Smlouva o zajištění služby GitLab v perimetru Objednatele
č. 20260167

Smluvní strany:

VZLU AEROSPACE, a.s. Se sídlem: Beranových 130, Letňany, 199 00 Praha 9 Zastoupena: Ing. Josefem Kašparem, FEng., předsedou představenstva a JUDr. Petrem Matouškem, místopředsedou představenstva IČ: 00010669, DIČ: CZ00010669 Bankovní s[redacted]Spisová značka: B 446 vedená u Městského soudu v Praze (dále jen „Objednatel")

a

STORAGE ONE, a.s. Sídlem: Jeremiášova 947/16, Stodůlky, 155 00 Praha 5. Zastoupena: Reném Valvodou, předsedou představenstva. IČ: 02301245, DIČ: CZ02301245. Bankovní spojení: UniCredit Bank Czech Republic and Slovakia, a.s., č. ú. 2109680467/2700. Spisová značka: B 19458 vedená u Městského soudu v Praze (dále jen „Poskytovatel")

uzavřely níže uvedeného dne, měsíce a roku tuto **Smlouvu o zajištění služby GitLab v perimetru Objednatele** (dále jen „Smlouva")

1 Definice a výklad

1.1 Pro účely této Smlouvy se rozumí:

„Služba" — služba GitLab poskytovaná formou managed service v Perimetru Objednatele, zahrnující veškeré činnosti dle článku 2 a příloh této Smlouvy.

„Perimetr Objednatele" — prostory v sídle Objednatele na adrese Beranových 130, Praha 9 – Letňany, a lokální síťová infrastruktura Objednatele (LAN/VLAN) propojená s dodaným hardware. Za součást Perimetru se považuje rovněž autorizovaný VPN přístup z území EU/EHP, který splňuje bezpečnostní požadavky dle Přílohy č. 4. Za Perimetr se nepovažuje vzdálený přístup z území třetích zemí (mimo EU/EHP).

„Go-Live" — datum úspěšného dokončení implementace a předání Služby do produkčního provozu, potvrzené oboustranným akceptačním protokolem na základě splnění Akceptačních kritérií dle Přílohy č. 9.

„Provozní díla" — veškeré konfigurace, automatizační skripty, šablony, monitoring dashboardy, runbooky, procedury a dokumentace vytvořené Poskytovatelem výhradně pro účely poskytování Služby Objednateli.

„Background IP" — předexistující know-how, nástroje, metodiky a software Poskytovatele, které existovaly před uzavřením této Smlouvy nebo byly vyvinuty nezávisle na plnění této Smlouvy.

1.2 Nadpisy článků slouží pouze pro orientaci a nemají vliv na výklad Smlouvy.

2 Předmět Smlouvy

2.1 Poskytovatel se zavazuje poskytovat Objednateli Službu zahrnující zejména: dodání a uvedení do provozu veškerého hardware, instalaci, konfiguraci a provoz GitLab, správu CI/CD infrastruktury, monitoring a incident management, zálohování a obnovu dat, zajištění bezpečnosti a splnění SLA parametrů — vše v rozsahu stanoveném touto Smlouvou a jejími přílohami.

2.2 Objednatel se zavazuje za poskytování Služby platit Poskytovateli odměnu dle podmínek této Smlouvy.

2.3 Nedílnou součástí předmětu plnění je dodání hardware specifikovaného v Příloze č. 1, jeho instalace, konfigurace, servis po dobu trvání Smlouvy a převod vlastnického práva k HW na Objednatele po uplynutí 60 měsíců dle článku 11 této Smlouvy.

2.4 Služba musí být v souladu s technickým zadáním (Příloha č. 1), SLA parametry (Příloha č. 2), bezpečnostními požadavky (Příloha č. 4) a DPA (Příloha č. 5).

3 Doba trvání a účinnost

3.1 Smlouva se uzavírá na dobu určitou 60 měsíců ode dne Go-Live.

3.2 Smlouva nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti uveřejněním v Registru smluv dle zákona č. 340/2015 Sb.

3.3 Období od účinnosti Smlouvy do Go-Live (dále jen „**Implementační období**") je součástí předmětu plnění a jeho náklady jsou zahrnuty v ceně služby prvního smluvního roku. Implementační období se nefakturuje separátně.

3.4 Poskytovatel je povinen dosáhnout Go-Live nejpozději do 90 kalendářních dnů od účinnosti Smlouvy. Go-Live nastává splněním všech Akceptačních kritérií dle Přílohy č. 9 a podpisem oboustranného akceptačního protokolu. Nedodržení tohoto termínu je podstatným porušením Smlouvy.

4 Odměna a platební podmínky

4.1 Odměna za Službu je stanovena jako roční paušální částka dle Přílohy č. 3 (Cenová příloha). Odměna zahrnuje veškeré náklady Poskytovatele včetně licencí GitLab, provozu HW, servisu, zálohování, monitoringu, podpory, Implementačního období a veškerých dalších činností stanovených touto Smlouvou.

4.2 Odměna bude fakturována v ročních platbách, vždy k prvnímu dni příslušného smluvního roku. Splatnost faktur činí 30 dnů ode dne doručení daňového dokladu na e-

mailovou adresu Objednatele uvedenou v Příloze č. 7. První smluvní rok počíná dnem Go-Live.

4.3 Za období od Go-Live do konce prvního kalendářního roku se odměna vypočte poměrně (pro rata temporis).

4.4 Navýšení počtu licencí nad sjednaný rozsah je možné jedenkrát ročně na základě písemného oznámení Objednatele doručeného nejpozději 60 dnů před výročím Go-Live. Cena dodatečných licencí se stanoví jako doložená cena licence od autorizovaného distributora GitLab v okamžiku objednávky navýšená o neměnnou marži Poskytovatele uvedenou v Příloze č. 3.

4.5 Veškeré ceny jsou uvedeny bez DPH. DPH bude účtována dle platných právních předpisů.

5 Povinnosti Poskytovatele

5.1 Poskytovatel je povinen zajistit nepřetržité poskytování Služby po celou dobu trvání Smlouvy v souladu s SLA parametry stanovenými v Příloze č. 2.

5.2 Poskytovatel je povinen dodržovat minimální bezpečnostní požadavky dle Přílohy č. 4 a postupovat v souladu s DPA (Příloha č. 5) při zpracování osobních údajů.

5.3 Poskytovatel je povinen provádět pravidelné aktualizace a bezpečnostní záplaty GitLab a souvisejících komponent. Kritické bezpečnostní záplaty musí být aplikovány do 14 kalendářních dnů od jejich publikace výrobcem, není-li s Objednatelem dohodnuto jinak.

5.4 Poskytovatel je povinen předkládat Objednateli měsíční provozní report obsahující minimálně: dostupnost Služby s podkladovými daty z monitoringu, přehled incidentů s kategorizací a dobami řešení, stav kapacit, bezpečnostní události, provedené změny a plánované údržbové aktivity. Report je předkládán do 5. pracovního dne následujícího měsíce.

5.5 Poskytovatel je povinen udržovat po celou dobu trvání Smlouvy pojištění odpovědnosti za škodu způsobenou třetím osobám s minimálním limitem plnění 10 000 000 CZK a na vyžádání předložit Objednateli kopii pojistné smlouvy.

5.6 Poskytovatel zajistí, že klíčoví členové realizačního týmu uvedení v nabídce (Příloha č. 6) budou po dobu trvání Smlouvy k dispozici. Změna klíčového člena týmu vyžaduje předchozí písemný souhlas Objednatele; náhradní osoba musí splňovat minimálně stejné kvalifikační předpoklady.

5.7 Poskytovatel nesmí bez předchozího písemného souhlasu Objednatele využít k plnění Smlouvy subdodavatele. Poskytovatel odpovídá za plnění subdodavatelů jako za plnění vlastní. Subdodavatel musí splňovat srovnatelné bezpečnostní požadavky dle Přílohy č. 4 a nesmí mít sídlo ani provozovnu mimo EU/EHP.

6 Povinnosti Objednatele

6.1 Objednatel je povinen poskytnout Poskytovateli přístup do Perimetru Objednatele v rozsahu nezbytném pro řádné plnění Smlouvy.

6.2 Objednatel určí kontaktní osoby pro komunikaci s Poskytovatelem dle Přílohy č. 7 a zajistí přiměřenou součinnost při řešení incidentů a provádění změn.

6.3 Objednatel je povinen bez zbytečného odkladu informovat Poskytovatele o změnách ve své IT infrastruktuře, které mohou mít dopad na Službu.

7 SLA, sankce a service credity

7.1 Poskytovatel se zavazuje dodržovat parametry SLA stanovené v Příloze č. 2. SLA se vztahuje na Službu jako celek, bez oddělování HW a SW složky.

7.2 Za nedodržení cílové měsíční dostupnosti Služby náleží Objednateli sleva z odměny (service credit) dle progresivní stupnice: při dostupnosti 95,0–98,9 % sleva 3 % z měsíční odměny za každé celé procento pod cílovou hodnotou, při dostupnosti 90,0–94,9 % sleva 5 % z měsíční odměny za každé celé procento pod cílovou hodnotou, při dostupnosti pod 90,0 % sleva 100 % měsíční odměny. Dostupnost pod 85,0 % v kterémkoliv kalendářním měsíci se považuje za podstatné porušení Smlouvy.

