Technická specifikace

Zajištění cloudové infrastruktury Města Horní Slavkov

1. SOUHRNNÉ ÚDAJE

1.1. Předmět obecně

Předmětem plnění zakázky je zajištění cloudové infrastruktury (servery a síť) včetně licencí s bezpečným propojením cloudové infrastruktury se sídlem Zadavatele. Dodávané služby musí splňovat bezpečností úroveň **vysoká** dle vyhlášky č. 315/2021 Sb.

1.2. Cena, doba a zajištění

Cena služeb	Cena – hrazena měsíčně na základě objednaných služeb.
Datum zahájení	účinností Smlouvy
Doba poskytování Služeb	Po dobu platnosti Smlouvy
Zádržné	ne
Bankovní záruka	ne
Reklamační lhůta služeb	3 měsíce

1.3. Harmonogram realizace

1.3.1. Zadavatel vyžaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky. Údaj D značí datum účinnosti Smlouvy, údaj Z značí datum, kdy Poskytovatel předal Zadavateli dokončenou část E1.1; čísla značí počet kalendářních dnů. Ve sloupci garant je uveden subjekt zodpovídající za danou část projektu.

Poř. č.	Aktivita projektu	Garant	Termín pro dokončení aktivity
Etapa 1 - dodávky a implementace			
E1.1	Příprava prostředí: a) vytvoření a zprovoznění virtuálních serverů; b) vytvoření bezpečného propojení mezi DC Poskytovatele a sídlem Zadavatele.	Poskytovatel	D+20
E1.2	Implementace, migrace, upgrade infrastruktury	Zadavatel	Z+70
E1.3	Školení uživatelů a administrátorů	Poskytovatel	D+90
E1.4	Zkušební provoz	Poskytovatel	D+104
E1.5	Akceptační testy	Zadavatel	D+120
Etapa 2 – Produkční provoz			
E2.1	Produkční provoz	Produkční provoz následuje po zkušebním provozu a splnění akceptačních testů po D+120	

1.3.2. Poskytovatel může dle svého uvážení výše uvedené maximální lhůty trvání v rámci Etapy 1 zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.

1.3.3. Maximální lhůty trvání nesmí Poskytovatel ani Zadavatel prodloužit.

1.3.4. V případě, že dojde k nedodržení termínů harmonogramu u položek, které na sebe navazují a jejich garantem jsou různé subjekty (Poskytovatel/Zadavatel), jedná se o překážku na straně

toho subjektu, který nedodržel termín (Poskytovatel/Zadavatel) a druhému subjektu se prodlužuje termín plnění o stejný počet dní, o který dokončila druhá strana svoji etapu později.

2. KONVENCE DOKUMENTU

2.1. Obecné

2.1.1. Všechny body požadavků jsou uvedeny pokud možno bez použití kondicionálů proto, aby každý požadavek šlo vyhodnotit jako splněný či nesplněný jednoduchou odpovědí ano / ne podle jeho aktuálního reálného stavu v době akceptace. Použití minulého času v tomto dokumentu neznamená automatické potvrzení Zadavatele o splnění tohoto bodu. Splnění či nesplnění požadavku je vždy předmětem akceptačního řízení.

2.1.2. Pokud z kontextu nevyplývá jinak, slova a slovní spojení v jednotném čísle zahrnují i množné číslo a naopak.

3. PROJEKT

3.1. Název projektu

Zajištění cloudové infrastruktury Města Horní Slavkov.

3.2. Základní popis a záměr

Cílem modernizace je přenesení stávajících on-premise systémů do cloudu (za podmínek eGC), při současném přechodu na aktuální verze systémů. Poskytovatel v rámci tohoto projektu při plnění veřejné zakázky zajistí virtuální infrastrukturu, licence pro MS Windows servery a MS SQL server, na kterých budou provozovány aplikace Zadavatele (eObec, SW Stavební úřad, SW MISYS, Helios Fenix, SW Windomy, el. úřední deska, terminálový server, souborový server atd.) a konfiguraci propojení mezi sítí Zadavatele a datacentrem (dále DC) Poskytovatele. Poskytovatel dále zajistí zálohování systémů a dat Zadavatele a školení pro administrátory.

