídky
2x hot-swap napájecí zdroj, každý minimálně o výkonu 750 W s minimální certifikací „80 PLUS Titanium“	ANO 2x ThinkSystem 1100W 230V Titanium Hot-Swap Gen2 Power Supply
Výsuvné ližiny do rackové skříně včetně ramena na kabely „cable management arm“	ANO Výsuvné ližiny do rackové skříně včetně ramena na kabely jsou součástí nabídky
2x napájecí kabel 230V CEE7/7 v délce minimálně 3 metry, každý v jiné barvě (černá, červená)	ANO 2x napájecí kabel 230V CEE7/7 v délce minimálně 3 metry, každý v jiné barvě (černá, červená) je součástí nabídky
Vzdálená správa HW pro HCI infrastrukturu - Nástroj pro jednotnou správu celé HW infrastruktury HCI řešení. - Nástroj dostupný ve formě SaaS a virtuální appliance s podporou Air-Gap. - Možnost konfigurace prostřednictvím nástroje jako Terraform, Ansible anebo Puppet, kde integrační moduly jsou poskytnuté přímo výrobcem. - Dokumentované API rozhraní pro volání veškerých dostupných funkcí, včetně těch, které jsou použité v grafickém uživatelském rozhraní. - Možnost připojení vzdálených médií. - Secure Boot.	ANO všechny udávané funkce vzdálené správy jsou součástí nabídky - Nástroj pro jednotnou správu celé HW infrastruktury HCI řešení. - Nástroj dostupný ve formě SaaS a virtuální appliance s podporou Air-Gap. - Možnost konfigurace prostřednictvím nástroje jako Terraform, Ansible anebo Puppet, kde integrační

- Digitální verifikace softwarového/FW balíčka hash algoritmem a jeho enkrypcí privátním klíčem, a digitálního podpisu připojeného k SW/FW balíčku.
- Runtime ochrana proti „injection“ útokům škodlivého kódu v běžícím SW.
- Řešení pro bezpečný identifikátor zařízení, krypto služby pro interní uložení a správu klíčů pro běžící OS a Aplikace.
- Kontinuální upozorňování na bezpečnostní zranitelnosti v HW, FW, SW běžícím na řešení.
- Pravidelná kontrola kompatibility serverových modelů, procesorů, firmwarů, adaptérů, operačních systémů a ovladačů.
- Integrace s managementem třetích stran (nativní integrace anebo pomocí např. redfish).
- Integrace s databázovými systémy Oracle a MS SQL.
- Integrace s hypervizorem Nutanix AHV, VMware vSphere.
- „zero-touch“ operace bez nutnosti instalace SW lokálně a bez nutnosti instalace integrované appliance.
- Automatická aktualizace funkcionalit a možností nástroje.
- Automatická integrace podpory výrobce, automatický sběr logů a možnost automatického vytvoření servisní požadavky.
- Integrovaný orchestrátor a automatizační framework na podporu řešení výrobce a systémů třetích stran (datové uložení, hypervizory).
- Nástroj pro správu podporuje bezstavové prostředí, kde identitu serveru vytváří správce anebo automatizační systém, který definuje konfigurace serveru, jako jsou: verze BIOSu, MAC ID, verze firmwaru NIC, WWPN, verze firmwaru FC-HBA, QoS adaptéru, UUID, Zásady spuštění serveru, KVM IP atd.
- IP adresa portu pro správu serveru (IMC / KVM) je definovaná jako součást profilu / identity serveru.

moduly jsou poskytnuté přímo výrobcem.

- Dokumentované API rozhraní pro volání veškerých dostupných funkcí, včetně těch, které jsou použité v grafickém uživatelském rozhraní.
- Možnost připojení vzdálených médií.
- Secure Boot.
- Digitální verifikace softwarového/FW balíčka hash algoritmem a jeho enkrypcí privátním klíčem, a digitálního podpisu připojeného k SW/FW balíčku.
- Runtime ochrana proti „injection“ útokům škodlivého kódu v běžícím SW.
- Řešení pro bezpečný identifikátor zařízení, krypto služby pro interní uložení a správu klíčů pro běžící OS a Aplikace.
- Kontinuální upozorňování na bezpečnostní zranitelnosti v HW, FW, SW běžícím na řešení.
- Pravidelná kontrola kompatibility serverových modelů, procesorů, firmwarů, adaptérů, operačních systémů a ovladačů.
- Integrace s managementem třetích stran (nativní integrace anebo pomocí např. redfish).
- Integrace s databázovými systémy Oracle a MS SQL.
- Integrace s hypervizorem Nutanix AHV, VMware vSphere.
- „zero-touch“ operace bez nutnosti instalace SW lokálně a bez nutnosti instalace integrované appliance.
- Automatická aktualizace funkcionalit a možností nástroje.
- Automatická integrace podpory výrobce, automatický sběr logů a možnost automatického vytvoření servisní požadavky.
- Integrovaný orchestrátor a automatizační framework na podporu řešení výrobce a systémů třetích stran (datové uložení, hypervizory).
- Nástroj pro správu podporuje bezstavové prostředí, kde identitu serveru vytváří

	správce anebo automatizační systém, který definuje konfigurace serveru, jako jsou: verze BIOSu, MAC ID, verze firmwaru NIC, WWPN, verze firmwaru FC-HBA, QoS adaptéru, UUID, Zásady spuštění serveru, KVM IP atd. IP adresa portu pro správu serveru (IMC / KVM) je definovaná jako součást profilu / identity serveru.
Záruka a servis: - Záruka a servis 5 let 24 x 7, s doručením náhradního dílu a dojezdem technika on-site do 24h od diagnostiky závady, jedná se o servisní model A4 dle ZOP. - Bez nutnosti vrácení paměťových medií v případě reklamace. Vadná média zůstávají v držení zákazníka. - Záruka a servis musí být pokryty oficiální servisní podporou výrobce tak, aby v případě závady, kterou není dodavatel schopen odstranit, mohl zákazník tuto závadu eskalovat přímo k technické podpoře výrobce.	ANO, součástí nabídky je - Záruka a servis 5 let 24 x 7, s doručením náhradního dílu a dojezdem technika on-site do 24h od diagnostiky závady, 5Yr Premier 24x7 4Hr Resp ThinkAgile CN HX630 V - Bez nutnosti vrácení paměťových medií v případě reklamace. Vadná média zůstávají v držení zákazníka. 5Yr KYD Add-On ThinkAgile CN HX630 V3 - Záruka a servis je pokryta oficiální servisní podporou výrobce. V případě závady, kterou není dodavatel schopen odstranit, může zákazník tuto závadu eskalovat přímo k technické podpoře výrobce.
Potvrzení od lokálního zastoupení výrobce, že nabízený hardware je nový, nepoužitý, je určen pro EU trh a bude servisním střediskem výrobce v ČR plně podporován.	ANO Potvrzení od lokálního zastoupení výrobce že nabízený hardware je nový, nepoužitý, je určen pro EU trh a bude servisním střediskem výrobce v ČR plně podporován je součástí nabídky

b) **Software a licence pro HCI řešení**

Nutanix Cloud Infrastructure Ultimate

Požadavek	Nabízené řešení
Podpora hypervizorů vSphere, AHV	ANO Nutanix podporuje vSphere, AHV hypervizory
Úložiště rozložené na všech uzlech musí být prezentováno jako jeden distribuovaný file systém všem hostitelským hypervizorům	ANO Úložiště rozložené na všech uzlech je prezentováno jako jeden distribuovaný file systém všem hostitelským hypervizorům
Unitární filesystém musí podporovat minimálně iSCSI, NFS a SMB protokoly	ANO filesystém podporuje iSCSI, NFS a SMB protokol
Podpora online bezvýpadkového rozšíření a odebrání uzlů	ANO online bezvýpadkového rozšíření a odebrání uzlů je podporováno

Škálování a rozšiřování všech HW prostředků najednou (CPU, RAM, úložiště, síťová část)	ANO Škálování a rozšiřování všech HW prostředků najednou (CPU, RAM, úložiště, síťová část) je podporováno
Podpora různých modelů/generací uzlů v rámci jednoho clusteru	ANO Nutanix podporuje různé modely/generace uzlů v rámci jednoho clusteru
Podpora minimálně 32 HW uzlů v rámci jednoho clusteru	ANO Nutanix podporuje minimálně 32 HW uzlů v rámci jednoho clusteru
Podpora virtualizačních, kontejnerových, blokových a souborových služeb	ANO Nutanix podporuje virtualizaci, kontejnerových, blokových a souborových služeb
Podpora integrace s cloudovými službami S3, AWS, Azure, Google cloud	ANO Nutanix podporuje integraci s cloudovými službami S3, AWS, Azure, Google cloud
Podpora integrace se Softwarově definovanými sítěmi	ANO Nutanix podporuje integraci se Softwarově definovanými sítěmi
Podpora all-flash a all-NVMe konfigurace diskového prostoru. Řešení musí umožňovat kombinaci all-flash a all-NVMe uzlů v rámci jednoho clusteru	ANO Nutanix podporuje all-flash a all-NVMe konfigurace diskového prostoru. Řešení umožňuje kombinaci all-flash a all-NVMe uzlů v rámci jednoho clusteru
Možnost rozšíření diskové kapacity řešení bez potřeby dokupu dalších licencí hypervisoru	ANO Nutanix podporuje rozšíření diskové kapacity řešení bez potřeby dokupu dalších licencí hypervisoru
In-line i post-process deduplikace a komprese dat musí být obsažena v ceně řešení	ANO Nutanix podporuje In-line i post-process deduplikaci a kompresi dat Licence je obsažena v ceně řešení
Podpora úspory kapacity pomocí techniky erasure coding	ANO Nutanix podporuje erasure coding
Automatické tierování dat	ANO Nutanix podporuje Automatické tierování dat
Podpora Block Services pro prezentaci diskového prostoru jako iSCSI LUN externím klientům	ANO Nutanix podporuje Block Services pro prezentaci diskového prostoru jako iSCSI LUN externím klientům
Nativní podpora replikace v režimech: Near-sync, asynchronní i synchronní	ANO Nutanix podporuje replikace v režimech: Near-sync, asynchronní i synchronní
Podpora DR konfigurace v režimu N:1, 1:N, N:N	ANO Nutanix podporuje DR konfigurace v režimu N:1, 1:N, N:N
Replikace je granulární a definovatelná v rámci jednotlivých virtuálních strojích, ne jenom jako replikace celého úložiště	ANO Nutanix podporuje granulární a definovatelnou replikaci v rámci jednotlivých virtuálních strojů, ne jenom jako replikaci celého úložiště
Podpora definice konzistenčních skupin (definované VM + prezentovaný diskový prostor v rámci definované skupiny)	ANO Nutanix podporuje definice konzistenčních skupin (definované VM + prezentovaný diskový prostor v rámci definované skupiny)
Možnost vynuceného přiřazení konkrétního virtuálního stroje na konkrétní uzel nebo rack	ANO Nutanix podporuje vynucené přiřazení konkrétního virtuálního stroje na konkrétní uzel nebo rack
Možnost vynuceného přiřazení konkrétního virtuálního stroje čistě do SSD/NVMe kapacity úložiště pro zajištění optimálního výkonu	ANO Nutanix podporuje vynucené přiřazení konkrétního virtuálního stroje čistě do SSD/NVMe kapacity úložiště pro zajištění optimálního výkonu
Podpora replikačního faktoru RF1, RF2 a RF3 (každý blok dat je bez repliky, má jednu anebo dvě repliky)	ANO Nutanix podporuje replikační faktoru RF1, RF2 a RF3 (každý blok dat je bez repliky, má jednu anebo dvě repliky)
Podpora mikrosegmentace a grafické zobrazení toku dat v infrastruktuře	ANO Nutanix podporuje mikrosegmentace a grafické zobrazení toku dat v infrastruktuře

Podpora bezvýpadkové migrace VM mezi clustery	ANO Nutanix podporuje bezvýpadkově migrace VM mezi clustery
Integrovaný nástroj pro správu klíčů (KMS)	ANO Nutanix má Integrovaný nástroj pro správu klíčů (KMS)
Podpora vynucení přístupu pouze pomocí SSH klíčů	ANO Nutanix podporuje vynucení přístupu pouze pomocí SSH klíčů
Podpora konfigurace odolnosti systému vůči výpadku na úrovni uzlu, bloku nebo racku	ANO Nutanix podporuje konfigurace odolnosti systému vůči výpadku na úrovni uzlu, bloku nebo racku
Možnost kombinovat RF1, RF2 a RF3 v rámci jednoho clusteru	ANO Nutanix umí kombinovat RF1, RF2 a RF3 v rámci jednoho clusteru
Nativní podpora řádově desítek snapshotů dané VM bez zásadního negativního dopadu na výkon	ANO Nutanix podporuje řádově desítky snapshotů dané VM bez zásadního negativního dopadu na výkon
Vestavěná podpora pro obnovu jednotlivých souborů ze snapshotů i ze vzdálených replik umístěných v jiném clusteru	ANO Nutanix má vestavěnou podporu pro obnovu jednotlivých souborů ze snapshotů i ze vzdálených replik umístěných v jiném clusteru
Možnost nezávislého nastavení retence i počtu snapshotů v rámci primární i DR lokality/clusteru	ANO Nutanix umí nezávislé nastavení retence i počtu snapshotů v rámci primární i DR lokality/clusteru
Možnost testovat DR scénáře v odděleném síťovém segmentu bez vlivu na produkční prostředí	ANO Nutanix umí testovat DR scénáře v odděleném síťovém segmentu bez vlivu na produkční prostředí
Jednotný management bez ohledu na celkovou velikost řešení a počet nasazených clusterů	ANO Nutanix podporuje jednotný management bez ohledu na celkovou velikost řešení a počet nasazených clusterů
Jednotný management pro HW vrstvu, hypervisor, softwarově definované úložiště i ochranu dat	ANO Nutanix podporuje jednotný management pro HW vrstvu, hypervisor, softwarově definované úložiště i ochranu dat
Podpora automatického bezvýpadkového upgrade firmware a software (vyžadovaná automatická detekce a stažení vhodného FW/SW, ověření nutných prerekvizit a kompatibilit)	ANO Nutanix umí automatický bezvýpadkový upgrade firmware a software (vyžadovaná automatická detekce a stažení vhodného FW/SW, ověření nutných prerekvizit a kompatibilit)
Podpora automatické diagnostiky a hlášení chybových stavů - "call home"	ANO Nutanix podporuje automatickou diagnostiku a hlášení chybových stavů - "call home"
Vzdálené bezdotykové nasazení bez DHCP	ANO Nutanix podporuje vzdálené bezdotykové nasazení bez DHCP
Automatizován Vlastní pracovní postup pro vzdálenou instalaci operačního systému na baremetal server	ANO Nutanix má automatizován Vlastní pracovní postup pro vzdálenou instalaci operačního systému na baremetal server
Kontrola kompatibility vestavěného firmwaru (HCL) zabudovaná do automatizovaného pracovního postupu	ANO Nutanix umí kontrolovat kompatibilitu vestavěného firmwaru (HCL) která je zabudovaná do automatizovaného pracovního postupu
Automatické stahování firmwaru a aktualizace při nasazení clusteru	ANO Nutanix umí automatické stahování firmwaru a aktualizací při nasazení clusteru
Jednoduchý ověření a bezpečný mechanismus nasazování nových serverů pomocí konektoru zařízení BMC	ANO Nutanix má jednoduchý ověření a bezpečný mechanismus nasazování nových serverů pomocí konektoru zařízení BMC
Bezpečnostní doporučení a varování a notifikace o bezpečnostních zranitelnostech hardwaru a softwaru	ANO Nutanix má bezpečnostní doporučení a varování a notifikace o bezpečnostních zranitelnostech hardwaru a softwaru