7.3 Za nedodržení reakční doby u kritické poruchy náleží Objednateli smluvní pokuta ve výši [redacted] za každou i započatou hodinu prodlení nad sjednanou reakční dobu, maximálně však [redacted] za jeden incident.

7.4 Za nedodržení doby vyřešení u kritické poruchy náleží Objednateli smluvní pokuta ve výši [redacted] za každý i započatý pracovní den prodlení nad sjednanou dobu vyřešení, maximálně však [redacted] za jeden incident.

7.5 Opakované porušení SLA — tj. 3 a více kritických poruch za kalendářní čtvrtletí nebo dostupnost pod cílovou hodnotu 3 po sobě jdoucí měsíce — se považuje za podstatné porušení Smlouvy a zakládá právo Objednatele odstoupit od Smlouvy.

7.6 Smluvní pokuty a service credity se uplatňují zápočtem proti nejbližší splatné faktuře. Uplatněním smluvní pokuty není dotčeno právo na náhradu škody.

8 Bezpečnost a ochrana dat

8.1 Poskytovatel je povinen zajistit, že osobní údaje nebudou zpracovávány ani přenášeny mimo území EU/EHP a že nebude umožněn vzdálený administrátorský ani podpůrný přístup k systémům a datům z území mimo Perimetr Objednatele, pokud takový přístup nesplňuje definici Perimetru dle článku 1. Porušení těchto povinností je podstatným porušením Smlouvy.

8.2 Podmínky zpracování osobních údajů jsou upraveny v DPA (Příloha č. 5).

8.3 Poskytovatel je povinen oznámit Objednateli jakýkoliv bezpečnostní incident bez zbytečného odkladu, nejpozději do 24 hodin od okamžiku, kdy se o incidentu dozvěděl nebo měl dozvědět, a poskytnout Objednateli plnou součinnost při jeho řešení.

8.4 Objednatel je oprávněn provést bezpečnostní audit Služby jedenkrát ročně na své náklady po předchozím oznámení v přiměřené lhůtě (nejméně 10 pracovních dnů). Poskytovatel poskytne auditnímu týmu přístup k relevantním systémům, logům, konfiguraci a dokumentaci. V případě bezpečnostního incidentu je Objednatel oprávněn provést mimořádný audit bez předchozího oznámení.

8.5 Poskytovatel je povinen uchovávat auditní logy minimálně 12 měsíců a na vyžádání je zpřístupnit Objednateli ve strojově čitelném formátu do 5 pracovních dnů.

9 Odpovědnost za škodu a limitace

9.1 Odpovědnost smluvních stran za škodu se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník.

9.2 Celková kumulativní odpovědnost Poskytovatele za škodu vzniklou z nebo v souvislosti s touto Smlouvou je omezena na částku rovnající se roční odměně za Službu za posledních 12 měsíců předcházejících vzniku škody (dále jen „Cap odpovědnosti").

9.3 Cap odpovědnosti se neuplatní na škodu způsobenou úmyslně nebo hrubou nedbalostí, na porušení bezpečnostních zákazů dle článku 8, na porušení povinnosti důvěrnosti dle článku 12 a na nároky třetích osob z titulu porušení práv duševního vlastnictví.

9.4 Poskytovatel neodpovídá Objednateli za nepřímé škody a následné škody, s výjimkou škod způsobených úmyslně nebo hrubou nedbalostí. Objednatel neodpovídá Poskytovateli za nepřímé škody, ušlý zisk ani následné škody, s výjimkou škod způsobených úmyslně.

10 Duševní vlastnictví

10.1 Provozní díla, která splňují znaky autorského díla dle § 2 zákona č. 121/2000 Sb. (autorský zákon), se považují za dílo vytvořené na objednávku dle § 61 autorského zákona, přičemž majetková práva autorská vykonává Objednatel jako objednatel díla. Ustanovení § 2634 občanského zákoníku se použije přiměřeně.

10.2 Provozní díla, která nedosahují prahu originality pro autorskoprávní ochranu (zejména konfigurační soubory, datové struktury, parametry nastavení), přecházejí do vlastnictví Objednatele okamžikem jejich vzniku. Poskytovatel se zavazuje, že nebude uplatňovat žádná práva k těmto výstupům a že je předá Objednateli v plném rozsahu, ve strojově čitelné podobě, kdykoliv o to Objednatel požádá a nejpozději při ukončení Smlouvy.

10.3 Background IP zůstává ve vlastnictví Poskytovatele. Poskytovatel tímto uděluje Objednateli nevýhradní, neodvolatelnou, teritoriálně neomezenou, bezúplatnou licenci na dobu neurčitou k užití Background IP v rozsahu nezbytném pro provoz, údržbu a rozvoj Služby a pro její převod na jiného poskytovatele nebo do vlastní správy Objednatele.

10.4 Práva k softwaru GitLab se řídí licenčními podmínkami výrobce (GitLab Inc.). Poskytovatel je povinen zajistit, aby licence GitLab Ultimate byly po celou dobu trvání Smlouvy platné a aktivní, a bez zbytečného odkladu informovat Objednatele o jakékoliv změně licenčních podmínek ze strany výrobce.

11 Hardware: dodání, vlastnictví a převod

11.1 Poskytovatel je povinen dodat a uvést do provozu hardware specifikovaný v Příloze č. 1 nejpozději v termínu stanoveném harmonogramem implementace.

11.2 Hardware je po dobu trvání Smlouvy ve vlastnictví Poskytovatele. Objednatel je oprávněn hardware užívat výhradně pro účely provozu Služby. Poskytovatel nesmí hardware zatížit právy třetích osob (zástavním právem, výhradou vlastnictví, leasingem, exekucí) po celou dobu trvání Smlouvy; porušení tohoto zákazu je podstatným porušením Smlouvy.

11.3 Po uplynutí 60 měsíců od Go-Live (řádné ukončení pětiletého období) Poskytovatel převede vlastnické právo k veškerému dodanému hardware na Objednatele za zůstatkovou kupní cenu [redacted] bez DPH. K ceně bude připočtena DPH dle platných právních předpisů. Zůstatková kupní cena odpovídá účetní zůstatkové hodnotě hardware po 60 měsících rovnoměrného odepisování (odpisová skupina 2 dle přílohy č. 1 k § 30 zákona č. 586/1992 Sb.); investice do hardware je amortizována v ceně Služby po dobu trvání Smlouvy.

11.4 Převod bude realizován na základě předávacího protokolu. Poskytovatel předá veškerou dokumentaci k hardware (záruky, servisní historie, konfigurace, seznam sériových čísel) a provede součinnost k převodu registrací výrobce a servisních kontraktů.

11.5 V případě zahájení insolvenčního řízení vůči Poskytovateli je Objednatel oprávněn uplatnit právo na předčasný odkup hardware za poměrnou zůstatkovou cenu odpovídající zbývající době do uplynutí 60 měsíců. Poskytovatel se zavazuje, že v insolvenčním řízení nebude zpochybňovat oprávnění Objednatele hardware užívat a provozovat na něm Službu až do vypořádání.

11.6 V případě ukončení Smlouvy před uplynutím 60 měsíců se s hardware naloží dle Exit plánu (Příloha č. 8); převod za [redacted] se uplatní pouze při řádném doběhu pětiletého období, není-li dohodnuto jinak.

12 Důvěrnost informací

12.1 Za důvěrné informace se považují veškeré skutečnosti obchodní, technické, finanční a organizační povahy, které se smluvní strana dozví v souvislosti s plněním této Smlouvy a které nejsou veřejně dostupné.

12.2 Smluvní strany se zavazují zachovávat mlčenlivost o důvěrných informacích a nepoužít je k jinému účelu než k plnění Smlouvy. Povinnost mlčenlivosti trvá po dobu 5 let po ukončení Smlouvy.

12.3 Povinnost mlčenlivosti se nevztahuje na informace, které jsou v době zpřístupnění veřejně dostupné, které se stanou veřejně dostupnými bez zavinění přijímající strany, které musí být zpřístupněny na základě právního předpisu nebo rozhodnutí orgánu veřejné moci, nebo které jsou nezávisle vyvinuty přijímající stranou bez použití důvěrných informací.

12.4 Poskytovatel je oprávněn uvádět skutečnost, že pro Objednatele zajišťuje Službu, jako svou referenci pouze s předchozím písemným souhlasem Objednatele a ve formě jím schválené.

13 Governance a řízení změn

13.1 Smluvní strany zřídí společný řídící výbor (Steering Committee) složený z kontaktních osob uvedených v Příloze č. 7. Řídící výbor se schází čtvrtletně, poprvé do 30 dnů od Go-Live.

13.2 Poskytovatel předkládá Objednateli měsíční provozní report dle článku 5 a roční souhrnný report s vyhodnocením SLA, trendů kapacitního využití a doporučeními pro následující období.

13.3 Změny Služby se dělí na standardní změny (konfigurace, minor updates) realizované v rámci paušálu bez schválení, rutinní změny (major updates, rozšíření kapacity) realizované na základě písemné žádosti do 10 pracovních dnů v rámci paušálu, a zásadní změny (změna architektury, integrace nových komponent) realizované formou change requestu s nacenění do 5 pracovních dnů, po schválení Objednatelem, mimo paušál. Veškeré změny musí být v souladu s § 222 ZZVZ; kumulativní hodnota zásadních změn nesmí překročit limity stanovené § 222 odst. 3 a 4 ZZVZ.