Je požadováno řešení, které bude umožňovat bezproblémový provoz (kompatibilitu) současně používané (serverové) platformy Microsoft. Zadavatel nepředpokládá přechod na jinou platformu, tento přechod by způsobil uživatelské a provozní potíže.

3.3. Předmět veřejné zakázky

Předmětem veřejné zakázky je zajištění virtuální infrastruktury a licencí Microsoft pro provoz aplikací Zadavatele. Zajištění zálohování a případné obnovy provozovaných virtuálních serverů. Součástí plnění je i příprava virtuální infrastruktury a potřebná součinnost při

migraci ze stávajícího on-premise prostředí a dále konfigurace bezpečného propojení DC Poskytovatele se sídlem Zadavatele.

3.4. Cíle veřejné zakázky

Provoz virtuálních serverů na zabezpečené infrastruktuře Poskytovatele včetně zálohování a případné obnovy pro potřeby Zadavatele bez omezení činnosti úřadu a uživatelů. Kapacitu virtuální infrastruktury bude možné škálovat dle potřeb Zadavatele, tzn. virtuální infrastruktura bude umožňovat zakoupení vyšší, ale i nižší kapacity. Tím může Zadavatel optimalizovat náklady spojené s provozem infrastruktury.

3.5. Součástí veřejné zakázky není

a. Infrastruktura ani licence pro MS Exchange, která je součástí aktuálního on-premise prostředí.

b. Migrace on-premise řešení do cloud prostředí ani konfigurace hybrid Azure AD cloudu.

4. ODPOVĚDNOSTI

4.1. Činnosti zajišťované Poskytovatelem

4.1.1. Poskytovatel zajistí zejména:

a. Projektového vedení realizace předmětu plnění (Poskytovatel obdrží kontakt na osobu, která bude zajišťovat projektové vedení na straně Zadavatele, a která bude zajišťovat součinnost se správci stávajícího on-premise řešení – servery, sítě apod.);

b. přípravu nabízeného řešení cloudu a součinnost při migraci on-premise řešení do virtuální infrastruktury;

c. součinnost při přípravě stávajících firewallů a zabezpečené napojení na cloud infrastrukturu;

d. součinnost při migraci aplikačního prostředí do prostředí cloudu;

e. součinnost při optimalizaci aplikačního prostředí v prostředí cloudu;

f. součinnost při migraci stávajících SW systémů v prostředí cloudu na aktuální verze Win OS, SQL a RDS podporované výrobcem;

g. nastavení zálohování a jeho kontrola;

h. nastavení rolí a oprávnění v prostředí online zákaznického portálu;

i. licence a podporu třetích stran;

j. provedení školení;

k. zkušební provoz v rozsahu 14 dnů; na žádost Zadavatele může být v odůvodněných případech (Zadavatel má objektivní technický důvod pro prodloužení zkušebního provozu) zkušební provoz prodloužen až na 60 dnů, potom se prodlužuje lhůta harmonogramu od bodu 1.4. dále o počet dní stanovených nad rámec 14denního zkušebního provozu;

l. zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu.

m. provoz cloud infrastruktury

4.2. Činnosti zajišťované Zadavatelem

4.2.1. Zadavatel zajistí:

a. projektové vedení na straně Zadavatele

b. koordinaci správce stávající on-premise infrastruktury s Poskytovatelem při migraci on-premise prostředí do cloudu

c. potřebnou součinnost dodavatelů aplikací Zadavatele při migraci do cloudu

d. součinnost správce stávajících infrastrukturních služeb, zejména konfiguraci firewallů Zadavatele pro připojení do infrastruktury Poskytovatele

e. přípravu, migraci infrastruktury a služby spojené s povýšením serverů na aktuální verze na straně Zadavatele

4.3. Organizační požadavky

4.3.1. Poskytovatel zajistí projektové vedení po celou dobu realizace zakázky osobou odpovědnou za realizaci předmětu plnění, která bude hlavní kontaktní osobou a která bude přítomna při všech jednáních týkajících se projektu.