Proaktivní notifikace a výměna poškozeného hardwaru	ANO Nutanix má proaktivní notifikace a výměna poškozeného hardwaru
Automatické uploadování logů pro potřeby technické podpory	ANO Nutanix má automatické uploadování logů pro potřeby technické podpory
Podpora file serveru s využitím protokolů NFS a SMB	ANO Nutanix podporuje file server s využitím protokolů NFS a SMB
Podpora integrace s MS Active Directory a MS Entra ID	ANO Nutanix podporuje integraci s MS Active Directory a MS Entra ID
Možnost volby edice s dlouhodobou podporou s konzervativním aktualizacím cyklem nebo naopak častěji frekvenci aktualizací s cílem získání nových funkcionalit	ANO Nutanix má možnost volby edicí s dlouhodobou podporou s konzervativním aktualizacím cyklem nebo naopak častější frekvenci aktualizací s cílem získání nových funkcionalit
Podpora Rest-API	ANO Nutanix podporuje Rest-API
Řešení musí být odolné vůči výpadku SSD/NVMe i jednoho celého uzlu (N+1 odolnost)	ANO Nutanix řešení je odolné vůči výpadku SSD/NVMe i jednoho celého uzlu (N+1 odolnost)
V případě poruchy pevného disku (SSD, NVMe) nesmí být vyřazeny další disky	ANO Nutanix v případě poruchy pevného disku (SSD, NVMe) nevyřadí další disky
V případě selhání HW musí řešení samo přejít do stavu odolného vůči dalším výpadkům – self-healing bez nutnosti manuálního zásahu	ANO Nutanix v případě selhání HW umí sám přejít do stavu odolného vůči dalším výpadkům – self-healing bez nutnosti manuálního zásahu
Automatické balancování zátěže pro optimální využití HW prostředků	ANO Nutanix umí automatické balancování zátěže pro optimální využití HW prostředků
Celé řešení musí být spravováno z jednotné konzole dostupné z jakéhokoli počítače pomocí HTML5 bez nutnosti instalace klienta.	ANO Nutanix řešení je spravováno z jednotné konzole dostupné z jakéhokoli počítače pomocí HTML5 bez nutnosti instalace klienta.
Granulární licenční model umožňující prvotní nákup a další rozšiřování po jednotkách (1 TB nebo 1 cpu jádro – dle licenční metriky)	ANO Nutanix má granulární licenční model umožňující prvotní nákup a další rozšiřování po jednotkách (1 TB nebo 1 cpu jádro – dle licenční metriky)
Globální podpora výrobce pro celé HCI řešení (HW, SW, síťovou část a možnost zahrnout aplikace běžící na HCI řešení)	ANO Nutanix má globální podporu pro celé HCI řešení (HW, SW, síťovou část a možnost zahrnout aplikace běžící na HCI řešení)

Instalační materiál

- 8x minimálně 5m optický patch kabel SM LC/LC OM4
- 8x minimálně 5m DAC kabel pro propojení FC
- Materiál pro montáž dodaného Hardware do racku

Kvalita a specifikace Hardware: Veškerý Hardware je nový, nepoužitý, pochází z oficiální české distribuce a je podporován servisním střediskem výrobce v ČR.

Specifikace dalšího zařízení, které je součástí Plnění: Žádné další zařízení není součástí plnění.

Prodávající je povinen předat Kupujícímu spolu s Hardware doklady, které jsou nutné k převzetí a k užívání Hardware, a to:

- technickou dokumentaci Hardware a Software;
- návod k obsluze;
- prohlášení výrobce o shodě;
- Dodací list;

a další dokumenty potřebné k užívání Hardware či Software: Žádné další dokumenty potřebné k užívání Hardware či Software nejsou součástí nabídky.

2. INSTALACE HARDWARE

Instalace dodaného Hardware v lokalitě

- Montáž dodaného Hardware do racku zadavatele
 - 4ks Server
- Konfigurace dodaného Hardware do prostředí zadavatele
- Ekologickou likvidaci odpadu

SPECIFIKACE SOFTWARE DODÁVANÉHO K HARDWARE

Současně s Dodávkou poskytne Prodávající Kupujícímu tento Software (např. firmware, obslužné ovladače a další níže specifikovaný Software): Lenovo XClarity Pro

Specifikace Software:	
název Software:	Lenovo XClarity Pro
název výrobce Software:	Lenovo
popis jakým způsobem budou Kupujícímu zajištěny aktualizace Software	Aktualizace SW jsou dostupné na oficiálním webu výrobce Lenovo a jsou volně stažitelné

3. ŠKOLENÍ

Školení není součástí zakázky.

4. AKCEPTAČNÍ ŘÍZENÍ

Podmínky akceptačního řízení dle čl. 8 Zvláštních obchodních podmínek se neuplatní. O předání a převzetí Hardware dle čl. 2 této přílohy bude sepsán a oboustranně podepsán předávací protokol o dodání Hardware, a to po instalaci dodaného Hardware v lokalitě.

5. SLUŽBY

Není součástí dodávky.

Příloha č. 2 Smlouvy

Cena plnění

1. CENA ZA HARDWARE

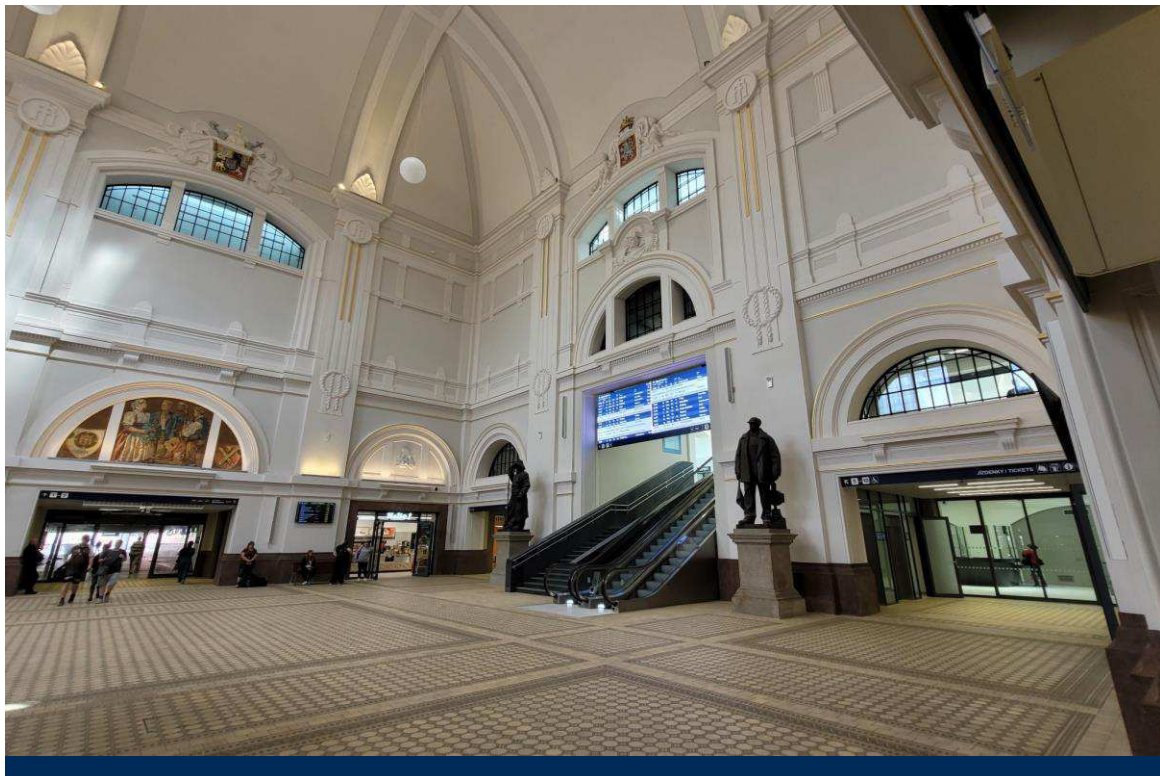
Specifikace Hardware	cena za jeden kus Hardware (v Kč bez DPH)	Počet kusů	cena za počet kusů Hardware (v Kč bez DPH)
Serverový nod pro DMZ Farmu (položka a. dle Specifikace plnění)	370 602,50	4	1 482 410,00
Instalační materiál (dle Specifikace plnění)	nebude oceněno za kus, ale za kompletní instalační materiál	komplet	20 790,00
cena celkem za Hardware v Kč bez DPH	1 503 200,00		
Výše DPH	315 672,00		
Cena celkem za Hardware v Kč včetně DPH	1 818 872,00		

2. CENA ZA SOFTWARE

Specifikace Software	cena za jeden kus Software (v Kč bez DPH)	Počet kusů	cena za počet kusů Software (v Kč bez DPH)
Software a licence pro HCI řešení (položka b. dle Specifikace plnění)	767 812,50	4	3 071 250,00
cena celkem za Software v Kč bez DPH	3 071 250,00		
Výše DPH	644 962,50		
Cena celkem za Software v Kč včetně DPH	3 716 212,50		

CELKOVÁ CENA ZA PLNĚNÍ

Celková Cena za Plnění, tj. součet výše uvedených celkových cen za HW a SW (v Kč bez DPH):	4 574 450,00
Výše DPH	960 634,50
Cena celkem za Plnění v Kč včetně DPH	5 535 084,50



Platforma SŽ Základní dokument

Červen 2024

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 dodavateli	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	Systém 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)

- 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 releasů 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. Integrační 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:

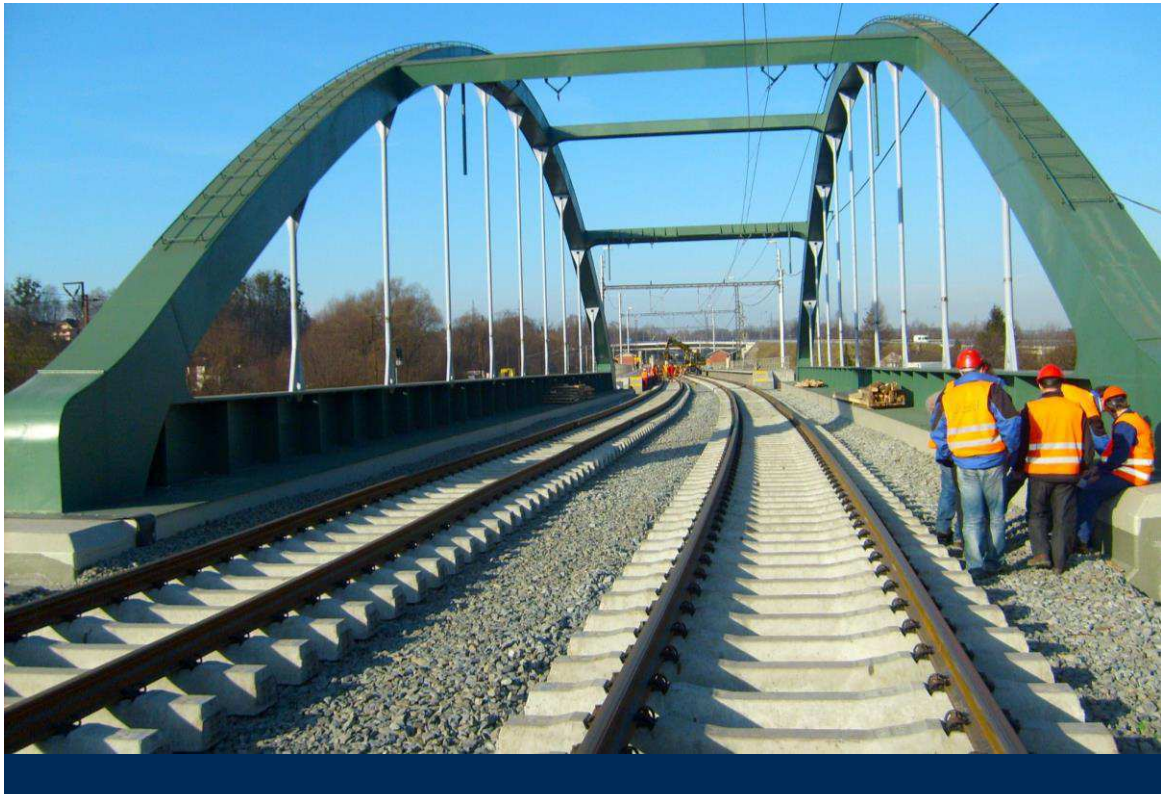
- Příloha 1 – Standardy softwarového vývoje
- Příloha 2 – Datová centra a serverovny
- Příloha 3 – Virtuální prostředí, serverové farmy a servery
- Příloha 4 – Konektivita a síťové prostředí
- Příloha 5 – Integrační standardy
- Příloha 6 – Komunikační standardy
- Příloha 7 – Standardy zálohování a disaster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

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

© 2024

Datum tisku
2024-10-01

spravazeleznic.cz



Platforma SŽ Standardy vývoje software

Červen 2024

Obsah

1	Úvod	5
2	Standardy vývoje informačních systémů Správy železnic	5
2.1	Dvouvrstvá architektura	5
2.1.1	Datová vrstva	5
2.1.2	Aplikační vrstva	5
2.2	Třívrstvá a vícevrstvá architektura	6
2.2.1	Datová vrstva	6
2.2.2	Aplikační vrstva	6
2.2.3	Prezentační vrstva	6
2.2.4	Integrační vrstva	7
2.3	Požadavky na prezentační vrstvu	7
2.3.1	Uživatelské rozhraní	7
2.3.2	Uživatelská zkušenost	7
2.4	Bezpečnost	8
2.4.1	Zabezpečení aplikací	8
2.4.2	Autentizace a autorizace	9
2.4.3	Zpracování osobních údajů	9
2.5	Dokumentace	9
2.5.1	Technická dokumentace jádra systému	9
2.5.2	E-R modely databáze	9
2.5.3	Objektový model pro aplikace	10
2.5.4	Procesní diagramy, schémata toků dat	10
2.5.5	Komunikační rozhraní	10
2.5.6	Drátové modely všech obrazovek uživatelského rozhraní aplikací	10
2.5.7	Popis konfigurace provozního prostředí	10
2.5.8	Uživatelská příručka	10
2.5.9	Příručka administrátora	10
2.5.10	Disaster Recovery postup (D/R Postup)	10
2.6	Modelování EA architektury	10
2.7	Předávání vývoje do provozu	11

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, uchovávání 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>)
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.
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
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 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.

2.1.1 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.

2.1.2 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 2.4.

2.2 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

2.2.1 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 vrstvou. Veškerá aplikační logika musí být umístěna výhradně v aplikační vrstvě.

2.2.2 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 2.4.

2.2.3 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.

2.2.4 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.

2.3 Požadavky na prezentační vrstvu

2.3.1 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
- 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

2.3.2 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

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

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 dialogích na stejných místech s popisky s jednotnou terminologií

2.4 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

2.4.1 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:

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

- 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.

2.4.2 Autentizace a autorizace

2.4.2.1 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

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.

2.4.2.2 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

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.

2.4.3 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.

2.5 Dokumentace

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

2.5.1 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.

2.5.2 E-R modely databáze

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

2.5.3 Objektový model pro aplikace

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

2.5.4 Procesní diagramy, schémata toků dat

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

2.5.5 Komunikační rozhraní

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

2.5.6 Drátové modely všech obrazovek uživatelského rozhraní aplikací

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

2.5.7 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.)

2.5.8 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.

2.5.9 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.

2.5.10 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.

2.6 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 kompatibilita.

Hlavním schvalovatelem předkládaných modelů je Odbor IT architektury SŽT.

2.7 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.

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

© 2024

Datum tisku
2024-10-01

spravazeleznic.cz



Platforma SŽ Datová centra a serverovny

Červen 2024

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 Přerov)
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 umístěné 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

Datacentrum / 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 směrnicemi.