13.4 Objednatel je oprávněn po 36 měsících od Go-Live požádat o nezávislý benchmarking ceny a kvality Služby. Náklady benchmarkingu nese Objednatel. Pokud benchmarking prokáže odchylku od tržních podmínek větší než 15 %, strany v dobré víře vyjednají úpravu podmínek. Pokud strany nedosáhnou dohody do 60 kalendářních dnů od předložení výsledků benchmarkingu, je Objednatel oprávněn vypovědět Smlouvu se zkrácenou výpovědní dobou 3 měsíce, nebo jednostranně snížit odměnu o prokázanou odchylku od tržní ceny, maximálně však o 10 % roční odměny.

14 Ukončení Smlouvy

14.1 Smlouva zaniká uplynutím doby, na kterou byla uzavřena.

14.2 Každá smluvní strana může Smlouvu vypovědět bez udání důvodu písemnou výpovědí. Výpovědní doba činí 6 měsíců a počíná běžet prvním dnem měsíce následujícího po doručení výpovědi.

14.3 Objednatel je oprávněn odstoupit od Smlouvy s okamžitou účinností v případě podstatného porušení Smlouvy Poskytovatelem, zejména: porušení bezpečnostních zákazů dle článku 8, opakovaného porušení SLA dle článku 7, dostupnosti pod 85 % dle článku 7, zahájení insolvenčního řízení vůči Poskytovateli, neposkytování Služby po dobu delší než 5 po sobě jdoucích pracovních dnů bez ospravedlnitelného důvodu, nebo zatížení hardware právy třetích osob v rozporu s článkem 11.

14.4 V případě ukončení Smlouvy z jakéhokoliv důvodu se aktivuje Exit plán dle Přílohy č. 8 a článku 15.

15 Exit a přenositelnost služby

15.1 Poskytovatel je povinen po aktivaci Exit plánu poskytnout součinnost při přechodu Služby k novému poskytovateli nebo do vlastní správy Objednatele v rozsahu minimálně 80 hodin odborných prací v ceně Služby. Práce nad rámec budou fakturovány dle hodinové sazby uvedené v Příloze č. 3.

15.2 Poskytovatel je povinen do 30 kalendářních dnů od aktivace Exit plánu předat Objednateli kompletní export dat GitLab (repozitáře, metadata, CI/CD definice, konfigurace, účty), poslední konzistentní zálohy včetně dešifrovacích klíčů, veškerou provozní dokumentaci (runbooky, architekturu, monitoring, postupy obnovy) a veškerá Provozní díla dle článku 10.

15.3 Po potvrzení převzetí dat Objednatelem Poskytovatel provede bezpečný výmaz všech kopií dat včetně záloh a vydá protokol o výmazu do 30 kalendářních dnů. Povinnost výmazu se nevztahuje na data, jejichž uchování vyžaduje právní předpis.

15.4 Poskytovatel je povinen po dobu výpovědní doby a po dobu realizace Exit plánu poskytovat Službu ve stávajícím rozsahu a kvalitě. Degradace Služby v období ukončení je porušením Smlouvy a zakládá nárok na smluvní pokutu dle článku 7.

15.5 Vypořádání hardware se řídí článkem 11.

16 Vyšší moc

16.1 Smluvní strany se zprošťují odpovědnosti za nesplnění povinností z této Smlouvy po dobu trvání vyšší moci v rozsahu, v jakém nebylo možno neplnění předejít.

16.2 Za vyšší moc se považuje událost nezávislá na vůli smluvních stran, kterou nebylo možno předvídat ani odvrátit — zejména přírodní katastrofa, válka, stávka. Za vyšší moc se nepovažují technické poruchy zařízení Poskytovatele, nedostatek personálu Poskytovatele ani výpadek subdodavatelů Poskytovatele.

16.3 Dotčená strana je povinna oznámit druhé straně vznik a ukončení vyšší moci do 48 hodin od okamžiku, kdy se o ní dozvěděla nebo měla dozvědět.

16.4 Pokud vyšší moc trvá déle než 60 kalendářních dnů, je kterákoliv strana oprávněna od Smlouvy odstoupit bez nároku na náhradu škody.

17 Registr smluv a compliance

17.1 Objednatel zajistí uveřejnění Smlouvy v Registru smluv dle zákona č. 340/2015 Sb. ve strojově čitelné podobě. Poskytovatel je povinen poskytnout k tomu nezbytnou součinnost. Přílohy obsahující bezpečnostně citlivé informace (Příloha č. 4 — Minimální bezpečnostní požadavky) budou z uveřejnění vyloučeny dle § 3 odst. 1 zákona č. 340/2015 Sb. v rozsahu, v jakém by jejich zveřejnění ohrozilo bezpečnost Služby; o rozsahu vyloučení rozhodne Objednatel.

17.2 Poskytovatel prohlašuje, že splňuje základní způsobilost dle § 74 ZZVZ a že po celou dobu plnění bude dodržovat právní předpisy České republiky a EU.

17.3 Poskytovatel prohlašuje, že vůči němu není vedeno insolvenční řízení, exekuce ani výkon rozhodnutí, a zavazuje se o zahájení takového řízení neprodleně informovat Objednatele.

18 Řešení sporů

18.1 Smluvní strany se zavazují řešit spory vzniklé z nebo v souvislosti s touto Smlouvou přednostně smírnou cestou v následujícím pořadí: jednání kontaktních osob (do 10 pracovních dnů od vzniku sporu), eskalace na Steering Committee (do 20 pracovních dnů), jednání na úrovni statutárních orgánů (do 30 pracovních dnů).

18.2 Pokud smírné řešení nevede k dohodě do 30 pracovních dnů od vzniku sporu, jsou strany oprávněny předložit spor k rozhodnutí mediátorovi zapsanému v seznamu mediátorů vedeném Ministerstvem spravedlnosti ČR. Mediace se koná v Praze a její náklady nesou strany rovným dílem.

18.3 Pokud mediace nevede k dohodě do 60 kalendářních dnů od jejího zahájení, nebo pokud se kterákoliv strana mediace nezúčastní, je kterákoliv strana oprávněna předložit spor k rozhodnutí věcně příslušnému soudu v Praze.

18.4 Zahájení eskalačního nebo mediačního postupu nemá vliv na povinnost smluvních stran plnit závazky z této Smlouvy.

19 Závěrečná ustanovení

19.1 Smlouva se řídí právním řádem České republiky, zejména zákonem č. 89/2012 Sb.

19.2 Smlouva může být měněna pouze písemnými dodatky podepsanými oběma smluvními stranami, v souladu s § 222 ZZVZ. Zadavatel si vyhrazuje změny dle § 100 odst. 1 ZZVZ v rozsahu stanoveném v zadávací dokumentaci.

19.3 Nedílnou součástí Smlouvy jsou přílohy:

Příloha č. 1 — Technické zadání a konfigurace HW,

Příloha č. 2 — SLA (Service Level Agreement),

Příloha č. 3 — Cenová příloha,

Příloha č. 4 — Minimální bezpečnostní požadavky,

Příloha č. 5 — DPA (Smlouva o zpracování osobních údajů),

Příloha č. 6 — Realizační tým,

Příloha č. 7 — Kontaktní osoby a komunikace,

Příloha č. 8 — Exit plán / Reversibility plan,

Příloha č. 9 — Akceptační kritéria Go-Live.

19.4 Je-li některé ustanovení Smlouvy neplatné, neúčinné nebo nevynutitelné, zůstávají ostatní ustanovení nedotčena, pokud z povahy Smlouvy nebo z okolností nevyplývá, že takové ustanovení nelze oddělit.

19.5 Smlouva je vyhotovena elektronicky a podepsána kvalifikovanými elektronickými podpisy.

Objednatel: V Praze dne dle elektronického podpisu

Poskytovatel: V Praze dne dle elektronického podpisu

Příloha č. 1 — Technické zadání a konfigurace HW

Kapacita a škálování

Řešení bude dimenzováno na minimálně 140 aktivních uživatelů (seatů) včetně výkonové rezervy pro CI/CD zátěž a růst objemu dat.

Architektura

Veškeré komponenty budou provozovány výhradně v perimetru Objednatele.

Architektura nabízeného řešení je postavena na dvou fyzických serverech pro produkční workload a jednom dedikovaném serveru pro zálohování. Na produkčních serverech bude nasazena virtualizace ProxMox VE a veškerý workload poběží formou virtuálních serverů na platformě Linux.

Logické rozdělení rolí:

- GitLab Core – řídicí engine celého systému (aplikační vrstva GitLab, interní DB, repozitáře, registry).
- CI/CD runnery – dvě dedikované VM s GitLab Runner pro paralelní běh CI/CD jobů.
- Úložiště repozitářů a artefaktů – logicky a síťově oddělené ve vlastním datastoru na enterprise NVMe. Oddělení od ostatních VM a komponent je zajištěno na úrovni hypervisoru (vyhrazený datastore), na úrovni VM (vlastní storage VM, oddělené credentials a oprávnění) a na úrovni sítě (vlastní VLAN, ACL na firewall). Smysl požadavku §3 zadávací dokumentace na „oddělené úložiště enterprise třídy" tím je naplněn – data repozitářů nesdílí I/O cestu ani filesystem s ostatními komponentami, jsou na NVMe enterprise třídy a mají vlastní snapshot a replikační politiku.
- Záloha – realizována na dedikovaném fyzickém serveru zcela mimo produkční servery (viz bod 2 níže).

GitLab Core a runnery budou realizovány jako OCI kontejnery pod Kubernetes, což zajistí běh všech procesů v izolovaných prostředích.