4.3.2. Veškeré dodávané technologie budou implementovány za plného provozu.

4.3.3. Poskytovatel nesmí svou činností narušit provoz úřadu Zadavatele. Případné dílčí či částečné omezení provozu musí být předem projednáno a schváleno Odběratelem, musí být omezeno na minimum a nesmí negativně ovlivnit poskytování základních služeb úřadu.

5. POPIS VÝCHOZÍHO STAVU – STÁVAJÍCÍ INFRASTRUKTURA

5.1. LAN infrastruktura

5.1.1. LAN infrastruktura je tvořena stohy přepínačů HPE, 2x HP 5120-48G EI Switch a 2x HP 192024GPoE+. Do internetu je město připojeno přes dvojicí firewallů FortiGate 60F, HW + 24x7 Unified Threat Protection režimu active/active.

5.2. Virtualizační platforma

5.2.1. Virtualizační platforma je tvořena dvěma servery HP DL360 Gen9 8SFF virtualizovanými technologií Hyper-V, které tvoří cluster.

5.2.2. Vlastní instalace je realizována v jednom racku.

5.2.3. Napájení je zálohováno dvojící UPS HP R/T3000.

5.2.4. Prostředí je zálohováno pomocí produktu Veeam Backup & Recovery s ukládáním záloh na síťové úložiště NAS Synology.

5.3. Operační systémy, databáze, groupware

5.3.1. Hlavním serverovým operačním systém je Windows Server 2012 R2. Jednotnou adresářovou službou je Active Directory.

5.3.2. Jako Groupware je využíván Microsoft Exchange 2013.

5.3.3. Hlavním databázovým systémem je Microsoft SQL Server Standard 2012. Tento systém je sdílen aplikacemi a systémy úřadu a jejich výkon a dostupnost jsou tak kritické pro zajištění bezproblémového běhu uživatelského prostředí.

5.3.4. Databázový Microsoft SQL server je využíván aplikacemi:

a. eObec (spisová služba), výrobce Asseco Solutions
b. SW Stavební úřad, výrobce VITA Software
c. SW MISYS, výrobce Gepro
d. účetní systém Helios Fenix, výrobce Asseco Solutions
e. SW Windomy, výrobce OK Soft
f. el. úřední deska

5.4. Prostředí koncových uživatelů

5.4.1. Prostředí aplikací je virtualizováno pomocí Microsoft Windows RDS 2012 R2

5.4.2. Jako koncové stanice jsou převážně využívány HW terminály HP t530 W10P 32GF/4GR

5.4.3. Jako klientský Microsoft SW je využíván Microsoft Office Standard 2016 (nákup v rámci licenčního programu Microsoft Select Plus)

5.4.4. Prostředí používá 25 uživatelů

5.5. Software

Serverová virtualizace	Hyper – V	1 instance
Virtualizace aplikací / desktopů	MS RDS server 2012 R2	1 instance
OS Windows server	MS Windows server 2012R2	4 instance
Zálohovací SW	Veeam Backup Essentials Enterprise 2 socket bundle for Hyper-V	1 instance
Databázový SW	MS SQL	1 instance
Poštovní systém	MS Exchange 2013	1 instance
Aplikační SW SIEM	SolarWinds Log & Event Manager	1 instance

6. POŽADOVANÉ PARAMETRY DODANÉHO ŘEŠENÍ A SLUŽEB

6.1. Obecné

6.1.1. Dodávky musí splňovat bezpečností úroveň **vysoká** dle vyhlášky č. 315/2021 Sb.

6.1.2. Pokud Poskytovatelem nabízené řešení vyžaduje komponenty či služby neobsažené v požadavcích zadání, zahrne Poskytovatel do své ceny všechny náklady na jejich pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu.