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. Nepísaným 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 8 kW špičkového příkonu (3 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, trakční napájecí soustava). 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 „ostrovských“ 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

© 2024

Datum tisku
2024-10-16

spravazeleznic.cz

```
hdac0: <NVIDIA (0x0083) HDA CODEC> at cad 0
hdac0: <NVIDIA (0x0083) Audio Function Group>
pcm0: <NVIDIA (0x0083) (HDMI/DP 8ch)> at nid
pcm1: <NVIDIA (0x0083) (HDMI/DP 8ch)> at nid
pcm2: <NVIDIA (0x0083) (HDMI/DP 8ch)> at nid
pcm3: <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 2024

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.
- Klasická virtualizace s dedikovanou storage – preferované řešení pro menší cluster
- 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 cluster

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

Samostatné fyzické servery již není možné do ICT prostředí Správy železnic umisťovat. 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:

- Umisťují 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.
- 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:

- Umisťují 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

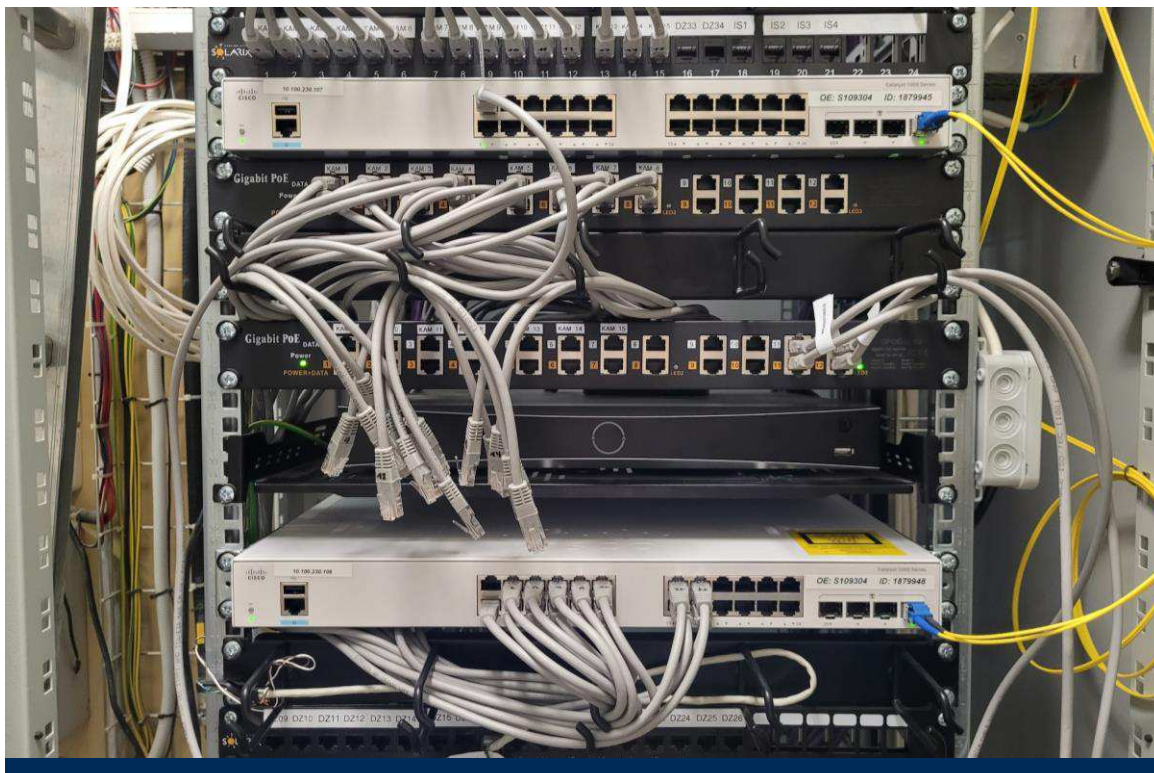
Služba	Popis
Liferay na Win.VMware.x86_64	Liferay je přední open-source podnikové portálové řešení založené na jazyce Java, které umožňuje správu dat, aplikací, procesů a integrace současných i nových aplikací z jednoho centrálního uživatelského rozhraní.

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

© 2024

Datum tisku
2024-10-01

spravazeleznic.cz



Platforma SŽ Konektivita a síťové prostředí

Červen 2024

Obsah

1	Úvod	6
2	Perimetr Správy železnic	6
2.1	Perimetr	6
2.2	Demilitarizovaná zóna	6
2.2.1	Demilitarizovaná zóna pro OT	6
2.3	Přístup přes VPN	6
2.3.1	Uživatelské VPN s MFA	7
2.3.2	Site to Site VPN	7
2.4	Komunikační směry	7
3	Fyzické sítě Správy železnic	8
3.1	Uživatelsko-aplikační síť	8
3.2	Technologické datové sítě	8
3.2.1	Segmentace sítě	8
3.2.2	Ostrovní oddělené sítě	8
4	Logické síťové prostředí	9
4.1	Komunikace mezi sítěmi	9
4.2	Georedundance	9
4.3	Řešení High Availability	9
5	Sítě APN	10
6	Síťová zařízení	10
6.1	Používané technologie	10
6.1.1	VLAN	10
6.1.2	VRF	10
6.1.3	Technologie DWDM	11
6.1.4	Sítě MPLS	11
6.1.5	Síťová spine-leaf topologie	11
6.1.6	Technologie Cisco ACI	11
6.1.7	Sítě OOB	11
6.2	Firewally	12
6.3	Routery	12
6.4	Switche	12
6.4.1	Switche pro datová centra	13
6.4.2	Switche pro fibre channel	13
6.4.3	Switche pro kamerové systémy	13
6.4.4	Switche pro management zařízení	13
6.4.5	Switche pro lokální sítě	14
6.5	Huby	14
6.6	Modemy a datová zařízení	14

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 útočníků (<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 Authentification</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 (<i>Software</i>)
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>)

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.

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 firewallly 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 Sítě 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

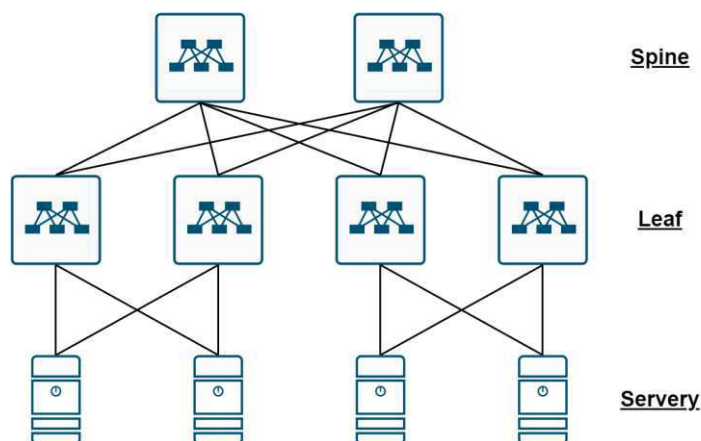
U technologie DWDM jde o metodu vlnového multiplexování, díky tomu se optické vlákno využije pro více vlnových délek (více barev) pro oddělené datové přenosy. V rámci celorepublikového řešení síťové infrastruktury Správy železnic jsou použity DWDM propoje mezi jednotlivými lokalitami jako nosná přenosová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

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 sítě. 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 sítě 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 31x0
Pro datová centra	Firewall pro aplikační farmy, clustery, single nody, NAS atd.	Cisco Firepower 31x0 Fortinet Fortigate vyšších řad
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
MPLS	Routery typu CE	Cisco C9400 Cisco C9300
IT	Routery pro datová centra a IT síť	Cisco C9300 Cisco ISR4000
OT	Lokální routery pro OT síť	Cisco ISR

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
End of Support	Dosluhující řada, postupně se nahrazují	Cisco C2960 více variant Cisco C2950

6.5 Huby

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

6.6 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

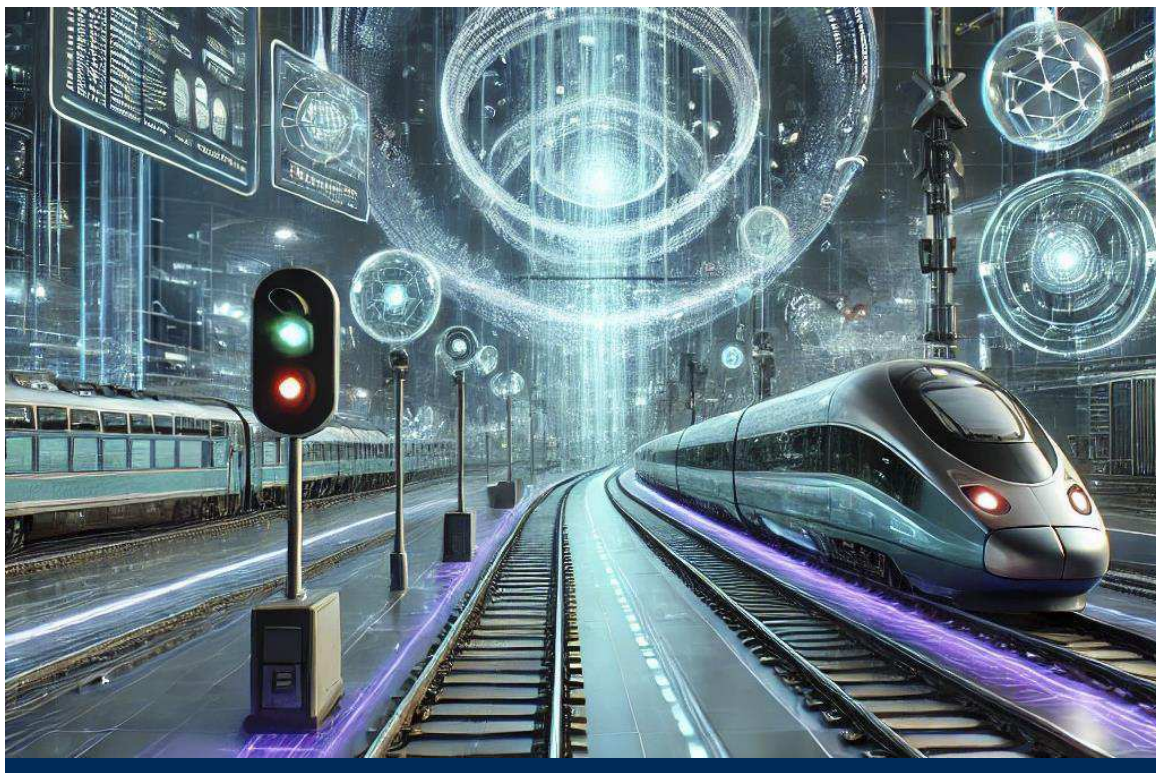
Výrobce	Technologie	Popis	Konkrétní řady/modely
Patton	DSL		1088, 3200, 3088
Albis / Siemens	DSL		BSTU4 / ULAF+
RAD	DSL		ASMI50
Patton	2-pair		3202
CONEL	GPRS	GPRS modem, již ukončená výroba	ER75i
Siemens	GPRS		M35i
Teltonika	4G/LTE	Průmyslové LTE routery s rozhraním RS232, RS485, Ethernet, M-bus	TRBxxx
Advantech	4G/LTE	Průmyslové LTE routery s rozhraním RS232, RS485, Ethernet	ICR-xxxx

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

© 2024

Datum tisku
2024-10-01

spravazeleznic.cz



Platforma SŽ Integrační standardy

Červen 2024

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 WSO2	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

Seznam zkratek

API	Komplexně definované komunikační rozhraní aplikace (<i>Application Programming Interface</i>)
CSV	Jednoduchý textový souborový formát (<i>Comma-separated values</i>)
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 úroveň 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 subsystémy 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 popsaných 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 (nešifrované)	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 (nešifrované), 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

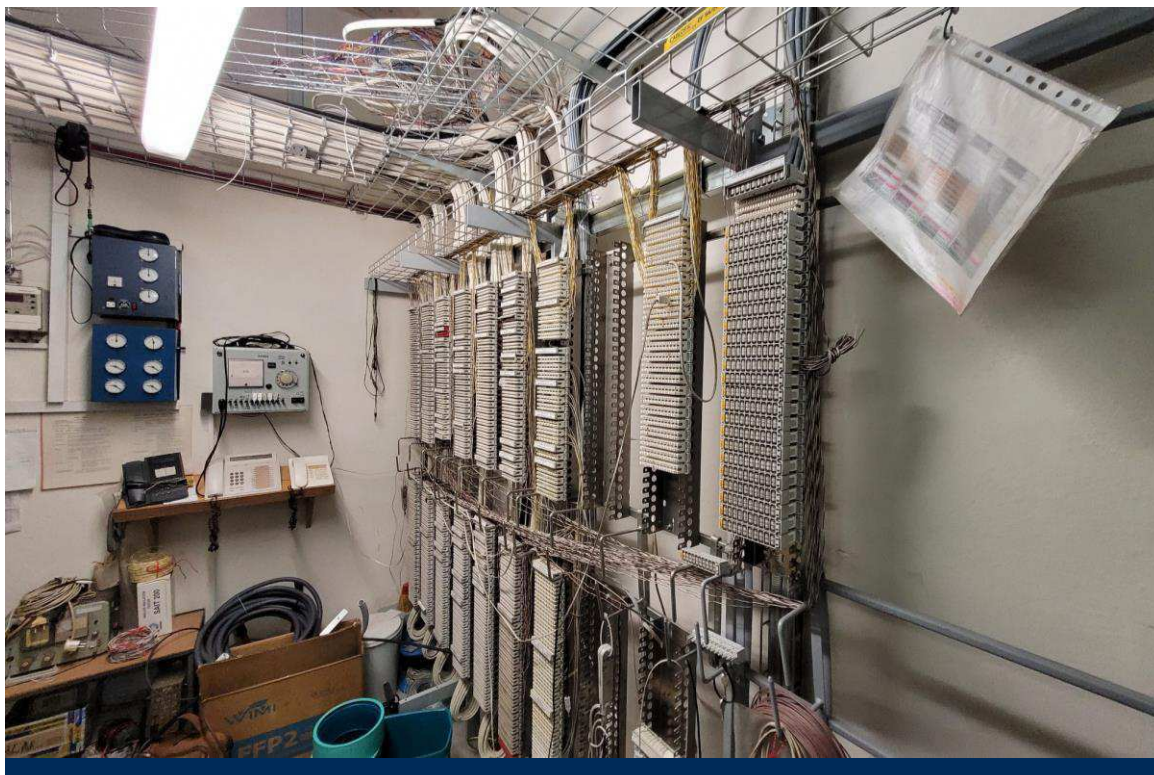
Jakékoliv nové Integrační scénáře, či změny Integračních scénářů musí projít skrze Architecture Board nebo Change management a být posouzeny v širším kontextu. Skrze jaký proces bude integrační scénář posuzován určí matice, která zahrnuje posouzení složitosti změny a její dopady. Integrační scénář následně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

© 2024

Datum tisku
2024-10-01

spravazeleznic.cz



Platforma SŽ Komunikační standardy

Červen 2024

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

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

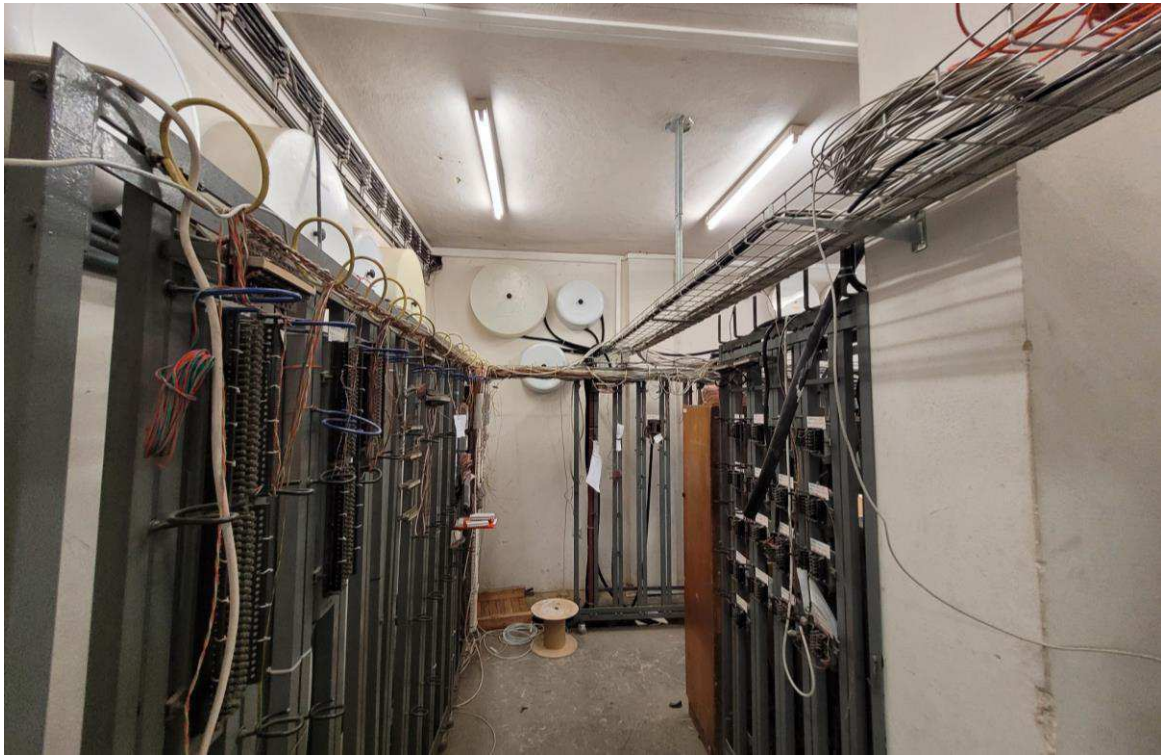
Odesílání emailové komunikace z vnějších sítí mimo perimetr Správy železnic (například SAP Cloud, MS Azure atp.) není v současné době možné.

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.

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

© 2024

Datum tisku
2024-10-01



Platforma SŽ Standardy zálohování a disaster recovery

Červen 2024

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 syntaxi (<i>Structured Query Language</i>)
SŽ	Správa železnic, státní organizace
TSM	Nástroj pro zálohování, v současné době již nese název IBM Spectrum 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 Spectrum Protect (dříve známý jako TSM). Jedná se o komplexní řešení pro fyzické fileservery, virtualizovaná prostředí a širokou škálu aplikací. IBM Spectrum 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.

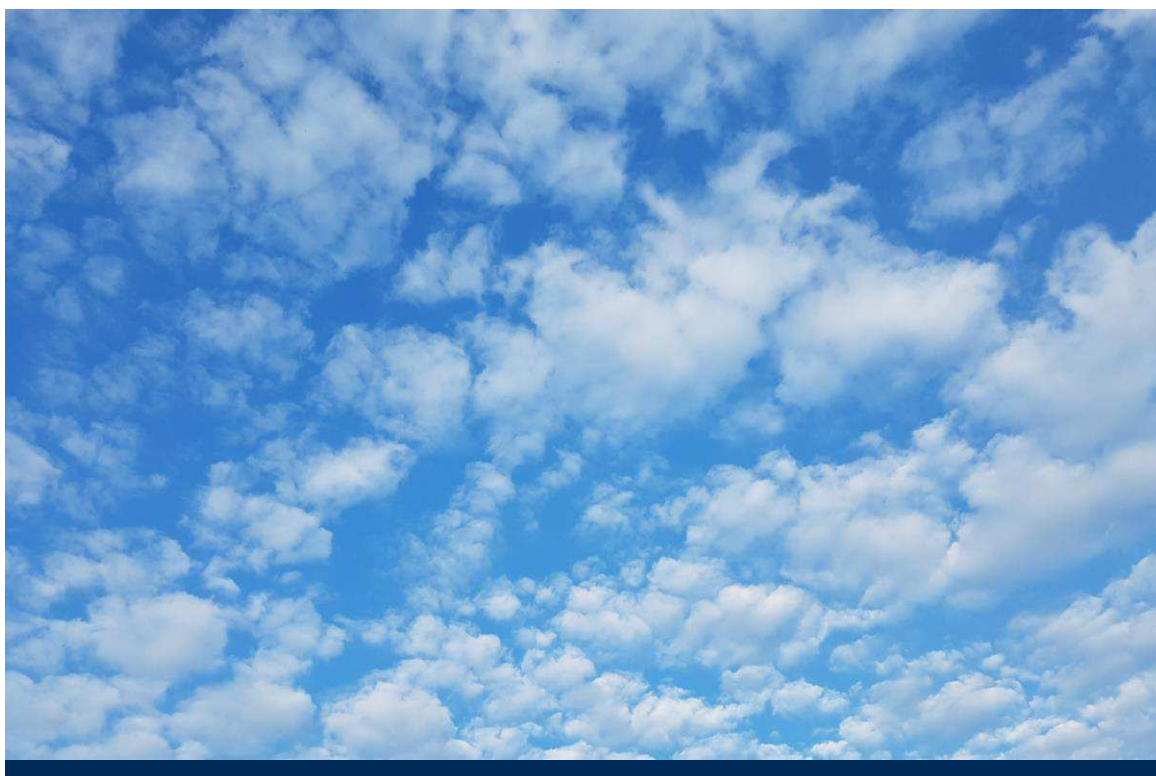
Všechny zálohy jsou pravidelně testovány a veškeré offline zálohy uložené na LTO páskách jsou pravidelně převáženy do zabezpečeného prostoru (do trezoru v jiné budově).

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

© 2024

Datum tisku
2024-10-01

spravazeleznic.cz



Platforma SŽ Cloudové prostředí

Červen 2024

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 až 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 (pay-as-you-go). 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

© 2024

Datum tisku
2024-10-01

spravazeleznic.cz

Příloha č. 4 Smlouvy

Poddodavatelé

Prodávající poskytuje Kupujícímu předmět plnění dle Smlouvy sám.

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	8
4. POVINNOSTI DODAVATELE.....	9
5. POVINNOSTI OBJEDNATELE	10
6. LICENČNÍ UJEDNÁNÍ	10
7. ZDROJOVÝ KÓD A DOKUMENTACE	14
8. AKCEPTAČNÍ ŘÍZENÍ	15
9. ŠKOLENÍ	17
10. HELPDESK.....	17
11. NAHLÁŠENÍ INCIDENTU	18
12. SERVISNÍ MODELY	19
13. ÚČAST PODDODAVATELŮ.....	21
14. REALIZAČNÍ TÝM	21
15. KOMUNIKACE STRAN	22
16. SMLUVNÍ POKUTY.....	22
17. ZÁRUKA ZA JAKOST A PRÁVA Z VADNÉHO PLNĚNÍ	24
18. UKONČENÍ SMLUVNÍHO VZTAHU	25
19. ZMĚNY SMLOUVY A ZMĚNOVÉ ŘÍZENÍ	26
20. KYBERNETICKÁ BEZPEČNOST	27
21. OCHRANA OSOBNÍCH ÚDAJŮ	31
22. OCHRANA DŮVĚRNÝCH INFORMACÍ.....	32

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 Objednatелеm. 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 nikoliv však výlučně 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 Helpdesku, vytěžením e-mailu z e-mailového serveru Objednatele a jeho vložení do Helpdesku jako ticketu anebo ukončením telefonátu.
- 1.9. **Data** jsou jakékoliv údaje či informace vznikající v souvislosti s Plněním dle Smlouvy.
- 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:
- a. neobdržení podkladů a informací vyžádaných Dodavatelem, které jsou nezbytně nutné pro lokalizaci nebo replikaci Incidentu, od Objednatele;
 - b. 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);
 - c. 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. **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).
- 1.15. **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 dle příslušného Servisního modelu dle ZOP.
- 1.16. **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.
- 1.17. **FOSS licence** znamená Free Open Source Software licence.
- 1.18. **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).
- 1.19. **GUI** znamená grafické uživatelské rozhraní.
- 1.20. **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
- 1.21. **Hardware** znamená veškeré hmotné součásti počítačových systémů a veškeré související vybavení hmotné povahy spolu se vším příslušenstvím, a včetně veškeré související dokumentace.
- 1.22. **Informační či komunikační systém** znamená informační či komunikační systém kritické informační infrastruktury Objednatele ve smyslu § 2 b) ZKB nebo jiný informační či komunikační systém, na který se vztahuje ZKB.
- 1.23. **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 Helpdesku, 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

- 1.24. **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.
- 1.25. **ISDS** znamená informační systém datových schránek ve smyslu zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů.
- 1.26. **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*.
- 1.27. **Insolvenční zákon** znamená zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.
- 1.28. **IT prostředí Objednatele** znamená veškerý Hardware ve vlastnictví Objednatele a Software, ve vztahu k němuž je Objednatel nositelem potřebných oprávnění, nebo Hardware a Software využívaný Objednatelem na základě jiného právního titulu než Smlouvy. 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*.
- 1.29. **Kvalifikovaná osoba** je člen Realizačního týmu, kterým Dodavatel prokazoval splnění kvalifikačních předpokladů v rámci Veřejné zakázky.
- 1.30. **Kybernetický bezpečnostní incident** je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací podle § 7 ZKB v důsledku Kybernetické bezpečnostní události.
- 1.31. **Kybernetická bezpečností událost** je událost podle § 7 ZKB, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
- 1.32. **MD** znamená manday/člověkoden. Nestanoví-li Smlouva jinak, odpovídá jeden MD 8 MH.
- 1.33. **MH** znamená manhour/člověkohodinu. Nestanoví-li Smlouva jinak, odpovídá jedna MH 60 minutám práce.
- 1.34. **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.).
- 1.35. **NÚKIB** znamená Národní úřad pro kybernetickou a informační bezpečnost.
- 1.36. **Občanský zákoník** znamená zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
- 1.37. **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.
- 1.38. **Objednatel** je Správa železnic, státní organizace, IČO 70994234, se sídlem Praha 1 – Nové Město, Dlážděná 1003/7, PSČ 110 00, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. Zn. A 48384.
- 1.39. **Ohlašovatel** znamená osobu určenou Objednatelem, zpravidla uživatel Předmětu Smlouvy.

- 1.40. **Opční právo** představuje vyhrazenou změnu závazku v souladu s ustanovením § 100 odst. 3 ZZZV ze Smlouvy spočívající v pořízení dalšího obdobného Plnění od vybraného uchazeče v rámci zadávacího řízení Veřejné zakázky, tj. od Dodavatele dle Smlouvy.
- 1.41. **Osobní údaje** znamenají osobní údaje ve smyslu GDPR, včetně zvláštních kategorií osobních údajů ve smyslu článku 9 a rozsudků ve smyslu článku 10 GDPR.
- 1.42. **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.
- 1.43. **Paušální služby** jsou služby definované ve Smlouvě, jsou-li takové, zpravidla trvajících či opakujících se charakteru.