Hardware

Objednatel neposkytne vlastní HW pro provoz ani zálohování; Poskytovatel dodá HW jako součást plnění.

Poskytovatel dodá a uvede do provozu celkem tři fyzické servery HPE ProLiant DL325 Gen11. Rozdělení rolí je následující:

- 2× HPE ProLiant DL325 Gen11 (AMD EPYC 9335, 768 GB RAM, 4× 3,2 TB NVMe SSD) – produkční workload (GitLab Core + CI/CD runnery + úložiště repozitářů/artefaktů na odděleném datastoru).
- 1× HPE ProLiant DL325 Gen11 (AMD EPYC 9015, 32 GB RAM, 2× 4 TB SATA HDD) – dedikovaný backup server, fyzicky oddělený od produkčních serverů.

Zálohování je realizováno nástrojem ProxMox Backup Server. Zálohovaná data jsou ukládána výhradně na dedikovaný backup HW, zcela mimo produkční výpočetní servery. Vlastní zálohovací provoz probíhá dedikovanou sítí (fyzicky oddělenou nebo logicky pomocí VLAN); na úrovni firewall jsou povoleny pouze backup-traffic porty, ostatní směrování mezi produkční a backup sítí je zakázáno.

Zálohy budou šifrovány AES-256-GCM v klidu i při přenosu — šifrování bude aktivováno před prvním zálohováním. Klíče budou spravovány v perimetru Objednatele.

Pro zajištění neměnnosti záloh (WORM/immutability) bude na úrovni ProxMox Backup Serveru aktivována ochrana proti přepsání a smazání kombinací verified pruning a immutable tier (retention lock na datastoru). Tím je naplněn požadavek na immutability/WORM ochranu záloh. Retence záloh je nastavena minimálně na 14 dní. Test obnovy bude prováděn minimálně 1× ročně a jeho výstup bude součástí ročního, resp. měsíčního reportu.

Navržená architektura je dimenzována na povinné minimum 80 aktivních uživatelů včetně výkonové rezervy pro CI/CD zátěž. Kapacitní model pro scénář 80 uživatelů:

Parametr	**Scénář 80 uživatelů**
GitLab Core – vCPU	16 vCPU
GitLab Core – RAM	64 GB
GitLab Core – úložiště	1 TB NVMe
CI/CD runnery – počet VM	1–2 aktivní runner VM
CI/CD runnery – vCPU/VM	12 vCPU
CI/CD runnery – RAM/VM	32 GB
Úložiště repozitářů/artefaktů	5–10 TB NVMe
Backup kapacita (retence 14 dní)	cca 15 TB
IOPS produkčního úložiště (ø)	≥ 5 000 IOPS
Síťová propustnost (produkční)	10 GbE
Síťová propustnost (backup)	10 GbE dedikovaně

Fyzické servery disponují souhrnnou kapacitou víc než 1,5 TB RAM, 128 vláken (2× 32 jader/64 vláken EPYC 9335) a 12,8 TB NVMe SSD, což výrazně přesahuje výše uvedené požadavky a vytváří významnou rezervu pro nárazové CI/CD zátěže i pro pozdější navýšení počtu uživatelů v rámci dohodnutého škálování (až 140 uživatelů orientačně).

Škálovací strategie: horizontální – při spuštění CI/CD jobu se využije buď existující runner, nebo se runner vytvoří automatizovaně jako dočasný kontejner; po dokončení jobu je kontejner recyklován nebo zrušen. Vertikální škálování GitLab Core VM je možné v rámci kapacity fyzických hostitelů až do 32 vCPU / 128 GB RAM. Tím je zajištěna možnost plynulého pokrytí poptávky až do orientačního kapacitního maxima 140 uživatelů.

Poskytovatel předá inventární seznam HW včetně SN a servisních podmínek.

Vlastnictví HW a převod po 5 letech

HW bude po dobu trvání smlouvy (60 měsíců) ve vlastnictví Poskytovatele; Objednatel je oprávněn HW užívat výhradně pro účely provozu služby.

Po uplynutí 60 měsíců od zahájení poskytování služby (řádném ukončení pětiletého období) Poskytovatel převede vlastnické právo k veškerému dodanému HW na Objednatele za zůstatkovou kupní cenu [redacted] bez DPH; k ceně bude připočtena DPH dle právních předpisů, je-li aplikovatelná.

Převod bude realizován na základě předávacího protokolu a kupní smlouvy / převodního ujednání; Poskytovatel prohlásí, že HW není zatížen právy třetích osob (zejm. zástavním právem, výhradou vlastnictví, leasingem, exekucí) a že na Objednatele přechází HW bez právních vad.

Poskytovatel předá Objednateli veškerou dokumentaci k HW (záruky, servisní historie, konfigurace, licenční/dodavatelské doklady, seznam SN) a provede součinnost k převodu (např. převod registrací výrobce, servisních kontraktů, pokud to výrobce umožňuje).

V případě ukončení smlouvy před uplynutím 60 měsíců se s HW naloží dle Exit plánu; převod za [redacted] se uplatní pouze při řádném doběhu pětiletého období, není-li mezi stranami dohodnuto jinak.

Integrace s IAM

GitLab nativně podporuje autentizaci proti externím IAM. Řešení počítá s napojením na centrální Active Directory doménu, případně na existující LDAP. Podporovány jsou protokoly LDAP, AD, SAML 2.0, OIDC a MFA. Součástí konfigurace bude mapování rolí GitLab (Developer, Maintainer, Owner) na skupiny v IAM Objednatele a auditní logování přístupů, změn oprávnění a administrativních zásahů.

Migrace stávajících dat

Technický postup migrace stávajících dat GitLab:

Postup:

- Krok 0 – Analýza stávajícího prostředí (verze GitLab, počty projektů, alokovaný diskový prostor, konfigurace, CI/CD runnery dedikované i sdílené, externí integrace).
- Krok 1 – Export dat ze zdrojového GitLab pomocí nativních zálohovacích nástrojů (gitlab-backup create).
- Krok 2 – Přenos dat výhradně v perimetru Objednatele do cílového prostředí; import dat pomocí gitlab-backup restore.
- Krok 2 (alternativně) – V případě nekompatibility verzí lze využít klonování projektů pomocí vestavěné funkcionality nástroje Git.
- Krok 3 – Finalizace: kontrola přemigrovaných projektů, rekonfigurace CI/CD manifestů s ohledem na novou konfiguraci runnerů, akceptační test.

Předpoklady:

- Přístup s administrátorským oprávněním na zdrojový GitLab a oprávnění k vytvoření zálohy.
- Síťová dostupnost cílového prostředí z místa zdrojového prostředí v perimetru Objednatele.
- Schválené cutover okno (typicky 4 hodiny mimo pracovní dobu).

Rizika a omezení:

- Nekompatibilita verzí GitLab (řešeno upgrade-path před exportem).
- Velké LFS objekty a binární artefakty (řešeno paralelním přenosem a verifikací kontrolních součtů).
- Závislost na externích integracích (webhooks, runner tokeny, deploy keys) – řešeno seznamem rebindů provedeným po importu.

Etapizace:

- Analýza zdroje → pilotní migrace 1–2 projektů → generální zkušební migrace → ostrá cutover migrace → verifikace a předání.

Součinnost Objednatele:

- Zpřístupnění zdrojového GitLab s administrátorskými právy.
- Schválení migračního okna a komunikační podpora vůči koncovým uživatelům.
- Akceptační test po migraci a podpis akceptačního protokolu.

Migrace bude realizována výhradně v perimetru Objednatele; data v žádné fázi nebudou přenášena mimo území EU/EHP a nebude k nim umožněn vzdálený přístup ze třetích zemí.

Monitoring (mimo migraci): V rámci provozu služby plánujeme nasazení dedikovaného Zabbix serveru pro monitoring dostupnosti, výkonu a kapacit GitLab i HW. Alerty budou směrovány do ticketingu a kontaktním osobám Objednatele dle dohodnuté eskalační matice.

Zákazy a omezení (OÚ, EU/EHP, vzdálené přístupy)

Zákaz přenosu osobních údajů mimo EU/EHP: Poskytovatel nebude zpracovávat ani zpřístupňovat osobní údaje mimo území EU/EHP, ani neuumožní jakýkoliv jejich přenos (včetně vzdáleného přístupu) mimo EU/EHP.

Zákaz vzdáleného přístupu ze třetích zemí: Poskytovatel neumožní vzdálený administrátorský ani podpůrný přístup k systémům a datům z území třetích zemí (mimo EU/EHP), a to ani dočasně.

Porušení výše uvedených zákazů se bude považovat za podstatné porušení smlouvy.