6.1.3. Veškeré produkty, které Poskytovatel dodává v rámci plnění Zadavateli, musí splňovat následující podmínky:

a. byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
b. obsahují všechny nezbytné licence na používání příslušného softwaru,
c. jsou určeny pro provoz v České republice.

6.1.4. Pokud Poskytovatel vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k realizaci zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.

6.2. Infrastruktura

6.2.1. Datové centrum s umístěním virtuální infrastruktury musí splňovat parametry minimálně kategorie Tier III.

6.2.2. Virtuální infrastruktura musí zajišťovat alokovanou kapacitu. Alokovaná kapacita je definována jako poskytnutý výpočetní výkon vCPU (počtem jader procesoru s minimální frekvencí 1000Mhz), alokovanou velikostí pamětí RAM (vyjádřeno v GB) a alokovaným diskovým prostorem v GB.

6.2.3. DC Poskytovatele musí poskytnout vyhrazené připojení do NIX (nebo obdobného peeringového centra) pro Zadavatele s kapacitou minimálně 50 Mbps (symetricky). DC Poskytovatele musí být s NIX (nebo obdobném peeringovém centru) propojen linkou s kapacitou min 10 Gbps.

6.2.4. Mezi cloud a on-premise prostředím Zadavatele bude navázaný virtuální kanál (IPSec). Veškerá komunikace do/z cloudu bude procházet přes stávající on-premise dvojici firewallů, které budou zajišťovat ochranu provozu (UTM, Antivir, SSL inspekce, VPN apod).

6.2.5. Data do prostředí Poskytovatele budou migrována formou replikace záloh celých virtuálních serverů Zadavatele. Po dokončení budou celé virtuální servery spuštěny v prostředí Poskytovatele a přepojen provoz tak aby nedošlo ke ztrátě a nekonzistenci dat a za

minimálního výpadku a omezení činnosti úřadu a jeho uživatelů. Po dokončení přechodu bude infrastruktura optimalizována Poskytovatelem dle požadavků Zadavatele na potřebnou kapacitu a výkon a dle potřeb migrovaných systémů.

6.2.6. Fyzická bezpečnost DC

a. non-stop 24x7 přístup jen s doprovodem odpovědného pracovníka helpdesku po ověření totožnosti
b. zabezpečovací systém
c. uzamykatelné racky
d. požární čidla
e. automatický zhášecí systém.

6.2.7. Cloud infrastruktura umožňuje případné budoucí bezproblémové rozšíření služeb o ochranu firewallem, kontrolu integrity, šifrování virtuálních serverů a dat, včetně u záloh.

6.2.8. Plná redundance všech zdrojů je zajištěna pro všechny významné služby

a. Síť WAN musí být do NIXu (nebo obdobného peeringového centra) dvěma nezávislými nesouběžnými linkami o kapacitě minimálně 10 Gbps. Zahraniční konektivita DC musí být zajištěna minimálně dvěma nezávislými poskytovateli transitní IP konektivity o souhrnné kapacitě minimálně 40 Gbps.
b. Síťová infrastruktura LAN je provozována na plně redundantních routerech a switchích.
c. Fyzické servery jsou provozovány nad plně redundantním serverovým systémem.
d. Jako disková úložiště jsou používána plně redundantní disková pole.
e. Virtualizační platforma plnou redundanci prostředí pro běh virtuálních serverů.
f. Poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí. Poskytovatel umožní vzdálené zpřístupnění všech událostí Zadavateli. Nové události zpřístupní Zadavateli okamžitě po vzniku události, nejpozději však do 24 hodin.
g. Poskytovatel chrání obsah Infrastruktury Zadavatele šifrováním při přenosu a v úložištích pomocí některého z algoritmů uvedených v doporučení v oblasti kryptografických prostředků vydaného NÚKIB, které je zveřejněno na jeho internetových stránkách, případně umožní Zadavateli využití vlastního šifrovacího klíče (BYOK). Poskytovatel musí kdykoliv na vyžádání Zadavatele umožnit import či export dat Zadavatele prostřednictvím zaslání šifrovaných paměťových médií, a to i v objemu větším než 2 TB.
h. Poskytovatel vyhotovuje záznam o přístupu jeho interních a externích pracovníků k nezašifrovaným datům Zadavatele, ke kterému došlo bez přechozího svolení Zadavatele v daném případě. Tento záznam musí obsahovat alespoň důvod, čas, trvání, typ a rozsah přístupu a dostatek dalších údajů potřebných k tomu, aby mohl Zadavatel vyhodnotit rizikovost tohoto přístupu. Poskytovatel o záznamu Zadavatele informuje ihned po