- 1.44. **Plnění** představuje plnění, které tvoří Předmět Smlouvy a k němuž se váže povinnost Dodavatele toto plnění Objednateli poskytovat. Plnění je blíže specifikované ve Smlouvě a v Příloze Smlouvy *Specifikace Plnění*.
- 1.45. **Poddodavatel** znamená kteroukoli třetí osobu realizující poddodávky pro Dodavatele v souvislosti s Předmětem Smlouvy. Poddodavatelé mohou být výslovně uvedeni v Příloze Smlouvy *Poddodavatelé*.
- 1.46. **Požadavek** znamená žádost ze strany Objednatele o službu nebo její podporu předanou v souladu se Smlouvou Dodavatel, 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
- 1.47. **Produkční prostředí** znamená IT prostředí Objednatele v ostrém provozu běžně přípustnou uživatelům Software, vyjma Testovacího prostředí.
- 1.48. **Provozovatel** znamená provozovatel ve smyslu § 2 písm. g) ZKB.
- 1.49. **Předmět Smlouvy** znamená dle typu Smlouvy Software nebo Hardware, přičemž parametry a vlastnosti Předmětu Smlouvy jsou blíže specifikovány v Příloze Smlouvy *Specifikace Plnění*.
- 1.50. **Převzetí poskytování plnění** je předání znalostí Dodavatel 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*.
- 1.51. **Příloha Smlouvy** je dokument, který tvoří nedílnou součást Smlouvy a obsahuje bližší specifikaci smluvních podmínek.
- 1.52. **Reakce** znamená kvalifikovanou a konkrétní odpověď na nahlášení Incidentu nebo na jiný požadavek, ve formě a způsobem dále definovanými v Příloze Smlouvy *Specifikace Plnění*.
- 1.53. **Reakční doba** je pro každou kategorii Incidentů uvedena v Příloze *Specifikace Plnění* a představuje dobu od Času nahlášení Incidentu do doručení Reakce Objednateli nebo Ohlašovatel.
- 1.54. **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.
- 1.55. **Recovery Point Objective (RPO)** je parametr, který vyjadřuje maximální ztrátu dat uživatelů při havárii systému a následné obnově.
- 1.56. **Recovery Time Objective (RTO)** je parametr, který vyjadřuje dobu nutnou k obnově chodu služby do akceptované úrovně provozu.
- 1.57. **Helpdesk** je Software provozovaný Dodavatelem nebo Objednatelem sloužící ke komunikaci Stran v průběhu provádění Plnění dle Smlouvy, v rámci něhož bude evidován postup Dodavatele při 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.

- 1.58. **Servisní model** je standardizovaný model provozu a podpory aplikace, systému nebo instance služby.
- 1.59. **SLA** znamená úroveň kvality Plnění představující dohodu o úrovni poskytovaných ICT služeb dle Smlouvy.
- 1.60. **Služby** jsou služby definované ve Smlouvě, jsou-li takové.
- 1.61. **Smluvní strany či Strany** jsou strany Smlouvy, tj. Objednatel a Dodavatel či jinak označené strany Smlouvy, jejíž součástí jsou tyto ZOP.
- 1.62. **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.
- 1.63. **Standardní Software** znamená Software, který je distribuován pod standardními licenčními podmínkami více třetím osobám. Mezi Standardní software patří:
- a. 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.
 - b. 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.
 - c. 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.
 - d. Software, o kterém to stanoví Smlouva.
- 1.64. **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.
- 1.65. **Testy** se rozumí provádění testovacího užívání Předmětu Smlouvy v Testovacím prostředí prostřednictvím simulace ostrého provozu v Produkčním prostředí a reálných situací a Testovacích scénářů.
- 1.66. **Testovací prostředí** znamená virtuální či fyzickou kopii Předmětu Smlouvy anebo IT prostředí Objednatele určenou Objednatelem k provádění Testů.
- 1.67. **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.
- 1.68. **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.
- 1.69. **Vada kategorie C** znamená vadu, která není Vadou kategorie A anebo B (např. špatná grafická úprava aplikace, špatný pravopis u nápovědy apod.).
- 1.70. **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.

- 1.71. **VKB** znamená vyhlášku 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.
- 1.72. **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.
- 1.73. **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).
- 1.74. **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.
- 1.75. **Významný dodavatel** znamená Dodavatel, který je Provozovatelem, jakož i každý, kdo s Objednatelem vstupuje do právního vztahu, který je významný z hlediska bezpečnosti Informačního či komunikačního systému ve smyslu § 2 odst. m) VKB.
- 1.76. **Významná změna** znamená změna, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko, např.
- a. změny pravidel ochranných systémů aplikačních firewallů a pravidel přepínání a směrování v sítích,
 - b. změny autentizačních mechanismů,
 - c. přidání, změna nebo odebrání služeb, informačních systémů/aplikací nebo ochranných systémů,
 - d. změny, které umožňují sdílení informací, služeb nebo zdrojů mimo provozní prostředí,
 - e. změny opatření pro zajištění bezpečnosti vzdáleného přístupu,
 - f. zavedení skriptů pro automatické přihlášení,
 - g. migrace dat do jiné Databáze, apod. ve smyslu § 2 odst. o) VKB.
- 1.77. **Zadávací dokumentace** je souborem dokumentů obsahujících zadávací podmínky, sdělované nebo zpřístupňované účastníkům zadávacího řízení na Veřejnou zakázku.
- 1.78. **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).
- 1.79. **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.
- 1.80. **ZKB** znamená zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.
- 1.81. **ZOP** znamená tento dokument, tedy zvláštní obchodní podmínky, které definují další parametry a upřesňují konkrétní podmínky a specifické požadavky Objednatele.
- 1.82. **ZZVZ** znamená zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

- 1.83. 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.
- 1.84. 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.
- 1.85. Pokud je uveden v ZOP čas, jedná se o čas SEČ.
- 1.86. 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. 20. 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 § 7 ZKB 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*. Podpisem Smlouvy Dodavatel prohlašuje, že měl možnost se seznámit s Interními předpisy Objednatele, jejichž seznam je uveden v Příloze Smlouvy *Seznam interních předpisů*, a dále bere na vědomí, že Interní předpisy mohou být přiměřeným způsobem jednostranně měněny či jinak doplňovány Objednatelem, přičemž každá nová verze je pro Dodavatele závazná vždy ode dne, kdy se s ní seznámil či měl prokazatelnou možnost se s nimi seznámit. Rozsah Interních předpisů může být Objednatelem jednostranně rozšířen o další dokumenty stanovující jeho interní procesy.

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 a změně oprávnění nakládat s těmito aktivy.
- 4.3. Dodavatel se zavazuje poskytovat v rámci Plnění veškerou součinnost nezbytnou k provádění Plnění, zejména, nikoliv však výlučně:
- a. poskytovat Plnění dle Smlouvy ve vysoké kvalitě s odbornou péčí odpovídající podmínkám sjednaným ve Smlouvě;
 - a. 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;
 - b. 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;
 - c. zajistit v souladu s podmínkami Smlouvy poskytnutí Dokumentace, a to rovněž vždy při každé Aktualizaci nebo jiné změně Předmětu smlouvy, nestanoví-li Objednatel jinak;
 - d. 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;
 - e. bez zbytečného odkladu oznamovat Objednateli všechny Kybernetické bezpečnostní události a Kybernetické bezpečnostní incidenty s potenciálním negativním dopadem na Objednatele;
 - f. 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;
 - g. 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 výzvu 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;
 - h. 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.

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 náležité souhlasy, 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 jakékoli 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 užít 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 užít veškerá Autorská díla a k výkonu práva vytěžovat a zužívat 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 zužitkovat 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. 1.63 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 Softwaru 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 užit 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 poskytnout Objednateli o zajištění oprávnění a veškerých souhlasů dle tohoto článku ZOP písemné prohlášení a na výzvu Objednatele 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 Objednatele, která je součástí Smlouvy, a dále vlastnosti a funkcionality uvedené ve specifikaci plnění Dodavatele (je-li taková), 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 nejméně čtrnáct (14) dní předem o termínu předání Předmětu Smlouvy či její části.

- 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 Helpdesku, 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 vady (zejména vady, pro které není vhodné dělení Vad dle ZOP -> např. některý HW měly-li být dle Návrhu řešení provedeny), 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 třiceti (30) kalendářních dnů 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**“ nezbujuje odpovědnosti Dodavatele odstranit vyznačené Vady či vady. Dodavatel je povinen takové Vady či vady odstranit ve lhůtě určené Objednatel, 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 není Objednatel povinen zaplatit 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 Objednatel, 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 odstavce 8.5 ZOP.

8.5.2. Řádné dodání Hardware bude potvrzeno předávacím protokolem podepsaným 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. 20. ZOP. Tuto skutečnost je povinen na vyžádání Objednateli prokázat.

10. **HELPDESK**

10.1. Dodavatel se zavazuje:

10.1.1. nejpozději v den účinnosti Smlouvy založit a po celou dobu trvání Smlouvy udržovat v provozu Helpdesk (včetně úhrady případných licenčních poplatků za aplikaci Helpdesk) a udělit náležitá oprávnění k přístupu do Helpdesku, a to v počtu přístupů pro Ohlašovatele dle určení Objednatele. Helpdesk bude fungovat prostřednictvím webové adresy;

nebo

10.1.2. po celou dobu trvání Smlouvy užívat Helpdesk provozovaný Objednatelem.

10.2. Provozovatele Helpdesku stanoví Smlouva. Pokud Smlouva provozovatele Helpdesku nestanoví, má se za to, že provozovatelem Helpdesku je Dodavatel. V případě, že provozovatelem bude Objednatel, poskytne Dodavateli nezbytnou součinnost k řádnému užívání Helpdesku včetně případného poskytnutí licencí.

10.3. Dodavatel se zavazuje zajistit Helpdesk prostřednictvím přímého přístupu do Helpdesku na webové adrese určené Dodavatelem/Objednatelem dle provozních podmínek aplikace Helpdesk, případně prostřednictvím přímého datového propojení Helpdesků 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) vždy zároveň 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 Helpdesk v rámci příslušného režimu začíná rovněž v 7:00).

10.5. Helpdesk 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 Helpdesk provozován Dodavatelem musí být zabezpečen tak, aby odpovídal požadavkům vyplývajícím ze ZKB a Interních předpisů. Výstupem z Helpdesku je záznam o veškerých úkonech Helpdesku ve formě přehledného logu, jež umožňuje vyhledávání a uchovávání záznamů tak, aby byly naplněny požadavky ZKB a Interních předpisů na takové záznamy.

10.6. Helpdesk bude dostupný pouze pro Objednatele a Ohlašovatele.

10.7. Nestanoví-li Smlouva jinak, je Dodavatel povinen nezávisle na Helpdesk mít nejpozději k okamžiku nabytí účinnosti Smlouvy zřízenou elektronickou adresu a telefonní linku a tuto adresu a telefonní číslo linky sdělit Objednateli, 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 Helpdesk dle odst. 10.3 ZOP.

11. NAHLÁŠENÍ INCIDENTU

11.1. Hlášení o Incidentu Dodavateli bude provedeno Ohlašovatelem, a to přímým zadáním Incidentu do Helpdesku (vytvoření ticketu v Helpdesku, 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 Objedatele vyrozuměl, a to nejpozději v době určené na zpracování Incidentu dle určeného Servisního modelu, v takovém případě je Incident dle 11.3 ZOP nahlášen okamžikem doplnění požadované informace.
- 11.3. Je-li Incident nahlášován prostřednictvím Helpdesku, pak se za Čas nahlášení Incidentu považuje čas vytvoření ticketu v Helpdesku. 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 Helpdesku. 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 Helpdesku 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.

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 podmínky, 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:

$$Doba\ výpadku = \sum_{i=1}^n T_i$$

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:

- dočasná vyřazení Hardware z provozu na základě předchozí dohody Objednatele a Dodavatele (odstávka),
- pravidelná vyřazení Hardware z provozu Dodavatelem v časech sjednaných ve Smlouvě nebo její příloze (servisní okna)
- 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. ÚČAST PODDODAVATELŮ