Konfigurace hardware

PN	Popis	Počet
P54200-B21	**HPE DL325 G11 4LFF CTO Svr**	**1**
P72661-B21	AMD EPYC 9015 CPU for HPE	1
P64985-B21	HPE 32GB 2Rx8 PC5-6400B-R Smart Kit	1
861683-B21	HPE 4TB SATA 7.2K LFF LP HDD	2
P01366-B21	HPE 96W Smart Stg Li-ion Batt 145mm Kit	1
P58335-B21	HPE MR408i-o Gen11 SPDM Storage Cntlr	1
P10115-B21	BCM 57414 10/25GbE 2p SFP28 OCP3 Adptr	1
455883-B21	HPE BLc 10G SFP+ SR Transceiver	2
P58462-B21	HPE DL3XX Gen11 1U Perf Fan Kit	7
P03178-B21	HPE 1000W FS Ti Ht Plg PS Kit	2
BD505A	HPE iLO Adv 1-svr Lic 3yr Support	1
S1A05A	HPE Cmp Cloud Mgmt Srv FIO Enablement	1
P52341-B21	HPE DL3XX Gen11 Easy Install Rail 3 Kit	1
P58456-B21	HPE DL3XX Gen11 Stnd 1U Heat Sink Kit	1
R7A12AAE	HPE COM Std 5yr Up ProLiant SaaS	1
HU4B2A5	HPE 5Y Tech Care Basic SVC	1
HU4B2A5 R2M	HPE iLO Advanced Non Blade Support	1
HU4B2A500DE	HPE ProLiant DL325 Gen11 Support	1

P54199-B21	**HPE DL325 G11 8SFF CTO 5vr**	**2**
P72656-B21	AMD EPYC 9335 CPU for HPE	2
P64986-B21	HPE 64GB 2Rx4 PC5-6400B-R Smart Kit	24
P54999-B21	HPE DL325 G11 8SFF x1Tmode U.3 BC BP Kit	2
P65015-B21	HPE 3.2T NVMe MU SFF BC U.3ST V2 MV SSD	4
P01366-B21	HPE 96W Smart Stg Li-ion Batt 145mm Kit	2
P58335-B21	HPE MR408i-o Gen11 SPDM Storage Cntlr	2
P10115-B21	BCM 57414 10/25GbE 2p SFP28 OCP3 Adptr	2
455883-B21	HPE BLc 10G SFP+ SR Transceiver	4
P58462-B21	HPE DL3XX Gen11 1U Perf Fan Kit	14
P03178-B21	HPE 1000W FS Ti Ht Plg PS Kit	4
BD505A	HPE iLO Adv 1-svr Lic 3yr Support	2
S1A05A	HPE Cmp Cloud Mgmt Srv FIO Enablement	2
P59619-B21	HPE DL325 Gen11 8SFF x1 OCP2 TM Cbl Kit	2
P52351-B21	HPE DL3XX Gen11 Easy Install Rail 2 Kit	2
P58457-B21	HPE DL3XX Gen11 Perf 1U Heat Sink Kit	2
R7A12AAE	HPE COM Std 5yr Up ProLiant SaaS	2
HU4B2A5 R2M	HPE 5Y Tech Care Basic SVC	1
HU4B2A5	HPE iLO Advanced Non Blade Support	2
HU4B2A500DE	HPE ProLiant DL325 Gen11 Support	2

Příloha č. 2 — SLA (Service Level Agreement)

Předmět a rozsah SLA

Tato Příloha č. 2 (Service Levele Agreement, dále jen „SLA") stanová závazné a měřitelné parametry úrovně poskytování služby GitLab (dále jen „Služba") poskytované Poskytovatelem Objednateli formou managed service a na základě uzavřené Smlouvy.

SLA vymezuje zejména:

- garantovanou dostupnost Služby,
- kategorizaci incidentů a závazné reakční a řešící lhůty,
- pravidla měření a reportingu,
- bezpečnostní a provozní omezení,
- vazbu na sankční mechanismus dle Smlouvy.

SLA se vztahuje na Službu jako nedělitelný celek, zahrnující zejména:

- aplikační vrstvu GitLab,
- CI/CD komponenty a runnery,
- databázové a aplikační služby,
- infrastrukturu (výpočetní zdroje, síťové prvky, virtualizaci),
- úložiště dat a mechanismy zálohování,
- veškerý dodaný hardware.

Hardware není předmětem samostatné HW SLA. Jeho dostupnost, výkon, kapacita a spolehlivost jsou nedílnou součástí poskytované Služby. Oddělování odpovědnosti Poskytovatele za HW a SW se nepřipouští.

Provozní režim a dostupnost služby

Provozní okno

Služba je provozována v definované provozním okně, kterým jsou:

- pracovní dny (pondělí až pátek),
- v čase od 7:00 do 18:00.

V tomto provozním okně Poskytovatel garantuje dostupnost Služby a plnění parametrů stanovených touto SLA.

Cílová dostupnost

Cílová měsíční dostupnost Služby činí minimálně 97 % v rámci provozního okna.

Dostupnost je počítána jako poměr doby, kdy je Služba plně funkční a dostupná koncovým uživatelům, k celkové době provozního okna v daném kalendářním měsíci.

Za nedostupnost služby se považuje stav, kdy:

- Služba není dostupná vůbec, nebo
- není možné využívat její klíčové funkcionality.

Pro účely výpočtu dostupnosti platí, že:

- doba nedostupnosti se počítá v minutách (od okamžiku, kdy je nedostupnost prokazatelně zajištěna, do okamžiku obnovení plné funkčnosti),
- do výpočtu se nezahrnují žádné oznamené plánované odstávky provedené mimo provozní okno,
- doba nedostupnosti zahrnuje dopady jak na HW, tak na SW, protože Služba je posuzována jako nedělitelný celek.

Plánované odstávky a servisní okna

Plánované odstávky

Plánovaná odstávka je předem oznámený zásah do Služby, jehož cílem je zejména:

- údržba infrastruktury,
- aplikace bezpečnostních záplat,
- aktualizace aplikace nebo jejich komponent,
- preventivní technické zásahy.

Plánované odstávky:

- probíhají mimo provozní okno,
- nezapočítávají se do výpočtu dostupnosti Služby,
- jsou Objednateli oznámeny předem vhodným komunikačním kanálem.

Servisní okno

Standardní servisní okno je stanoveno následovně – každé úterý v čase od 19:00 do 24:00. V servisním okně je Poskytovatel oprávněn provádět plánované zásahy bez negativního dopadu do SLA.

Kategorizace incidentů

Incidentem se rozumí jakákoli událost, která má nebo může mít negativní dopad na dostupnost, bezpečnost služby nebo funkčnost Služby.

Incidenty jsou klasifikovány podle jejich dopadů následujícím způsobem.

Kritická porucha

Kritická porucha představuje stav, kdy:

- je Služba zcela nedostupná, nebo
- dojde ke kritickému bezpečnostnímu incidentu (např. únik dat, kompromitace systému, neoprávněný přístup).

Reakční doba do 24 hodin od nahlášení.

Doba vyřešení HW NBD+1, SW vyřešení best effort.

Vážná porucha

Vážná porucha je charakterizována:

- významnou degradací klíčových funkcí Služby,
- omezením provozu, které má dopad na větší část uživatelů, avšak Služba není zcela nedostupná.

Reakční doba následující pracovní den (NBD).

Doba vyřešení vyřešení HW NBD+3.

Běžná porucha

Běžná porucha zahrnuje:

- dílčí omezení funkčnosti,
- drobné chyby bez zásadního dopadu na provoz,
- požadavky na úpravu konfigurace.

Reakční doba následující pracovní den (NBD).

Doba vyřešení best effort.

Řešení incidentů

Reakční dobou se rozumí doba, do které Poskytovatel zahájí aktivní diagnostiku a práce na odstranění incidentu.

Dobou vyřešení se rozumí doba, do které je:

- obnovena plná funkčnost Služby, nebo
- minimalizován dopad incidentu na úroveň nižší kategorie.

Řešení incidentu může zahrnovat zásahy do:

- aplikace,
- konfigurace,
- infrastruktury,
- hardware.

V rámci řešení incidentů není přípustné oddělovat HW a SW zásahy.

Hlášení incidentů a komunikace

Poskytovatel zajišťuje jedno centrální kontaktní místo (SPOC) pro hlášení incidentů.

Při řešení kritické poruchy Poskytovatel:

- průběžně informuje Objednatele o stavu,
- poskytuje informaci o přijatých opatřeních a předpokládaném termínu obnovení.

Eskalace

V případě, že hrozí nedodržení parametrů SLA je Poskytovatel povinen incident eskalovat na odpovídající úroveň řízení a informovat Objednatele.

Eskalace je nedílnou součástí procesu řízení incidentů.

Měření a reporting

Dodržování SLA je průběžně monitorováno Poskytovatelem.

Poskytovatel poskytuje Objednateli pravidelné provozní přehledy, obsahující zejména:

- vyhodnocení dostupnosti Služby,
- přehled incidentů,
- Informace o významných provozních událostech.

Sankce za nedodržení SLA

Nedodržení parametrů stanovených touto SLA je považováno za porušení smluvních povinností Poskytovatele.

Uplatnění sankcí se řídí příslušnými ustanoveními Smlouvy.

Bezpečnostní omezení

Služba je provozována výhradně v rámci EU/EHP.

Vzdálený administrátorský nebo podpůrný přístup ze třetích zemí (mimo EU/EHP), není povolen, a to ani dočasně.

Porušení tohoto ustanovení je považováno za podstatné porušení Smlouvy.

Vymezení odpovědností smluvních stran a součinnost

Odpovědnost Poskytovatele

Poskytovatel odpovídá za:

- zajištění provozu Služby (včetně infrastruktury, úložišť, zálohování a veškerého dodaného hardware),
- zajištění dostupnosti a organizaci plánovaných odstávek,
- provoz a údržbu Služby, včetně aplikace bezpečnostních záplat a aktualizací v souladu se servisním oknem,
- nepřetržité přijímání incidentů prostřednictvím jednotného kontaktního místa jejich řešení v parametrech,
- vedením evidence incidentů a poskytování reportingu,
- dodržování bezpečnostních omezení, zejména zákazu vzdáleného administrátorského a podpůrného přístupu ze třetích zemí mimo EU/EHP.