přístupu k datům Zadavatele a umožní Zadavateli přístup k záznamu alespoň po dobu 1 roku zpětně.

i. Bezpečnostní požadavky na Platformu
j. Poskytovatel musí být zapsán v katalogu služeb cloud computingu v kategorii vysoká bezpečnostní úroveň. https://www.mvcr.cz/clanek/katalog-cloud-computingu.aspx
k. Poskytovatel musí doložit, že datové centrum vyhovuje vyhlášce č. 316/2021. To je možné doložit např. certifikací ISO 27001; a ověřeným souladem s nařízením GDPR (dokumentace, procesy, technologie)
l. Infrastruktura je pravidelně auditována třetí stranou (buď nezávislou organizací nebo výrobcem).

6.3. Servery a úložiště dat

6.3.1. Virtuální Server s operačním systémem

vServer je služba provozovaná nad výpočetním systémem, na kterém je provozována serverová virtualizační vrstva umožňující abstrakci, flexibilitu a partitioning výpočetního výkonu. Virtuální server má přesně dané výkonnostní parametry a SLA popisující garantovanou dostupnost služby. vServery, jsou definovány počtem virtuálních procesorů (vCPU) a velikostí dostupné paměti RAM. Parametr vCPU je virtuální procesor provozovaný na jednom jádře fyzického procesoru a garantovaném frekvenci min. 1GHz.

V rámci dodávky Poskytovatel připraví 4 virtuální servery:

a. vServer 2_4
b. vServer 2_8
c. vServer 4_16
d. vServer 12_32

6.3.2. Disky k virtuálním serverům

Veškeré virtuální disky v nabídce musí splňovat minimálně tyto hodnoty pro parametr throughput:

velikost HDD disku od (včetně)	velikost disku do	min. throughput pro HDD
40 GB	250 GB	60 MiB/s
250 GB		150 MiB/s

velikost SSD disku od (včetně)	velikost disku do	min. throughput pro SSD
40 GB	200 GB	150 MiB/s
200 GB	300 GB	300 MiB/s
300 GB	500 GB	450 MiB/s
500 GB	750 GB	750 MiB/s
750 GB		1 125 MiB/s

vHDD a vSSD jsou služby provozované nad virtualizovaným storage. Data jsou chráněna pomocí technologie RAID a rozdělena do logických jednotek zpřístupněných virtualizačním hypervisorům zajišťujícím virtualizaci diskového systému do jednotlivých produktů vHDD a vSSD. Jednotlivé typy produktů vHDD a vSSD se liší v parametrech kapacity a výkonu.

Disková kapacita je udávána v GB a výkon v IOPS (počet diskových transakcí za vteřinu) a throughput (In + Out), měřeno na úrovni požadavků virtualizovaného OS MS Windows server.

V rámci dodávky Poskytovatel připraví 4 virtuální disky a připraví je k použití s vServery z bodu 6.3.1:

a. vHDD 40_800_RPO24h/RET30
b. vHDD 200_800_RPO24h/RET30
c. vSSD 500_2500_RPO24h/RET30
d. vSSD 600_6000_RPO24h/RET30

Požadavky na výkon v bodech 6.3.1. a 6.3.2. jsou uvedeny jako požadované jednotky sloužící pro konfiguraci (nákup) konkrétního virtuálního serveru. Příklad: virtuální server bude sestaven ze dvou 6.3.1.c., jedné 6.3.2.c. a dvou 6.3.2.b.
Virtuální stroj tedy bude disponovat osmi vCPU s 32 GB RAM, jedním 500 GB virtuálním diskem SSD a jedním virtuálním diskem 400 GB virtuálním diskem HDD.