- 13.1. 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.
- 13.2. 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 nebudou jednat v rozporu s ujednáními Smlouvy a jejími Přílohami, kterou mezi sebou uzavřeli Dodavatel a Objednatel.
- 13.3. 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. REALIZAČNÍ TÝM

- 14.1. 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.
- 14.2. 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.
- 14.3. 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.
- 14.4. 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.
- 14.5. 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.

15. KOMUNIKACE STRAN

- 15.1. Objednatel a Dodavatel si pro vzájemnou komunikaci ohledně Smlouvy zvolí kontaktní osoby, jejichž seznam uvedou ve Smlouvě.
- 15.2. Jsou-li naplněny podmínky odst. 20.1. ZOP, vykonává kontaktní osoba na straně Dodavatele povinnosti kontaktní osoby pro kybernetickou bezpečnost vyplývající z článku 20. 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 20. ZOP).
- 15.3. Strany si navzájem oznámí jakékoliv změny v kontaktních osobách, přičemž taková změna je účinná uplynutím sedmého (7.) dne po jejím doručení.
- 15.4. 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.

16. NÁHRADA ŠKODY A SMLUVNÍ POKUTY

- 16.1. 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. 16.2. ZOP, pokud nejsou ve Smlouvě výslovně zakotveny jiné sankce, které vylučují aplikaci odst. 16.2. ZOP. Ustanovení § 2050 Občanského zákoníku se nepoužije. Objednatel je však oprávněn uplatnit po Dodavateli nárok na náhradu škody pouze do celkové souhrnné výše sta (100) procent Ceny. Pro vyloučení všech pochybností se limitace dle předchozí věty vztahuje i na souhrnnou výši smluvních pokut. Tímto není dotčena odpovědnost za škodu způsobenou úmyslně či hrubou nedbalostí.
- 16.2. Objednateli vzniká vůči Dodavateli právo na zaplacení smluvní pokuty:
 - a. poruší-li Dodavatel svoji povinnost řádně a včas provést Plnění ve výši 0,05 % z Ceny 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 řádně a včas provést jakoukoliv část Plnění ve výši 0,05 % z ceny takové části Plnění za každý započatý den prodlení až do řádného splnění této povinnosti; v případě, že by smluvní pokuty dle odst. 16.2. písm. a. a písm. b. ZOP měly běžet vůči Dodavateli zároveň, vzniká za takové období Objednateli nárok pouze dle odst. 16.2. písm. a. ZOP. Plnění se považuje pro účely této smluvní pokuty za řádně a včas provedené i v případě, že bylo akceptováno s výhradou;
 - c. poruší-li Dodavatel svoji povinnost dle odst. 8.1.11 ZOP ve výši 0,01 % z Ceny (případně ceny části Plnění, jedná-li se o akceptaci dílčí části Plnění) za každý započatý den prodlení až do řádného splnění této povinnosti;
 - d. 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;
 - e. 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;
 - f. poruší-li Dodavatel některou z povinností týkající se účasti Poddodavatelů anebo Realizačního týmu, ve výši 2 % z Ceny za každé jednotlivé porušení povinnosti;
 - g. 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;
- h. 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;
- i. 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;
- j. 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 odst. 12.8 ZOP
Od 2 (včetně) do 5 %	15 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle odst. 12.8 ZOP
Od 5 (včetně) do 10 %	25 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle odst. 12.8 ZOP
Od 10 % (včetně) a více	50 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle odst. 12.8 ZOP

- k. v případě prodlení 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;
 - l. ve výši a za podmínek dle článku 20. ZOP v oblasti kybernetické bezpečnosti;
 - m. ve výši a za podmínek dle článku 21. ZOP v oblasti ochrany osobních údajů;
 - n. ve výši a za podmínek dle článku 22. ZOP v oblasti ochrany Důvěrných informací; nebo
 - o. poruší-li Dodavatel svoji povinnost dle odst. 13.2. ZOP nebo 13.3. ZOP, ve výši 2 % z Ceny za každé jednotlivé porušení.
- 16.3. Pro smluvní pokuty stanovené v odst. 16.2. písm. 16.2.g. a 16.2.h. 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.
- 16.4. Zaplacením smluvních pokut není dotčeno právo Objednatele na náhradu Újmy v plném rozsahu.

- 16.5. Smluvní pokuta je splatná do 30 dnů ode dne doručení písemné výzvy Objednatele k jejímu uhrazení. Objednatel je oprávněn započíst nárok na zaplacení smluvní pokuty, i pokud ještě není splatný, proti jakémukoliv nároku Dodavatele na peněžitě plnění vyplývajícímu ze Smlouvy.
- 16.6. Za každý den prodlení s úhradou Smluvní pokuty je Objednatel oprávněn požadovat po Dodavateli úhradu úroků z prodlení ve výši stanovené obecně závaznými právními předpisy.

17. ZÁRUKA ZA JAKOST A PRÁVA Z VADNÉHO PLNĚNÍ

17.1. Společná ustanovení

- 17.1.1. Dodavatel uděluje Objednateli záruku za jakost Plnění a všech jeho částí na dobu dvou (2) let ode dne akceptace výstupu Plnění.
- 17.1.2. 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.
- 17.1.3. 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.
- 17.1.4. Dodavatel neodpovídá za vady, pokud byly způsobeny zásahem do takových výstupů Plnění ze strany Objednatele nebo jím pověřené osoby, případně jiných dodavatelů Objednatele.
- 17.1.5. Objednatel je povinen oznámit vady Plnění Dodavateli prostřednictvím Helpdesku, nebude-li Stranami dohodnuto jinak.
- 17.1.6. Dodavatel neodpovídá za vady Plnění vzniklé:
- provozováním Díla Objednatelem v rozporu s Dokumentací;
 - neoprávněným nebo neodborným zásahem či nesprávným užitím Díla Objednatelem;
 - vadami IT prostředí Objednatele.

17.2. Záruka vztahující se k Softwaru

- 17.2.1. Pokud výrobce Standardního Software poskytuje záruku za jakost, pak Dodavatel postupuje takovou záruku za jakost Objednateli. To nezabývá Dodavatele povinností poskytnout Objednateli vlastní záruku za jakost ve smyslu tohoto článku.
- 17.2.2. 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 Objednatelem
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

¹ Lhůta je stanovena v hodinách.

² Lhůta je stanovena ve dnech.

³ Lhůta je stanovena ve dnech.

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

17.3. Záruka vztahující se k Hardwaru

- 17.3.1. 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.
- 17.3.2. 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.
- 17.3.3. V případě, že odstranění reklamovaných vad bude trvat déle než dva (2) Pracovní dny, zavazuje se Dodavatel poskytnout Objednateli náhradní Hardware či jinou náhradní hmotnou věc po dobu trvání odstranění reklamované vady, nedohodnou-li se Strany jinak.

18. UKONČENÍ SMLUVNÍHO VZTAHU

18.1. Obecně k odstoupení od Smlouvy:

- 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 Objednatel.
- 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.
- Dodavatel nemá právo odstoupit od Smlouvy v případě nevhodných příkazů Objednatele či poskytnutí nevhodné věci Objednatel dle § 2595 Občanského zákoníku.

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

- 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.
- Dodavatel je v prodlení s Plněním dle Smlouvy déle než 60 dnů, a to i bez nutnosti zaslání předchozího upozornění.
- 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:
 - Dodavatel je opakovaně v prodlení s prováděním Plnění dle Smlouvy;
 - prohlášení Dodavatele učiněné na základě Smlouvy se ukáže jako nepravdivé;
 - Dodavatel bez upozornění a relevantního odůvodnění nepoužil k Plnění člena Realizačního týmu, ač k tomu byl povinen; nebo
 - Dodavatel poruší některou z povinností uvedenou v čl. 20. ZOP opakovaně nebo závažným způsobem.

⁴ Lhůta je stanovena v hodinách.

⁵ Lhůta je stanovena ve dnech.

⁶ Lhůta je stanovena ve dnech.

- 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. 13.2. ZOP nebo odst. 13.3. ZOP nebo Poddodavatel Dodavatele poruší některou z povinností vyplývajících z požadavků dle odst. 13.2. 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 splynutí).
 - 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.
- 18.3. 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 nenapravil 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 nenapraví.
- 18.4. Dodavatel není oprávněn odstoupit od Smlouvy ve vztahu k části Plnění, za kterou mu již bylo Objednatelem zapláceno.

19. ZMĚNY SMLOUVY A ZMĚNOVÉ ŘÍZENÍ

- 19.1. 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.
- 19.2. 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.
- 19.3. 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.

20. KYBERNETICKÁ BEZPEČNOST

- 20.1. Tento článek se uplatní v případě, kdy tak výslovně stanoví Smlouva, pokud je Předmětem Smlouvy Informační či komunikační systém, pokud má Plnění dopad na Informační či komunikační systém, nebo pokud je Smlouva uzavřena s Významným dodavatelem či Provozovatelem. Zda je Dodavatel Významným dodavatelem či Provozovatelem, stanoví Smlouva. Na jiné Smlouvy a vztahy se neuplatní, ledaže se Dodavatel stane Významným dodavatelem či Provozovatelem v průběhu plnění Smlouvy. V takovém případě se na něj čl. 20. uplatní v rozsahu v jakém to po něm lze spravedlivě požadovat.
- 20.2. Dodavatel se při plnění Smlouvy zavazuje postupovat v souladu se ZKB, VKB a souvisejícími právními předpisy, dodržovat zásady bezpečnosti informací, Interní předpisy Objednatele a z nich vyplývající povinnosti týkající se bezpečnostních opatření, provozní řády prostor Objednatele, rozhodnutí, 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 ZKB a VKB, včetně upozorňování a zajištění hlášení Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů Objednateli, jakož i další bezpečnostní politiky, metodiky a postupy, se kterými byl Objednatelem seznámen.
- 20.3. 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. Kontaktní osoba Dodavatele je povinna splnění povinnosti dle předchozí věty Objednateli potvrdit do 30 dnů od uzavření Smlouvy. 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.
- 20.4. Není-li ve Smlouvě ujednáno jinak, je Dodavatel povinen vytvořit, pravidelně aktualizovat a vynucovat vůči osobám podílejícím se, byť i nepřímo, na Předmětu Smlouvy:
- a. politiku řízení přístupu, na základě které přidělí oprávnění k výkonu činností jednotlivým rolím svých fyzických osob (přístup pro více osob na jednom účtu je nežádoucí a lze pouze se souhlasem Objednatele) podílejících se na plnění Smlouvy (zaměstnanci, programátoři podnikatelé apod.) 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; 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;
 - b. politiku zvládání Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů obsahující činnosti, role, odpovědnosti a pravomoci k rychlému a účinnému zvládání Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů.
- 20.4.2. Kontaktní osoba Dodavatele je povinna před započatím Plnění, nejpozději však do 30 dnů od uzavření Smlouvy, určit a popsat veškerá dotčená primární i podpůrná aktiva na straně Dodavatele potřebná pro plnění Smlouvy. 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. Dodavatel je povinen řídit rizika spojená s Plněním dle Smlouvy minimálně dle standardů požadovaných normou ISO 27001 a případně dle Interních předpisů, pokud obsahují závazná pravidla pro řízení rizik. Dodavatel je povinen bez zbytečného odkladu po uzavření Smlouvy kontaktní osobu Objednatele informovat o způsobu řízení rizik a o zbytkových rizicích souvisejících s Plněním Smlouvy a následně v pravidelných intervalech informovat o změnách.

- 20.5. Dodavatel je povinen zaslat kontaktní osobě Objednatele bez zbytečného odkladu všechna hlášení o událostech, která mají charakter Kybernetické bezpečnostní události nebo 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 této Kybernetické bezpečnostní události anebo Kybernetickému bezpečnostnímu incidentu, případně zvolí jinou formu dohodnutou mezi Objednatelem a Dodavatelem určenou ke včasnému hlášení Kybernetické bezpečnostní události nebo Kybernetického bezpečnostního incidentu a/nebo již učiněných opatření. Dodavatel je povinen veškeré Kybernetické bezpečnostní události a Kybernetické bezpečnostní incidenty zaznamenávat a po nezbytně dlouhou dobu uchovávat. Dodavatel je povinen poskytnout Objednateli veškerou nezbytnou součinnost k detekci, vyhodnocení či řešení Kybernetické bezpečnostní události nebo Kybernetického bezpečnostního incidentu, a to včetně případné realizace nutných opatření dle pokynů Objednatele. 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 jednotlivou Kybernetickou bezpečnostní událost nebo Kybernetický bezpečnostní incident jedním z následujících způsobů:
- a. e-mailem na adresu kontaktní osoby uvedené ve Smlouvě; nebo
 - b. telefonicky na telefonní číslo kontaktní osoby uvedené ve Smlouvě; nebo
 - c. ohlášením do Helpdesku Objednatele.
- 20.6. Dodavatel je povinen pravidelně alespoň čtvrtletně předkládat Objednateli zprávu o počtu a druhu útoků a Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů, které zaznamenal ve spojení s Plněním a/nebo Předmětem Smlouvy.