Odpovědnost Objednatele

Objednatel odpovídá zejména za:

- určení kontaktních osob (primární/sekundární) pro provozní komunikaci, eskalace a schvalování změn,
- zajištění součinnosti při diagnostice incidentu (např. poskytnutí relevantních logů z prostředí Objednatele, potvrzení dopadu na uživatele, test obnovy),
- včasné poskytování informací, které jsou nezbytné pro provoz Služby v Perimetru Objednatele,
- dodržení provozních a bezpečnostních pokynů, které jsou nezbytné pro bezpečný provoz Služby.

Součinnost a vyloučení odpovědnosti

Poskytovatel je nedodržené parametrů SLA způsobeno prokazatelně:

- nedostatečnou součinnost Objednatele,

- zásahy Objednatele nebo třetích stran mimo kontrolu Poskytovatele,
- nedostupností systémů Objednatele, které jsou pro využívání Služby nezbytné (např. lokální síťové služby, přístupové prvky, integrace). Poskytovatel neodpovídá za takto vzniklé škody, a to v rozsahu prokazatelně způsobeném uvedenými okolnostmi.

Poskytovatel je však povinen i v těchto případech poskytnout přiměřenou součinnost k obnovení provozu a průběžně informovat Objednatele o zjištěních.

Rozšířená pravidla měření a reportingu

Způsob měření dostupnosti

Poskytovatel měří dostupnost Služby automatizovanými nástroji. Měření musí být zpětně dohledatelné a musí umožnit doložení:

- času vzniku nedostupnosti,
- času obnovení plné funkčnosti,
- charakteru události (incident / plánovaná odstávka),
- dopadu na Službu.

Měsíční provozní report

Poskytovatel předkládá Objednateli pravidelný měsíční provozní report, který obsahuje minimálně:

- Vyhodnocení dostupnosti služby v procentech a plnění SLA proti smluvním cílům.
- Přehled incidentů – počty dle priorit, čas otevření / uzavření, RCA u P1 (a vybraných P2).
- Klíčové provozní události – plánované odstávky, kapacitní trendy CPU / RAM / storage.
- Provedené změny – seznam change recordů (RFC), změnový log, release notes.
- Bezpečnostní záplaty – aplikované patche GitLab, OS i souvisejících komponent, patch log a plán patchování.
- Plánované aktivity na následující měsíc.

Report je předkládán nejpozději do 5. pracovního dne následujícího kalendářního měsíce, není-li ve Smlouvě stanoveno jinak.

Nezávislá kontrola a součinnost

Objednatel je oprávněn provozovat vlastní nezávislý monitoring dostupnosti z prostředí Objednatele. Poskytovatel poskytne nezbytnou součinnost pro jeho instalaci a konfiguraci.

V případě rozporu mezi měřením Poskytovatele a nezávislým měřením Objednatele se do doby vyjasnění považuje za směrodatný výsledek nepříznivější pro Poskytovatele.

Poskytovatel na vyžádání zpřístupní Objednatele relevantní podkladová data z monitoringu ve strojově čitelném formátu.

Vazba na sankční mechanismus a vyhodnocení porušení SLA

Obecná vazba na Smlouvu

Nedodržení parametrů této SLA (zejména dostupnosti nebo reakční/řešící lhůt) je porušením smluvních povinností Poskytovatele.

Sankce se uplatní v souladu se Smlouvou, porušení parametrů této přílohy se promítá do sankčního mechanismu automaticky dle smluvních podmínek.

Vyhodnocení a uplatnění sankcí

Vyhodnocení plnění SLA probíhá měsíčně na základě reportu.

Objednatel je oprávněn uplatnit sankce, pokud:

- je v reportu doloženo nesplnění cílové dostupnosti, nebo
- je doloženo nedodržení reakční doby či doby u vyřešení incidentů.

Případné námitky Poskytovatele musí být uplatněny bez zbytečného odkladu a musí být doloženy relevantními podklady (logy, tikety, monitoring), jinak se má za to, že údaje v reportu jsou správné.

Detailní řízení incidentů (proces, komunikace, eskalační hladiny)

Proces řízení incidentů

Poskytovatel provozuje proces řízení incidentů tak, aby bylo zajištěno:

- přijetí hlášení a založení záznamu v tiketovacím systému,
- klasifikace incidentu a potvrzení Objednateli,
- zahájení diagnostiky v reakční době,
- průběžná komunikace stavu řešení,
- obnovení služby (nebo snížení závažnosti) v době vyřešení,
- uzavření incidentů včetně závěrečného shrnutí.

Potvrzení přijetí a kategorizace

Poskytovatel potvrdí přijetí hlášení incidentu a přiřadí mu kategorii závažnosti. V případě nesouhlasu Objednatele s přiřazenou kategorií se do doby vyjasnění uplatní vyšší kategorie, aby byla chráněna kontinuita provozu a nedošlo k podhodnocení dopadu.

Komunikační režim při kritické poruše

Při řešení kritické poruchy Poskytovatel:

- poskytuje průběžné informace o postupu,
- sdělí předpokládaný čas obnovení a aktualizuje jej při změně situace,
- po obnovení služby poskytne stručné shrnutí příčiny a provedených opatření.

Eskalační hladiny

Poskytovatel zavede minimálně následující eskalační hladiny:

- L1 (Service Desk / dispečink) – příjem hlášení, základní diagnostika, koordinace,
- L2 (specialista služby / infrastruktury) – odborné řešení incidentu,
- L3 (seniorní expert / architekt) – řešení složitých a opakujících se problémů, návrh nápravných opatření,
- Management eskalace – při riziku nedodržení SLA nebo při incidentu se zásadním dopadem.

Eskalace se provede automaticky v případě, že:

- incident se blíží k vyčerpání významné části času doby vyřešení,
- existuje riziko opakovaného výskytu nebo bezpečnostního dopadu,
- incident vyžaduje koordinaci více týmů nebo dodavatelů.

Post-incidentní vyhodnocení (RCA)

U kritických poruch Poskytovatel zpracuje post-incidentní vyhodnocení (Root Cause Analysis), které zahrne:

- časovou osu události,
- identifikovanou příčinu,
- dočasná a trvalá nápravná opatření,
- doporučení pro prevenci opakování.

RCA je poskytnuto Objednateli v přiměřené lhůtě odpovídající závažnosti incidentu.

Za nedostupnost se považuje stav, kdy:

- Služba není dostupná vůbec, nebo
- není možné využívat její klíčové funkcionality.

Způsob hlášení incidentů

1. Založením servisního požadavku: na servisním portále https://helpdesk.storageone.cz
2. E-mailem: e-mailová adresa support@storageone.cz
3. Telefonicky: na tel číslo +420 910 800 875

V případě hlášení incidentů mimo pracovní hodiny, tj. během víkendů, státních svátků a v době od 17:00 hod do 8:00 hod v běžné pracovní dny, lze hlásit incidenty pouze telefonicky na výše uvedené telefonní číslo.

V případě telefonického hlášení incidentu je od Objednatele požadováno dodatečné zaslání emailu se servisním požadavkem, případně založení servisního požadavku v helpdesku Poskytovatele.