- 20.7. Dodavatel se zavazuje poskytnout Objednateli veškerou součinnost nezbytnou k tomu, aby Objednatel řádně naplňoval právní povinnosti stanovené ZKB, VKB a Interními předpisy. Zejména se Dodavatel zavazuje poskytnout Objednateli součinnost směřující k zavedení a provádění bezpečnostních opatření podle ZKB, VKB a Interních předpisů a řešení Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů. Jestliže Dodavatel při plnění Smlouvy zjistí či jako odborník mohl a měl zjistit rozpor ustanovení Interních předpisů se ZKB, VKB anebo rozhodnutím či jiným pokynem NÚKIB v souladu se ZKB, je povinen takový rozpor Objednateli neprodleně ohlásit a poskytnout Objednateli součinnost k jeho odstranění.
- 20.8. Dodavatel bere na vědomí, že v rámci provádění Plnění může být podroben Interním předpisům Objednatele či jeho pokynům v oblasti řízení kontinuity činností, zejména může být zahrnut do havarijních plánů, úkolů při aktivaci řízení kontinuity činností, bezpečnostní politiky apod., a to v rozsahu, v jakém lze po Dodavateli spravedlivě požadovat s ohledem na předmět plnění.
- 20.9. 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.
- 20.10. 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.
- 20.11. Objednatel má právo prostřednictvím určených osob provádět v pravidelných intervalech (1x ročně, 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 ZKB a/nebo VKB, audit kybernetické bezpečnosti, tj. dodržování bezpečnosti informací dle Interních předpisů, ZKB a VKB 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:

- a. nehlášená návštěva u Dodavatele v místě umístění členů Realizačního týmu či jiných osob podílejících se na plnění Smlouvy v rozsahu tří (3) hodin vždy nejčastěji čtyřikrát (4x) za rok; a
- b. nehlášený telefonát 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.

20.12. 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 vytčeného 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.

20.13. 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 a bezodkladně informovat Objednatele do 7 dnů.

20.14. Je-li součástí Předmětu 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 NÚKIB.

20.15. 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:

- a. provádět analýzy topologie sítě či skenování aktivních částí Předmětu Plnění; a
- b. realizovat bezpečnostní opatření pro odstranění nebo blokování síťových spojení, která neodpovídají požadavkům na ochranu integrity komunikační sítě.

20.15.2. Významný dodavatel je dále povinen:

- a. poskytnout Objednateli veškeré potřebné informace a součinnost v procesu řízení a evidence změn v souladu s § 11 VKB 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 dokumentace, souvisejícím testováním, zajištění možnosti navrácení do původního stavu a provedení dalších činností dle VKB);
- b. strpět a poskytnout Objednateli veškerou potřebnou součinnost v případě nutnosti provést penetrační testování;
- c. zpracovat a pravidelně aktualizovat bezpečnostní dokumentaci v rozsahu stanoveném ve Smlouvě;
- d. průběžně detekovat známé zranitelnosti dotčených aktiv Objednatele a bezodkladně na ně upozorňovat Objednatele; a
- e. vést v elektronické formě provozní deník obsahující veškeré podstatné okolnosti související s plněním povinností Dodavatele dle článku 20. ZOP a/nebo Plněním, provozní události důležitých aktiv a relevantní záznamy o plnění povinností Dodavatele dle článku 20. ZOP a zpřístupnit jej Objednateli prostřednictvím zabezpečeného vzdáleného přístupu, není-li ve Smlouvě ujednáno jiný způsob; v provozním deníku Významný dodavatel dále do 20. dne následujícího měsíce uvede výstup z monitoringu dostupnosti, důvěrnosti a integrity aktiv

Objednatele, se kterými pracuje v rámci plnění Smlouvy, prováděného nejméně jedenkrát měsíčně a vyhodnocovaného vždy k 10. dni následujícího měsíce.

20.15.3. Provozovatel je dále povinen:

- a. provádět pravidelné zálohy dat a programového vybavení vztahujících se k Plnění dle Smlouvy, zabezpečit je vhodnými prostředky proti neoprávněným přístupům nebo jejich ztrátě a v pravidelných intervalech testovat funkčnost těchto záloh, nejméně jedenkrát za měsíc, není-li ve Smlouvě ujednáno jinak;
- b. plnit další povinnosti vyplývající pro Provozovatele ze ZKB a VKB.

20.16. Pokud Objednatel zjistí, že Dodavatel postupuje v rozporu s tímto článkem, je Objednatel v takovém případě oprávněn požadovat 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 Smlouvou 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. Jestliže Dodavatel včas neodstraní nedostatky ve smyslu předchozí věty tohoto odstavce nebo se jedná o porušení povinnosti (bez ohledu na jeho závažnost), pak je Objednatel oprávněn od Smlouvy odstoupit.

20.17. 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 Kybernetické bezpečnostní události anebo 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.

20.18. Dodavateli nenáleží za plnění povinností souvisejících s bezpečností informací ve smyslu článku 20. ZOP jakákoliv další odměna, resp. taková odměna je součástí Ceny.

20.19. Objednatel je oprávněn požadovat na Dodavateli zaplacení smluvní pokuty:

- a. za každý den prodlení při zavedení bezpečnostních opatření podle ZKB, VKB, 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 ZKB, VKB, 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 Kybernetické bezpečnostní události nebo Kybernetického bezpečnostního incidentu;
- d. ve výši 2 % z Ceny za každý případ neumožnění nebo odepření provedení kontroly a auditu kybernetické bezpečnosti ve smyslu článku 20. ZOP;
- e. ve výši 5 % z Ceny za každý případ porušení článku 20. 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 20. ZOP, dané porušení nebylo odstraněno a negativní následek porušení povinnosti stále trvá; a
- g. ve výši 1 % z Ceny za každý případ jiného porušení článku 20. ZOP neuvedeného výše.

21. OCHRANA OSOBNÍCH ÚDAJŮ

- 21.1. 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.
- 21.2. 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.
- 21.3. 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.
- 21.4. 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.
- 21.5. 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.
- 21.6. 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.
- 21.7. 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.
- 21.8. 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.
- 21.9. 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.
- 21.10. 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.
- 21.11. 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.

- 21.12. 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.

22. OCHRANA DŮVĚRNÝCH INFORMACÍ

- 22.1. 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.
- 22.2. Dodavatel se zavazuje použít Důvěrné informace pouze k plnění svých povinností vyplývajících ze Smlouvy. Dodavatel nesmí použít Důvěrné informace k jinému účelu.
- 22.3. 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.
- 22.4. 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 jakémkoliv databázi, počítačovém programu, úložišti či na datovém nosiči, vyjma případů, kdy je takové uchování Důvěrných informací nezbytné pro účel vyplývající ze Smlouvy.
- 22.5. 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.
- 22.6. 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.
- 22.7. 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. 22.6. ZOP
 - b. ve výši 100 000 Kč za každé jednotlivé jednání, které představuje porušení jakékoli z povinností stanovených v odst. 22.6. ZOP.

Obchodní podmínky ke Kupní smlouvě

OBSAH OBCHODNÍCH PODMÍNEK

Obchodní podmínky ke Kupní smlouvě	1
ČÁST 1 - ÚVODNÍ USTANOVENÍ	2
ČÁST 2 - NÁVRH NA UZAVŘENÍ KUPNÍ SMLOUVY	2
ČÁST 3 - PŘEDMĚT KOUPĚ	3
ČÁST 4 - CENA A PLATEBNÍ PODMÍNKY	3
ČÁST 5 - MÍSTO DODÁNÍ PŘEDMĚTU KOUPĚ	5
ČÁST 6 - DOBA DODÁNÍ PŘEDMĚTU KOUPĚ	5
ČÁST 7 - PŘEPRAVA PŘEDMĚTU KOUPĚ	5
ČÁST 8 - DALŠÍ DODACÍ PODMÍNKY	6
ČÁST 9 - PŘEDÁNÍ A PŘEVZETÍ PŘEDMĚTU KOUPĚ	6
ČÁST 10 - PŘECHOD VLASTNICKÉHO PRÁVA A NEBEZPEČÍ ŠKODY	7
ČÁST 11 - VADY PLNĚNÍ A ZÁRUKA	7
ČÁST 12 - UPLATNĚNÍ PRÁV Z VADNÉHO PLNĚNÍ	7
ČÁST 13 - PODMÍNKY ODSTRANĚNÍ VAD	8
ČÁST 14 - SANKCE	9
ČÁST 15 - Odstoupení od kupní smlouvy	9
ČÁST 16 - OSTATNÍ UJEDNÁNÍ	10

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. **Kupující** – 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.
 - 1.5. **Prodávající** – osoba uvedená v Kupní smlouvě jako Proávající.
 - 1.6. **Smluvní strany** – Kupující a Proávající.
 - 1.7. **Smluvní strana** – Kupující nebo Proávající dle smyslu ujednání.
 - 1.8. **Kupní smlouva** – smlouva uzavřená mezi Smluvními stranami, která odkazuje na Obchodní podmínky.
 - 1.9. **Obchodní podmínky** – text těchto obchodních podmínek.
 - 1.10. **Předmět koupě** – věc nebo věci specifikované v Kupní smlouvě.
 - 1.11. **Kupní cena** – cena Předmětu koupě sjednaná v Kupní smlouvě.
 - 1.12. **Doklady** – veškeré listiny, které se k Předmětu koupě vztahují a které jsou třeba k jeho převzetí a užívání; veškerá rozhodnutí, sdělení, souhlasy, povolení či jiné výsledky úkonů orgánů státní správy či jiných subjektů, nezbytné dle právních předpisů k prodeji a dodání Předmětu koupě Kupujícímu; veškeré listiny (vyjma Výzvy k úhradě) které je Proávající dle Kupní smlouvy povinen předat Kupujícímu; veškeré Doklady je Proávající povinen předat Kupujícímu v českém jazyce nebo v originále a českém překladu.
 - 1.13. **Obalový materiál** – palety, dřevěné desky či jiné věci, které slouží pro potřeby přepravy nebo ochrany Předmětu koupě. Dle kontextu Kupní smlouvy se rozumí Obalovým materiálem též jednotlivý kus palety, dřevěné desky nebo jiné věci.
 - 1.14. **Dodací list** – list osvědčující dodání, jehož minimální náležitosti jsou uvedeny v části Předání a převzetí Předmětu koupě.
 - 1.15. **Záruční doba** – doba, do jejíhož uplynutí je Kupující oprávněn uplatňovat práva z vad plnění poskytnutého Proávajícím na základě Kupní smlouvy; Záruční doba činí 24 měsíců.
 - 1.16. **Výzva k úhradě** – daňový doklad, je-li Proávající povinen dle ZoDHP uhradit v souvislosti s dodáním Předmětu koupě nebo jeho části DPH, nebo faktura, pokud Proávající v souvislosti s dodáním Předmětu koupě nebo jeho části není dle ZoDHP povinen uhradit DPH.
 - 1.17. **CTD** – Centrum techniky a diagnostiky, jako organizační jednotka Kupujícího.
2. Kupní smlouva se řídí těmito Obchodními podmínkami, pokud tak Kupní smlouva stanoví, nebo pokud z ní jiným způsobem vyplývá, že tyto Obchodní podmínky jsou přílohou či součástí Kupní smlouvy, nebo pokud Kupní smlouva na Obchodní podmínky jiným způsobem odkáže.

ČÁST 2 - NÁVRH NA UZAVŘENÍ KUPNÍ SMLOUVY

3. Odpověď Smluvní strany na návrh na uzavření Kupní smlouvy učiněný druhou Smluvní stranou, která vymezuje obsah návrhu jinými slovy nebo která obsahuje jakékoliv, byť nepodstatné, dodatky, odchylky, výhrady nebo omezení není přijetím návrhu.
4. I pozdní přijetí návrhu na uzavření Kupní smlouvy má účinky včasného přijetí, pokud navrhuje Smluvní strana bez zbytečného odkladu alespoň ústně vyrozumí druhou Smluvní stranu, že přijetí považuje za včasné, nebo pokud se začne chovat ve shodě s návrhem.
5. Plyne-li z písemnosti, která vyjadřuje přijetí návrhu na uzavření Kupní smlouvy, že byla odeslána za takových okolností, že by došla navrhuje Smluvní straně včas, kdyby její přeprava probíhala obvyklým způsobem, má pozdní přijetí účinky včasného přijetí, ledaže

- navrhující Smluvní strana bez odkladu vyrozumí alespoň ústně druhou Smluvní stranu, že považuje návrh za zaniklý.
6. Bez ohledu na jakékoliv okolnosti nelze přijmout návrh na uzavření Kupní smlouvy tak, že se Smluvní strana, jíž je návrh určen, podle návrhu zachová.
 7. **Odkáží-li Smluvní strany v návrhu na uzavření Kupní smlouvy i v přijetí návrhu na obchodní podmínky, které si odporují, je Kupní smlouva přesto uzavřena s obsahem určeným v tom rozsahu, v jakém obchodní podmínky nejsou v rozporu; to platí i v případě, že to obchodní podmínky vylučují. Vyloučí-li to některá ze Smluvních stran nejpozději bez zbytečného odkladu po výměně projevů vůle, Kupní smlouva uzavřena není.**
 8. Kupní smlouva může být uzavřena pouze v písemné podobě.

ČÁST 3 - PŘEDMĚT KOUPE

9. Prodávající se zavazuje, že Kupujícímu odevzdá Předmět koupě, a umožní mu k němu nabýt vlastnické právo, a Kupující se zavazuje, že Předmět koupě převezme a zaplatí Prodávajícímu Kupní cenu a příslušnou DPH, je-li Prodávající povinen dle ZoDHP uhradit v souvislosti s dodáním Předmětu koupě nebo jeho části DPH.
10. Prodávající je povinen dodat Předmět koupě nový, v jakosti a provedení uvedeném v Kupní smlouvě a zároveň
 - 10.1. tak, aby jej bylo možno použít podle účelu Kupní smlouvy, je-li v ní účel vyjádřen,
 - 10.2. v jakosti a provedení dle odstavce 12 v rozsahu, ve kterém není v rozporu s jakostí a provedením sjednaným v Kupní smlouvě.
11. Je-li jakost či provedení zároveň určeno vzorkem nebo předlohou, musí Předmět koupě odpovídat jakostí nebo provedením vzorku nebo předloze. Liší-li se jakost nebo provedení určené v Kupní smlouvě a vzorek nebo předloha, rozhoduje Kupní smlouva. Určuje-li Kupní smlouva a vzorek nebo předloha jakost nebo provedení rozdílně, nikoliv však rozporně, musí Předmět koupě odpovídat Kupní smlouvě i vzorku nebo předloze.
12. Neurčuje-li Kupní smlouva jakost a provedení Předmětu koupě, je Prodávající povinen dodat Předmět koupě v takové jakosti a provedení,
 - 12.1. jež odpovídá vlastnostem, které Prodávající nebo výrobce popsal nebo které Kupující očekával s ohledem na povahu Předmětu koupě a na základě reklamy jimi prováděné,
 - 12.2. jež se hodí k účelu vyplývajícemu z Kupní smlouvy a není-li v ní vyjádřen pak k účelu, ke kterému se Předmět koupě obvykle používá,
 - 12.3. jež vyhovuje požadavkům právních předpisů.
13. Dodá-li Prodávající Kupujícímu větší množství Předmětu koupě, než bylo sjednáno, je Kupující oprávněn část přesahující sjednané množství odmítnout.

ČÁST 4 - CENA A PLATEBNÍ PODMÍNKY

14. Kupní cena zahrnuje veškeré náklady Prodávajícího spojené se splněním jeho povinností vyplývajících z Kupní smlouvy. Kupující není povinen hradit v souvislosti s Kupní smlouvou žádné jiné finanční částky, než Kupní cenu a případně příslušnou DPH, není-li uvedeno jinak (tím není dotčeno právo Prodávajícího na případnou úhradu smluvní pokuty, úroků z prodlení, či jiných sankcí, a právo na náhradu škody způsobené Kupujícím).
15. Kupní cena zahrnuje zejména
 - 15.1. náklady na pojištění Předmětu koupě, je-li Prodávající povinen Předmět koupě dle Kupní smlouvy pojistit,
 - 15.2. náklady na ověření jakosti, je-li dle Kupní smlouvy požadováno, včetně nákladů na veškeré související úkony (např. doprava),
 - 15.3. náklady na zabalení Předmětu koupě, včetně nákladů na nevratný Obalový materiál,
 - 15.4. náklady na dopravu Předmětu koupě Kupujícímu a jeho vyložení,

- 15.5. náklady na získání jakýchkoliv rozhodnutí, sdělení, souhlasů, povolení či jiných výsledků úkonů orgánů státní správy či jiných subjektů, nezbytných dle právních předpisů k prodeji a dodání Předmětu koupě Kupujícímu,
- 15.6. náklady na vytvoření, získání či překlad Dokladů a jejich dodání Kupujícímu,
- 15.7. cenu za udělení nebo převod licenčních oprávnění k Předmětu koupě nebo Dokladům, nebo jakékoliv jejich části na Kupujícího, jsou-li předmětem duševního vlastnictví, přičemž v takovém případě cena za takové licenční oprávnění činí 5% z Kupní ceny,
- 15.8. zaškolení obsluhy Předmětu koupě, je-li dle Kupní smlouvy nebo povahy Předmětu koupě zaškolení třeba,
- 15.9. náklady na zkušební provoz Předmětu koupě, bude-li Kupní smlouvou vyžadován.
16. Je-li Prodávající povinen dle ZoDHP uhradit v souvislosti s dodáním Předmětu koupě nebo jeho části DPH, je Kupující povinen Prodávajícímu takovou DPH uhradit vedle Kupní ceny.
17. Konečné finanční částky na fakturách/daňových dokladech nesmí být zaokrouhlovány na celé Kč. Kupující nebude akceptovat zaokrouhlení a haléřové vyrovnání v případě uvedení na faktuře/daňovém dokladu nebude hradit.
18. Stane-li se prodávající nespolehlivým plátcem nebo daňový doklad prodávajícího bude obsahovat číslo bankovního účtu, na který má být plněno, aniž by bylo uvedeno ve veřejném registru spolehlivých účtů, je Kupující oprávněn z finančního plnění uhradit daň z přidané hodnoty přímo místně a věcně příslušnému správci daně prodávajícího.
19. Kupní cenu a případnou DPH je Kupující povinen uhradit Prodávajícímu do 30 dnů ode dne převzetí Předmětu koupě; má-li být dle Kupní smlouvy proveden též zkušební provoz, pak do 30 dnů ode dne úspěšného ukončení zkušebního provozu, nastane-li den skončení zkušebního provozu později než převzetí Předmětu koupě Kupujícím.
20. Kupní cena a případná DPH je uhrazena dnem jejich odepsání z bankovního účtu Kupujícího.
21. Prodávající vyúčtuje Kupujícímu Kupní cenu a případnou DPH Výzvou k úhradě.
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 ZoDHP a náležitosti stanovené v § 435 Občanského zákoníku.
24. Výzva k úhradě musí vždy obsahovat číslo Kupní smlouvy, její přílohou musí být vždy jedno vyhotovení Dodacího listu potvrzeného Kupujícím.
25. Výzvu k úhradě je Prodávající povinen doručit Kupujícímu nejpozději 15 dnů před uplynutím doby uvedené v odstavci 19 Obchodních podmínek.
26. Výzvy k úhradě, vč. všech příloh, budou Kupujícímu 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 Kupujícího <https://www.spravazeleznic.cz/kontakty/podatelna>.
- Kupující 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. Splatnost Výzvy k úhradě musí být stanovena tak, aby nenastala dříve, než uplyne doba stanovená v odstavci 19 Obchodních podmínek.
28. Stanoví-li Výzva k úhradě splatnost delší, než je jako minimální stanovena v předchozím odstavci, je Kupující oprávněn uhradit Kupní cenu a případnou DPH ve lhůtě splatnosti určené ve Výzvě k úhradě.
29. Dodává-li Prodávající Předmět koupě v souladu s Kupní smlouvou po částech, je oprávněn vystavit Výzvu k úhradě dodávané části Předmětu koupě poté, co Kupující převezme příslušnou část Předmětu koupě.

30. Kupující neposkytuje zálohy.

ČÁST 5 - MÍSTO DODÁNÍ PŘEDMĚTU KOUPE

31. Prodávající je povinen dopravit Předmět koupě do místa dodání uvedeného v Kupní smlouvě, jinak do sídla organizační jednotky, která jménem Kupujícího uzavřela Kupní smlouvu. Nelze-li místo dodání určit dle předcházející věty, je místem dodání sídlo Kupujícího.

ČÁST 6 - DOBA DODÁNÍ PŘEDMĚTU KOUPE

32. Prodávající je povinen dopravit Předmět koupě do místa dodání v době stanovené v Kupní smlouvě, jinak bez zbytečného odkladu po uzavření Kupní smlouvy.
33. **Prodávající je povinen dopravit Předmět koupě do místa dodání v pracovní den v době od 8 do 15 hodin. Dodá-li Prodávající Předmět koupě Kupujícímu v jiné než uvedené době, je Kupující oprávněn odmítnout Předmět koupě převzít a není zároveň v prodlení s převzetím Předmětu koupě.**
34. Případne-li konec sjednané doby plnění na sobotu, neděli nebo svátek, není Prodávající v prodlení, dodá-li Předmět koupě nejbližší následující pracovní den v časovém rozmezí dle odstavce 33.

ČÁST 7 - PŘEPRAVA PŘEDMĚTU KOUPE

35. Je-li dle Kupní smlouvy nebo zvyklostí třeba Předmět koupě zabalit, Prodávající Předmět koupě zabalí dle Kupní smlouvy; není-li ujednání o balení Předmětu koupě v Kupní smlouvě, pak dle zvyklostí, a není-li jich, pak způsobem potřebným pro uchování Předmětu koupě a jeho ochranu.
36. Jestliže Prodávající označí Obalový materiál nejpozději do doby převzetí Předmětu koupě Kupujícím jako vratný, a to přímo na Obalovém materiálu, v Dokladech nebo jiným zřejmým způsobem, ze kterého bude zřejmé, který Obalový materiál je vratný, je Kupující oprávněn předat Prodávajícímu při předávacím řízení (viz část ČÁST 9 - Obchodních podmínek) stejné množství Obalového materiálu téhož druhu a srovnatelného nebo nižšího stupně opotřebení. V rozsahu předání Obalového materiálu Kupujícím Prodávajícímu dle předchozí věty zaniká právo Prodávajícího na vrácení Obalového materiálu.
37. V rozsahu, v němž Kupující nevrátí vratný Obalový materiál Prodávajícímu dle předchozího odstavce, je Prodávající oprávněn Kupujícímu vyúčtovat zálohu na vratný Obalový materiál. Výše zálohy nesmí přesáhnout dvojnásobek pořizovací ceny Obalového materiálu.
38. Doposud nevrácený vratný Obalový materiál je Kupující povinen na vlastní náklady dopravit do sídla Prodávajícího, a to nejpozději do jednoho roku od převzetí Předmětu koupě Kupujícím. Kupující 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 Prodávajícím, je Prodávající povinen vrátit Kupujícímu zaplacenou zálohu na vratný Obalový materiál. Nevrátí-li Kupující dosud nevrácený vratný Obalový materiál nebo Obalový materiál stejného druhu a srovnatelného nebo nižšího stupně opotřebení ani do dvou let od převzetí Předmětu koupě Kupujícím, stává se nevrácený vratný Obalový materiál vlastnictvím Kupujícího a složená záloha se stává vlastnictvím Prodávajícího.
39. Pokud Prodávající Předmět koupě Kupujícímu odesílá prostřednictvím dopravce, umožní Prodávající Kupujícímu uplatnit práva z přepravní smlouvy vůči dopravci, pokud o to Kupující Prodávajícího požádá.
40. Pokud Prodávající Předmět koupě Kupujícímu odesílá prostřednictvím dopravce, je Prodávající povinen zajistit dopravu u dopravce tak, aby Předmět koupě byl dodán Kupujícímu v době uvedené v odstavci 33 Obchodních podmínek.

41. Je-li třeba provést vyložení Předmětu koupě z dopravního prostředku, je vyložení povinen provést Prodávající na své náklady.
42. Je-li Kupující v prodlení s převzetím Předmětu koupě, uchová jej Prodávající, může-li s ním nakládat, pro Kupujícího způsobem přiměřeným okolnostem. Převzal-li Kupující Předmět koupě, který zamýšlí odmítnout, uchová jej způsobem přiměřeným okolnostem. Smluvní strana, která uchovává Předmět koupě pro druhou Smluvní stranu, má právo na náhradu účelně vynaložených nákladů spojených s uchováním Předmětu koupě, nemůže jej však za účelem zajištění svého práva na úhradu nákladů zadržet.

ČÁST 8 - DALŠÍ DODACÍ PODMÍNKY

43. Prodávající je povinen splnit svůj závazek z Kupní smlouvy na svůj náklad a nebezpečí řádně a včas.
44. Lze-li dluh Prodávajícího splnit několika způsoby, náleží volba způsobu plnění Prodávajícímu.
45. Nabízí-li Prodávající Kupujícímu částečné plnění Předmětu koupě, aniž by částečné plnění bylo sjednáno v Kupní smlouvě, není Kupující povinen částečné plnění přijmout. Přijme-li Kupující částečné plnění, je Prodávající povinen nahradit Kupujícímu zvýšené náklady způsobené mu částečným plněním.
46. Zjistí-li Prodávající jakékoliv skutečnosti, které by mohly mít vliv na dobu plnění, je Prodávající povinen bez zbytečného odkladu Kupujícího o takových skutečnostech informovat.
47. Ustanovení §1912 Občanského zákoníku se neužijí.

ČÁST 9 - PŘEDÁNÍ A PŘEVZETÍ PŘEDMĚTU KOUPE

48. Předání a převzetí Předmětu koupě probíhá v rámci předávacího řízení.
49. Předávací řízení začíná okamžikem, kdy je Předmět koupě dodán do místa dodání a Kupujícímu je umožněno Předmět koupě zkontrolovat.
50. Předávací řízení končí okamžikem odmítnutí převzetí Předmětu koupě nebo okamžikem potvrzení Dodacího listu Kupujícím.
51. Potvrzení Dodacího listu je okamžikem převzetí Předmětu koupě.
52. Dodací list musí vždy obsahovat
 - 52.1. přesné označení Prodávajícího a Kupujícího,
 - 52.2. číslo vagónu nebo SPZ kolového dopravního prostředku, jímž byl Předmět koupě dodán,
 - 52.3. číslo Dodacího listu a datum jeho vystavení,
 - 52.4. číslo Kupní smlouvy,
 - 52.5. specifikaci Předmětu koupě,
 - 52.6. množství dodaného Předmětu koupě,
 - 52.7. místo dodání dle Kupní smlouvy,
 - 52.8. seznam předaných Dokladů.
53. Nejpozději společně s Předmětem koupě je Prodávající povinen předat Kupujícímu též Doklady. Nesplní-li Prodávající povinnost dle předchozí věty, je v prodlení s plněním Kupní smlouvy.
54. Kupující je oprávněn odmítnout převzít Předmět koupě, není-li ve shodě s Kupní smlouvou, neobsahuje-li Dodací list stanovené náležitosti nebo nejsou-li Kupujícímu nejpozději s Předmětem koupě předány Doklady.
55. Hodlá-li Kupující Předmět koupě převzít, ačkoliv není ve shodě s Kupní smlouvou, jsou obě Smluvní strany oprávněny uvést do Dodacího listu svá stanoviska ke Kupujícím tvrzenému rozporu s Kupní smlouvou.
56. Připouští-li to povaha Předmětu koupě, má Kupující právo, aby byl Předmět koupě před ním překontrolován nebo aby byly předvedeny jeho funkce.

57. Je-li Předmět koupě dodáván po částech, vztahují se ustanovení Obchodních podmínek o předání a převzetí Předmětu koupě přiměřeně též na předání a převzetí části Předmětu koupě.

ČÁST 10 - PŘECHOD VLASTNICKÉHO PRÁVA A NEBEZPEČÍ ŠKODY

58. Vlastnické právo k Předmětu koupě přechází na Kupujícího okamžikem, kdy Kupující potvrdí Dodací list.
59. Nebezpečí škody na Předmětu koupě přechází na Kupujícího okamžikem, kdy Kupující potvrdí Dodací list, nebo kdy Kupující bezdůvodně odmítne Dodací list potvrdit.
60. Ustanovení §2121–2123 Občanského zákoníku se neužijí.

ČÁST 11 - VADY PLNĚNÍ A ZÁRUKA

61. Prodávající se zavazuje, že Předmět koupě a Doklady budou v okamžiku jejich převzetí Kupujícím vyhovovat všem požadavkům Kupní smlouvy, Obchodních podmínek a právních předpisů na rozsah, množství, jakost a provedení Předmětu koupě a Dokladů.
62. Prodávající se zavazuje, že Předmět koupě a Doklady budou vyhovovat též plnění nabídnutému Prodávajícím v nabídce podané do zadávacího řízení, na jehož základě je Kupní smlouva uzavřena.
63. Předmět koupě a Doklady musí být prosté všech faktických a právních vad a Prodávající je povinen zajistit, aby dodáním a užíváním Předmětu koupě a Dokladů nebyla porušena práva Prodávajícího nebo třetích osob vyplývající z práv duševního vlastnictví. Plnění má právní vadu, pokud k němu uplatňuje právo třetí osoba.
64. Prodávající se zavazuje (poskytuje Kupujícím záruku), že Předmět koupě a Doklady si po celou dobu od okamžiku jejich převzetí Kupujícím, až do uplynutí Záruční doby zachovají vlastnosti stanovené v odstavcích 61 - 63 Obchodních podmínek.