Příloha č. 3 — Cenová příloha

A. Jednotkové ceny

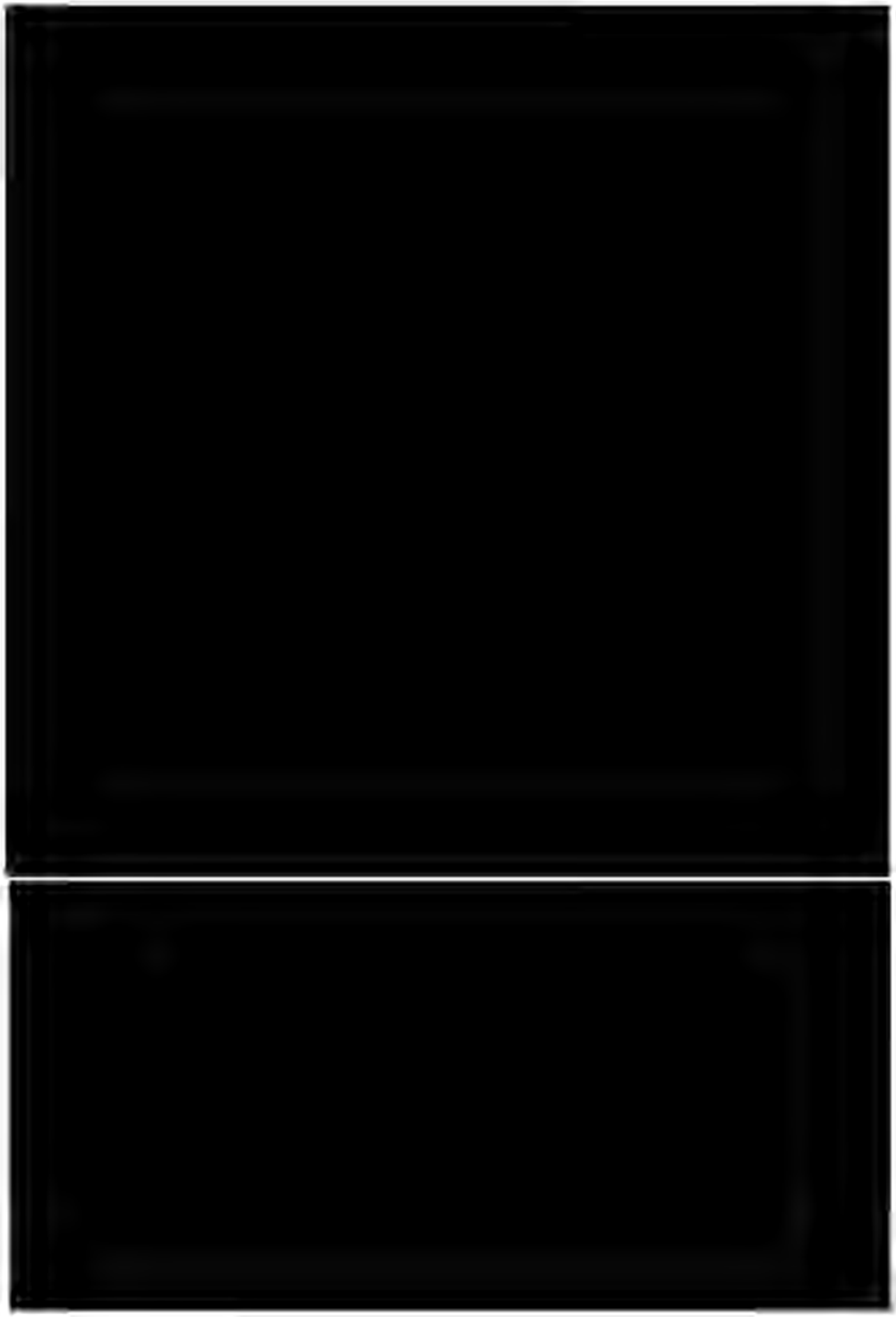
Položka	Jednotka	Jednotková cena v Kč bez DPH	Poznámka
Managed service GitLab – provoz + HW + backup (bez ceny licence)	1 uživatel / rok	[redacted]	Cena služby za seat/rok pro minimum 80 licencí; sizing a služby dimenzované na 140
Marže na licenci GitLab Ultimate nad cenu distributora	% / licence	[redacted]	Neměnná po celou dobu smlouvy; použije se při ročním navýšení licencí

B. Scénáře a TCO

Scénář	Počet licencí	Roční cena služby v Kč bez DPH	TCO 5 let bez DPH	Poznámka
Minimum (povinné)	80	[redacted]		Nepodkročitelné minimum
Kapacitní maximum (orientačně)	140			Orientačně pro škálování; HW i služby stále pro 140

C. Migrace stávajících dat (informativní; mimo hodnocení)

Položka	Jednotka	Cena bez DPH
Migrace stávajících dat GitLab	paušál / hodina	[redacted]
Odhadovaný rozsah prací	hodiny	



Příloha č. 5 — DPA (Smlouva o zpracování osobních údajů)

Smlouva o zpracování osobních údajů (DPA)

uzavřená dle čl. 28 nařízení (EU) 2016/679 (GDPR) jako Příloha č. 5 Smlouvy o zajištění služby GitLab v perimetru Objednatele č. 20260167 (dále jen „Smlouva")

1 — Strany a jejich role

Správce osobních údajů: VZLU AEROSPACE, a.s., IČ: 00010669, se sídlem Beranových 130, 199 00 Praha 9 (Objednatel dle Smlouvy). Zpracovatel osobních údajů: STORAGE ONE, a.s., IČ: 02301245, se sídlem Jeremiášova 947/16, 155 00 Praha 5 – Stodůlky (Poskytovatel dle Smlouvy). Tato DPA je nedílnou součástí Smlouvy a její ustanovení mají přednost před obecnými ustanoveními Smlouvy v rozsahu, v jakém se týkají zpracování osobních údajů.

2 — Předmět, doba a povaha zpracování

Zpracování probíhá po celou dobu poskytování Služby dle Smlouvy a v rozsahu nezbytném pro provoz, podporu, bezpečnost, logování, zálohování a obnovu služby GitLab. Povaha zpracování zahrnuje: hosting a provoz aplikace, správu uživatelských účtů a oprávnění, logování přístupů a operací, zálohování a obnovu dat, monitoring bezpečnostních událostí.

3 — Kategorie údajů a subjektů údajů

Kategorie osobních údajů: identifikační údaje uživatelů (jméno, příjmení, e-mailová adresa, uživatelské jméno), autentizační a autorizační údaje (přihlašovací údaje, role, skupiny, oprávnění), auditní údaje (logy přístupů, operací, změn konfigurace — obsahující IP adresy, časové značky, identifikátory uživatelů), metadata projektů a repozitářů (názvy, popisy, commitové zprávy obsahující jména autorů). Subjekty údajů: zaměstnanci a spolupracovníci Správce, zaměstnanci dceřiných společností Správce a další oprávněné osoby využívající GitLab na základě pověření Správce.

4 — Pokyny Správce

Zpracovatel zpracovává osobní údaje výhradně na základě dokumentovaných pokynů Správce. Za dokumentovaný pokyn se považuje tato DPA, Smlouva a její přílohy a jednotlivé písemné pokyny zaslané kontaktní osobou Správce. Pokud Zpracovatel obdrží pokyn, který podle jeho názoru porušuje GDPR nebo jiný právní předpis, je povinen na to Správce bez zbytečného odkladu upozornit a takový pokyn nesplnit do doby, než Správce pokyn potvrdí nebo upraví.

5 — Důvěrnost a personální opatření

Zpracovatel zajistí, že osoby oprávněné ke zpracování osobních údajů jsou vázány povinností mlčenlivosti (smluvní nebo zákonnou). Zpracovatel uplatňuje princip nejmenších oprávnění — přístup k osobním údajům mají pouze osoby, které jej nezbytně potřebují pro plnění svých úkolů. Zpracovatel provádí pravidelnou recertifikaci přístupů minimálně jednou za 6 měsíců.

6 — Technická a organizační opatření (TOMs)

Zpracovatel implementuje a udržuje opatření odpovídající rizikům zpracování, minimálně v rozsahu Přílohy č. 4 Smlouvy (Minimální bezpečnostní požadavky). Konkrétně zajistí: šifrování

osobních údajů při přenosu (TLS 1.2+) i v klidu (AES-256 nebo ekvivalent) včetně záloh, řízení přístupu s MFA pro administrátorské účty a zákazem sdílených účtů, oddělení produkčních a záložních dat (síťově i logicky), centralizované logování s retencí minimálně 12 měsíců, monitoring bezpečnostních událostí s alertingem, pravidelné testování a hodnocení účinnosti opatření minimálně jednou ročně. Zpracovatel je povinen na vyžádání Správce doložit aktuální stav TOMs.

7 — Podzpracovatelé

Zpracovatel nesmí zapojit dalšího zpracovatele (podzpracovatele) bez předchozího písemného souhlasu Správce. Žádost o souhlas musí obsahovat identifikaci podzpracovatele, zemi sídla, rozsah zpracování a potvrzení, že podzpracovatel splňuje srovnatelné bezpečnostní požadavky a má sídlo v EU/EHP. Zpracovatel zajistí, že podzpracovatel bude vázán povinnostmi minimálně v rozsahu této DPA. Zpracovatel odpovídá za plnění podzpracovatele jako za plnění vlastní. Zpracovatel je povinen udržovat aktuální seznam podzpracovatelů a předložit jej Správci při podpisu Smlouvy a při každé změně.

8 — Pomoc Správci a výkon práv subjektů údajů

Zpracovatel poskytne Správci součinnost při plnění povinností dle čl. 32–36 GDPR, zejména při: vyřizování žádostí subjektů údajů o výkon práv (přístup, výmaz, oprava, přenositelnost, omezení zpracování, vznesení námitky), posouzení vlivu na ochranu osobních údajů (DPIA) v rozsahu, v jakém se týká Služby, konzultacích s dozorovým úřadem. Zpracovatel je povinen informovat Správce o každé žádosti subjektu údajů obdržené přímo od subjektu do 2 pracovních dnů a nepodnikat žádné kroky bez pokynu Správce. Zpracovatel je povinen odpovědět na žádost Správce o součinnost do 5 pracovních dnů.

9 — Pověřenec pro ochranu osobních údajů

[redacted]

10 — Porušení zabezpečení

Zpracovatel oznámí Správci jakékoliv porušení zabezpečení osobních údajů bez zbytečného odkladu, nejpozději do 24 hodin od okamžiku, kdy se o porušení dozvěděl nebo měl dozvědět. Oznámení obsahuje: popis povahy porušení včetně kategorií a přibližného počtu dotčených subjektů údajů, kontaktní údaje osoby dle čl. 9 této DPA, popis pravděpodobných důsledků, popis opatření přijatých nebo navržených ke zmírnění dopadů. Zpracovatel poskytne Správci plnou součinnost při šetření porušení a při plnění oznamovacích povinností vůči dozorovému úřadu a subjektům údajů.

11 — Audit a kontroly

Správce je oprávněn provést audit zpracování osobních údajů po předchozím oznámení v přiměřené lhůtě (nejméně 10 pracovních dnů). Zpracovatel poskytne přístup k relevantním informacím, systémům, logům a dokumentaci. Audit může provést Správce sám nebo jím pověřený nezávislý auditor vázaný mlčenlivostí. Zpracovatel je povinen bez zbytečného odkladu odstranit nedostatky zjištěné auditem.