65. Záruční doba začíná běžet dnem převzetí Předmětu koupě Kupujícím nebo jeho poslední části, je-li Předmět koupě dodáván po částech, nebo ode dne úspěšného ukončení zkušebního provozu, je-li dle Kupní smlouvy vyžadován a nastane-li okamžik úspěšného ukončení zkušebního provozu později než okamžik převzetí Předmětu koupě, resp. jeho poslední části.
66. Předmět koupě a Doklady mají vady (Prodávající plnil vadně), jestliže při převzetí Kupujícím nebo kdykoliv od převzetí Kupujícím do konce Záruční doby nebudou mít vlastnosti stanovené v odstavcích 61 - 63 Obchodních podmínek.
67. Kupující má práva z vadného plnění i v případě, jedná-li se o vadu, kterou musel s vynaložením obvyklé pozornosti poznat již při uzavření Kupní smlouvy.
68. Prodávající nenesे odpovědnost za vady způsobené Kupujícím nebo třetími osobami, ledaže Kupující nebo takové osoby postupovaly v souladu s Doklady nebo pokyny, které obdrželi od Prodávajícího,
69. Kupující nemá práva z vadného plnění, způsobila-li vadu po přechodu nebezpečí škody na věci na Kupujícího vnější událost. To neplatí, způsobil-li vadu Prodávající nebo jakákoliv třetí osoba, jejímž prostřednictvím plnil své povinnosti vyplývající z Kupní smlouvy.
70. Prodávající neodpovídá za vady spočívající v opotřebení Předmětu koupě, které je obvyklé u věcí stejného nebo obdobného druhu jako Předmět koupě.
71. Prodávající odpovídá za vady spočívající v opotřebení Předmětu koupě, ke kterému do konce Záruční doby vzhledem k požadavkům Kupní smlouvy a Obchodních podmínek na jakost a provedení Předmětu koupě nemělo dojít.

ČÁST 12 - UPLATNĚNÍ PRÁV Z VADNÉHO PLNĚNÍ

72. Odpovídá-li Prodávající za vady Předmětu koupě nebo Dokladů, má Kupující práva z vadného plnění.

73. Kupující je oprávněn vady reklamovat u Prodávajícího jakýmkoliv způsobem, preferovaná je písemná forma. Prodávající je povinen přijetí reklamace bez zbytečného odkladu písemně potvrdit. V reklamaci Kupující uvede popis vady nebo uvede, jak se vada projevuje.
74. Vada je uplatněna včas, je-li písemná forma reklamace odeslána Prodávajícímu 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 Prodávajícímu nejblíže následující pracovní den.
75. Má-li Předmět koupě vady, za které Prodávající odpovídá, má Kupující právo
- 75.1. na odstranění vady dodáním nového Předmětu koupě nebo jeho části bez vady, pokud to není vzhledem k povaze vady zcela zřejmě nepřiměřené, nebo dodání chybějící části Předmětu koupě,
- 75.2. na odstranění vady opravou Předmětu koupě nebo jeho části,
- 75.3. na přiměřenou slevu z Kupní ceny, nebo
- 75.4. odstoupit od Kupní smlouvy.
76. Není nepřiměřené, požaduje-li Kupující odstranit vady dodáním nového Předmětu koupě nebo jeho části bez vady, vyskytla-li se stejná vada po její opravě opětovně, nebo nemůže-li Kupující řádně užívat Předmět koupě nebo jeho část pro větší počet vad.
77. Kupující je oprávněn nároky dle odstavce 75 kombinovat, je-li to vzhledem k okolnostem možné. Kupující není oprávněn kombinovat nároky, které si navzájem odporují (např. dodání nové části Předmětu koupě a zároveň slevy z Kupní ceny na tutéž část Předmětu koupě).
78. Kupující sdělí Prodávajícímu volbu nároku z vady v reklamaci, nebo bez zbytečného odkladu po reklamaci. Provedenou volbu nemůže Kupující změnit bez souhlasu Prodávajícího; to neplatí, žádal-li Kupující opravu vady, která se ukáže jako neopravitelná.
79. Nesdělí-li Kupující Prodávajícímu, jaké právo si zvolil ani bez zbytečného odkladu poté, co jej k tomu Prodávající vyzval, může Prodávající odstranit vady podle své volby opravou nebo dodáním nového Předmětu koupě nebo jeho části; volba nesmí Kupujícímu způsobit nepřiměřené náklady.
80. Kupující má nárok na náhradu nákladů účelně vynaložených v souvislosti s oznámením vad Prodávajícímu.

ČÁST 13 - PODMÍNKY ODSTRANĚNÍ VAD

81. Pokud Kupující požaduje v reklamaci odstranění vady, je Prodávající povinen neprodleně po obdržení reklamace zahájit činnosti vedoucí k odstranění reklamované vady.
82. Prodávající je povinen odstranit Kupujícím reklamovanou vadu nejpozději do 30 kalendářních dnů ode dne oznámení vady Prodávajícímu.
83. Nezahájí-li Prodávající činnosti vedoucí k odstranění vady do 10 dnů od oznámení vady Prodávajícímu, nebo nebude-li vada odstraněna ve lhůtě dle předcházejícího odstavce, je Kupující oprávněn
- 83.1. zajistit odstranění vady jinou odborně způsobilou právnickou nebo fyzickou osobou na účet Prodávajícího,
- 83.2. požadovat slevu z Kupní ceny, nebo
- 83.3. od Kupní smlouvy odstoupit.
84. Veškeré náklady vzniklé Kupujícímu v souvislosti s odstranění vady způsobem dle předchozího odstavce je Prodávající povinen Kupujícímu uhradit.
85. Prodávající je povinen odstranit vadu bez ohledu na to, zda je uplatnění vady oprávněné či nikoli. Prokáže-li se však kdykoli později, že uplatnění vady Kupujícím nebylo oprávněné, tj. že Prodávající za vadu neodpovídal, je Kupující povinen uhradit Prodávajícímu veškeré jím účelně vynaložené náklady v souvislosti s odstraněním vady.
86. Kupující je povinen poskytnout Prodávajícímu součinnost nezbytnou k odstranění vady.
87. Do odstranění vady nemusí Kupující platit dosud nezaplacenou část Kupní ceny a případnou příslušnou DPH odhadem přiměřeně odpovídající jeho právu na slevu.
88. Při dodání nového Předmětu koupě nebo jeho části vrátí Kupující Prodávajícímu na náklady Prodávajícího Předmět koupě nebo jeho část původně dodanou.

89. Týká-li se vada Dokladů nebo jiného plnění poskytnutého Prodávajícím dle Kupní smlouvy než Předmětu koupě, užijí se ustanovení odstavců 72 – 88 obdobně.
90. Ustanovení § 1917–1924, §2099–2101, §2103–2117 a §2165 - 2172 Občanského zákoníku se neužijí.

ČÁST 14 - SANKCE

91. Poruší-li Prodávající povinnost dodat Předmět koupě nebo Doklady či jakoukoliv jejich část ve sjednané době, je Prodávající povinen uhradit Kupujícímu smluvní pokutu ve výši 0,5 % z Kupní ceny za každý den prodlení.
92. Poruší-li Kupující povinnost zaplatit Kupní cenu ve sjednané době, je povinen uhradit Prodávajícímu úrok z prodlení ve výši právních předpisů.
93. Poruší-li Prodávající povinnost dodat Kupujícímu Předmět koupě bez vad, je povinen uhradit Kupujícímu smluvní pokutu ve výši 5% z Kupní ceny. Úhradou smluvní pokuty nejsou dotčena práva Kupujícího z vadného plnění Prodávajícího.
94. Poruší-li Prodávající povinnost nepostoupit žádnou svou pohledávku za Kupujícím vyplývající z Kupní smlouvy, byť by takové postoupení bylo neplatné či neúčinné, je Prodávající povinen uhradit Kupujícímu smluvní pokutu ve výši 10% z nominální hodnoty postoupené pohledávky, včetně hodnoty případného příslušenství ke dni účinnosti postoupení vůči postupníkovi.
95. Zaplacení smluvní pokuty nezavazuje Prodávajícího povinnosti splnit dluh smluvní pokutou utvrzený.
96. Kupující je oprávněn požadovat náhradu škody a nemajetkové újmy způsobené porušením povinnosti, na kterou se vztahuje smluvní pokuta, v plné výši.

ČÁST 15 - ODSTOUPENÍ OD KUPNÍ SMLOUVY

97. Poruší-li Smluvní strana Kupní smlouvu podstatným způsobem, může druhá Smluvní strana písemnou formou od Kupní smlouvy odstoupit.
98. Podstatné je takové porušení povinnosti, o němž Smluvní strana porušující Kupní smlouvu již při uzavření Kupní smlouvy věděla nebo musela vědět, že by druhá Smluvní strana Kupní smlouvu neuzavřela, pokud by toto porušení předvídala; v ostatních případech se má za to, že porušení podstatné není.
99. Podstatným porušením Kupní smlouvy je též prodlení s dodáním Předmětu koupě o více než 30 kalendářních dní.
100. Kupující je oprávněn od Kupní smlouvy odstoupit též z důvodů uvedených v části Předání a převzetí Předmětu koupě (viz ČÁST 9 - Obchodních podmínek).
101. Kupující je oprávněn odstoupit od Kupní smlouvy, ukáže-li se jako nepravdivé jakékoliv prohlášení Prodávajícího uvedené v odstavci 112, nebo ocitne-li se Prodávající ve stavu úpadku nebo hrozícího úpadku.
102. Smluvní strana může od Kupní smlouvy odstoupit, pokud z chování druhé Smluvní strany nepochybně vyplývá, že poruší Kupní smlouvu podstatným způsobem, a nedá-li na výzvu oprávněné Smluvní strany přiměřenou jistotu.
103. Jakmile Smluvní strana oprávněná odstoupit od Kupní smlouvy oznámí druhé Smluvní straně, že od Kupní smlouvy odstupuje, nebo že na Kupní smlouvě setrvává, nemůže volbu již sama změnit.
104. Zakládá-li prodlení Smluvní strany nepodstatné porušení její povinnosti z Kupní smlouvy, může druhá Smluvní strana od Kupní smlouvy odstoupit poté, co prodlévající Smluvní strana svoji povinnost nesplní ani v dodatečně přiměřené lhůtě, kterou jí druhá Smluvní strana poskytla výslovně nebo mlčky.
105. 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 Kupní smlouvy odstoupila.
106. Poskytla-li Smluvní strana Smluvní straně prodlévající nepřiměřeně krátkou dodatečnou lhůtu k plnění a odstoupí-li od Kupní smlouvy 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 Kupní smlouvy, aniž by prodlévající Smluvní straně dodatečnou lhůtu k plnění poskytla.
107. Kupující je oprávněn odstoupit do Kupní smlouvy v případě, že Prodávající uvedl v nabídce podané do zadávacího řízení veřejné zakázky informace nebo doklady, které neodpovídají skutečnosti a měly nebo mohly mít vliv na výsledek řízení.
 108. Odstoupením od Kupní smlouvy se závazek zrušuje od počátku.
 109. Plnil-li Prodávající zčásti, může Kupující od Kupní smlouvy odstoupit jen ohledně nesplněného zbytku plnění. Nemá-li však částečné plnění pro Kupujícího význam, může Kupující od Kupní smlouvy odstoupit ohledně celého plnění.
 110. Zavazuje-li Kupní smlouva Prodávajícího k opakované činnosti nebo k postupnému dílčímu plnění, může Kupující od Kupní smlouvy odstoupit jen s účinky do budoucna. To neplatí, nemají-li již přijatá dílčí plnění sama o sobě pro Kupujícího význam.
 111. Ustanovení §1977, §2002–2003 Občanského zákoníku se neužijí.

ČÁST 16 - OSTATNÍ UJEDNÁNÍ

112. Prodávající prohlašuje, že není v úpadku ani ve stavu hrozícího úpadku, a že mu není známo, že by vůči němu bylo zahájeno insolvenční řízení. Rovněž prohlašuje, že vůči němu není v právní moci žádné soudní rozhodnutí, případně rozhodnutí správního, daňového či jiného orgánu na plnění, které by mohlo být důvodem zahájení exekučního řízení na majetek Prodávajícího a že mu není známo, že by vůči němu takové řízení bylo zahájeno.
113. Prodávající na sebe přebírá nebezpečí změny okolností ve smyslu §1765 Občanského zákoníku.
114. Prodávající není oprávněn postoupit žádnou svou pohledávku za Kupujícím vyplývající z Kupní smlouvy nebo vzniklou v souvislosti s Kupní smlouvou.
115. Prodávající není oprávněn provést jednostranné započtení žádné své pohledávky za Kupujícím vyplývající z Kupní smlouvy nebo vzniklé v souvislosti s Kupní smlouvou na jakoukoliv pohledávku Kupujícího za Prodávajícím.
116. Kupující je oprávněn provést jednostranné započtení jakékoliv své splatné i nesplatné pohledávky za Prodávajícím vyplývající z Kupní smlouvy nebo vzniklé v souvislosti s Kupní smlouvou (zejm. smluvní pokutu) na pohledávky Prodávajícího za Kupujícím.
117. Prodávající je povinen zachovávat mlčenlivost o všech skutečnostech a informacích, které jsou obsaženy v Kupní smlouvě a dále o všech skutečnostech a informacích, které mu byly v souvislosti s Kupní 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 Prodávající seznámil, prokazatelně veřejně přístupné nebo těch, které se bez zavinění Prodávajícího veřejně přístupnými stanou. Prodávající 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 Kupujícího. Povinnosti dle tohoto odstavce je Prodávající povinen zachovávat i po zániku závazku z Kupní smlouvy, vyjma případů, kdy se takové skutečnosti a informace stanou prokazatelně veřejně přístupné bez zavinění Prodávajícího. Povinnosti dle tohoto odstavce se nevztahují na případy, kdy je Prodávající povinen zveřejnit takové skutečnosti nebo informace na základě povinnosti uložené mu právním předpisem nebo rozhodnutím orgánu veřejné moci.
118. Poruší-li Prodávající v souvislosti s Kupní smlouvou jakékoliv své povinnosti, nahradí Kupujícímu škodu a nemajetkovou újmu z toho vzniklou. Povinnosti k náhradě se Prodávající zproští, prokáže-li, že mu ve splnění povinnosti zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli. Překážka vzniklá z osobních poměrů Prodávajícího nebo vzniklá až v době, kdy byl Prodávající s plněním povinnosti v prodlení, ani překážka, kterou byl Prodávající povinen překonat, jej však povinnosti k náhradě nezproští.
119. Vzhledem k veřejnoprávnímu charakteru Kupujícího Prodávající výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním Kupní smlouvy v rozsahu a za podmínek vyplývajících z příslušných právních předpisů.

120. Prodávající 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.
121. Písemnou formou (podobou) se rozumí listina podepsaná oprávněnou osobou Smluvní strany nebo email podepsaný zaručeným elektronickým podpisem oprávněné osoby Smluvní strany.