12 — Lokalita zpracování a přenosy

Zpracovatel zpracovává osobní údaje výhradně v Perimetru Objednatele (dle definice v čl. I Smlouvy). Zpracovatel nesmí přenášet osobní údaje mimo EU/EHP ani umožnit vzdálený přístup k osobním údajům z území třetích zemí, a to ani dočasně. Porušení tohoto ustanovení je podstatným porušením Smlouvy i této DPA.

13 — Vrácení, přenositelnost a výmaz údajů

Po ukončení Služby Zpracovatel předá Správci veškeré osobní údaje ve strojově čitelném, strukturovaném a běžně používaném formátu (JSON, CSV nebo XML dle volby Správce), umožňujícím přenositelnost dle čl. 20 GDPR. Následně Zpracovatel provede bezpečný výmaz všech kopií včetně záloh, ledaže právní předpis EU nebo členského státu vyžaduje jejich uchování. Zpracovatel vydá Správci písemný protokol o výmazu do 30 kalendářních dnů od potvrzení převzetí dat. Postup je dále upraven v Exit plánu (Příloha č. 8 Smlouvy). Data, jejichž uchování vyžaduje právní předpis, budou uchovávána izolovaně od ostatních dat Zpracovatele a vymazána po uplynutí zákonné lhůty.

14 — Závěrečná ustanovení

Tato DPA je účinná po dobu trvání Smlouvy a po dobu nezbytnou k vypořádání povinností dle čl. 13 této DPA. V případě rozporu mezi DPA a Smlouvou mají v oblasti zpracování osobních údajů přednost ustanovení DPA. DPA se řídí právním řádem České republiky a nařízením (EU) 2016/679.

Příloha č. 6 — Realizační tým

Příloha č. 7 — Kontaktní osoby a komunikace

Příloha č. 8 — Exit plán / Reversibility plan

Cílem této přílohy je zajistit přenositelnost služby, ochranu dat a možnost ukončení smluvního vztahu bez vendor lock-in, včetně vypořádání HW dodaného dodavatelem.

Spouštěče exit procesu

Exit proces se aktivuje zejména: uplynutím doby smlouvy (5 let), výpovědí/odstoupením, opakovaným porušením SLA nebo zásadní změnou bezpečnostních podmínek.

Předání dat a dokumentace

- Kompletní export GitLab (repozitáře, metadata, konfigurace, účty a oprávnění, CI/CD definice).
- Poslední konzistentní zálohy včetně informací potřebných k dešifrování, předané bezpečným kanálem.
- Provozní dokumentace (runbooky, architektura, seznam HW, monitoring, postupy obnovy).

Součinnost při migraci

- Dodavatel poskytne součinnost při migraci k novému dodavateli nebo do interní správy, včetně předání znalostí a podpory testů obnovy/migrace. Minimální rozsah odborných prací v ceně služby (nebo vyšší dle nabídky): minimálně dle článku 15 Smlouvy.

Termíny a milníky

- Předání dat musí být dokončeno do 30 kalendářních dnů od aktivace exit procesu, není-li dohodnuto jinak.

Výmaz dat

- Po potvrzení převzetí dat Zadavateli dodavatel provede bezpečný výmaz všech kopií dat včetně záloh, pokud neexistuje zákonná povinnost uchování. O výmazu vydá protokol.

Vypořádání HW a převod vlastnictví po 5 letech

- Ujednání o HW je závazné a má přednost při vypořádání po ukončení smlouvy:
  - HW je po dobu trvání smlouvy (60 měsíců) ve vlastnictví dodavatele; Zadavatel je oprávněn HW užívat výhradně pro účely provozu služby.
  - Po uplynutí 60 měsíců od zahájení poskytování služby (řádném ukončení pětiletého období) dodavatel převede vlastnické právo k veškerému dodanému HW na Zadavatele za zůstatkovou kupní cenu [redacted] k ceně bude připočtena DPH dle právních předpisů, je-li aplikovatelná.
  - Převod bude realizován na základě předávacího protokolu a kupní smlouvy / převodního ujednání; dodavatel prohlásí, že HW není zatížen právy třetích osob (zejm. zástavním právem, výhradou vlastnictví, leasingem, exekucí) a že na Zadavatele přechází HW bez právních vad.
  - Dodavatel je povinen předat Zadavateli veškerou dokumentaci k HW (záruky, servisní historie, konfigurace, licenční/dodavatelské doklady, seznam SN) a provést součinnost k převodu (např. převod registrací výrobce, servisních kontraktů, pokud to výrobce umožňuje).
  - V případě ukončení smlouvy před uplynutím 60 měsíců se s HW naloží dle Exit plánu; převod za [redacted] se uplatní pouze při řádném doběhu pětiletého období, není-li mezi stranami dohodnuto jinak.

- Dodavatel zajistí, aby převod HW proběhl bez přerušení provozu Zadavatele, pokud Zadavatel rozhodne o pokračování provozu na převzatém HW (např. vlastní správou nebo s jiným dodavatelem).

Bezpečnostní omezení během exit procesu

- Zákaz přenosu osobních údajů mimo EU/EHP: Dodavatel nesmí zpracovávat ani zpřístupnit osobní údaje mimo území EU/EHP, ani umožnit jakýkoliv jejich přenos (včetně vzdáleného přístupu) mimo EU/EHP.
- Zákaz vzdáleného přístupu ze třetích zemí: Dodavatel nesmí umožnit vzdálený administrátorský ani podpůrný přístup k systémům a datům z území třetích zemí (mimo EU/EHP), a to ani dočasně.
- Porušení výše uvedených zákazů se považuje za podstatné porušení smlouvy.

Příloha č. 9 — Akceptační kritéria Go-Live.

Cílem přílohy je sumarizovat základní kritéria pro akceptační testování. Po splnění těchto kritérií bude možné prohlásit celé řešení za plně funkční a schopné provozního nasazení. Výchozím bodem pro zahájení testů je plně nakonfigurovaný systém, plánovaný pro produkční nasazení.

Akceptační kritéria jsou rozdělena do několika úrovní. Pro každou úroveň je navržena sada testů, které by měly skončit pozitivním, předvídatelným výsledkem.

Hardware

Tato sekce zahrnuje testy spojené s hardwarovou vrstvou. Víceméně se jedná o ověření redundance HW komponent

Popis testu	Očekávaný výsledek	Reálný výsledek	Akceptováno
Test redundance napájení	Po vytažení jednoho napájecího kabelu bude server dále v provozu		
Test redundance síťových adaptérů	Po vytažení síťového kabelu (simulace výpadku uplinku) zůstanou služby nadále dostupné a v provozu		
Test výpadku fyzického serveru, test HA	Po vypnutí jednoho serveru (simulace ztráty serveru) zůstanou služby funkční a dostupné		
Test dostupnosti iLO	Webové rozhraní HPE iLO je dostupné a server nereportuje žádné problémy		

Virtualizace

Tato sekce obsahuje testy navržené pro oblast virtualizace. Na obou serverech je instalovaný ProxMox Virtual Environment (PVE)

Popis testu	Očekávaný výsledek	Reálný výsledek	Akceptováno
Test dostupnosti webového managemetnu	Webový interface ProxMoxu je dostupný na obou serverech		
Test clusteru	Konfigurace na obou serverech je synchronní a cluster funkční		
Test vytvoření VM	Na obou serverech je možné vytvořit virtuální server		
Test migrace VM	Zvolený virtuální server je možné za běhu migrovat mezi oběma servery		
Test HA	Při pádu fyzického serveru je zvolený VM automaticky restartován na druhém serveru		

Orchestrace kontejnerů

Veškeré služby infrastruktury pro GitLab, včetně GitLabu samotného běží v OCI kontejnerech, spravovaných orchestrátorem Kubernetes (K8s)

Popis testu	Očekávaný výsledek	Reálný výsledek	Akceptováno
Test funkčnost K8s control plane	Řídicí engine K8s je dostupný a poskytuje požadované informace		
Test vytvoření kontejneru	Je možné vytvářet nové kontejnery, které jsou podle požadovaných kritérií umisťovány na jednotlivé fyzické servery		
Test monitoringu	Pomocí nástrojů K8s lze sledovat zátěž jednotlivých serverů		

Vlastní služby GitLab

GitLab je poměrně komplexní sada služeb, které musí být pro běžný provoz funkční.

Popis testu	Očekávaný výsledek	Reálný výsledek	Akceptováno
Test kontejnerů GitLabu	Kontejnery nevykazují žádné anomálie, nedochází k restartům a logy obsahují pouze informační zprávy		
Test dostupnosti GitLabu	Webové rozhraní GitLabu je dostupné a funkční		
Test napojení na IAM	Do rozhraní GitLab je možné se přihlasit		

	účtem vybraných uživatelů. Ověření těchto uživatelů probíhá mimo GitLab		
Ověření autorizace	Na vybraném projektu nebo skupině projektů mohou pracovat jen autorizovaní uživatelé. Ostatní k projektům nemají přístup		
Test CI/CD	Ve vybraném pojektu bude vytvořena CI/CD pipeline, která bude automaticky spuštěna.		

Zálohování a obnova

Součástí dodaného řešení je dedikovaný server pro zálohování.

Popis testu	**Očekávaný výsledek**	**Reálný výsledek**	**Akceptováno**
Test zálohování	Zálohování vybraných virtuálních serverů je funkční a bez chyb		
Test obnovy	Vybraný virtuální server je možné ze zálohy obnovit		
Test automatizace	Zálohovací joby probíhají podle nastaveného plánu		