6.4. Networking

6.4.1. Mezi cloudem a on-premise prostředím Zadavatele bude navázaný virtuální kanál (IPSec). Veškerá komunikace do/z cloudu bude procházet přes stávající on-premise dvojici firewallů, které budou zajišťovat ochranu provozu (UTM, Antivir, SSL inspekce, VPN apod).

6.4.2. 1 x VLAN

6.4.3. 1 x veřejná IP adresa v4

6.5. Licence

6.5.1. Licence zajistí Poskytovatel v rámci Microsoft Services Provider License Agreement (SPLA). Poskytovatel licence poskytne na základě platné smlouvy se společnosti Microsoft SPLA s dodatkem License Mobility a Shared Computer Activation (SCA).

6.5.2. Serverové licence - 4 ks Microsoft Windows Server

6.5.3. Klientské RDS licence - 25 ks Microsoft Remote Desktop SAL

6.5.4. Databázové licence 2 ks Microsoft SQL Standard 2 core

6.5.5. Licence jsou brány jako jednotky, které je možné přidělovat a odebírat vServerům individuálně (při zakoupení dalšího vServeru je možné vybrat příslušnou licenci, při smazání operačního systému z vServeru je možné licenci odebrat).

6.6. On-line zákaznický portál

6.6.1. Bezpečnost přístupu – veškeré nástroje pro správu musí umožňovat vícefaktorové ověřování uživatele.

6.6.2. Veškeré nástroje pro správu musí komunikovat se zařízeními šifrovanými protokoly (SSH apod.). Také v případě vestavěných nástrojů (např. www rozhraní hardware) musí být použita šifrovaná komunikace (např. HTTPS).

6.6.3. Definice uživatelských rolí

a. Administrátor,

b. Server Operátor,

c. Network Operátor.

d. Monitoring (pouze čtení)

6.6.4. Administrace virtuální infrastruktury

a. Vytváření serverů, změny parametrů serverů, mazání serverů

b. Vytváření virtuálních disků, změny parametrů disků, mazání disků

c. Instalace virtuálních serverů z předdefinovaných šablon (pouze výběrem základních parametrů jako je počet CPU, velikost RAM, kapacita a počet IOPS HDD/SSD a výběrem OS bude automatizovaně nainstalován virtuální server daných parametrů včetně funkčního OS)

d. Používání Virtual Media Access (ISO).

e. Podpora instalace operačního systému z tzv. ISO images

f. Přístup na konzoli virtuálního serveru prostředky pro vzdálenou správu.

g. Reporty. Pravidelné reporty (min. jednou za měsíc)

   I. Grafické zobrazení po dnech a souhrnná tabulka využití vCPU s následujícími údaji:
      1. Zakoupená kapacita vCPU – počet vCPU, celková velikost RAM a jejich využití v čase v GB.
      2. Průměrné využití CPU – průměrná hodnota využití CPU za celé období.
      3. Medián využití vCPU – medián využití vCPU za celé období počítán z hodinových intervalů.
      4. Maximum vCPU – maximální hodnota využití vCPU v hodinových intervalech.

   II. Grafické zobrazení po dnech a souhrnná tabulka využití virtuálních disků s následujícími údaji:
      1. Zakoupená propustnost – zakoupená propustnost v IOPS a celková zakoupená kapacita v GB.
      2. Průměrná propustnost – průměrná propustnost v IOPS za celé období.
      3. Medián propustnosti – medián propustnosti v IOPS za celé období je počítán z hodinových intervalů.
      4. Maximum propustnosti – maximum propustnosti v IOPS za jednotlivé zakoupené diskové jednotky.

h. Technické reporty. Pravidelné reporty (min. jednou za měsíc) s doporučením vhodných konfigurací infrastruktury a optimalizaci infrastruktury (minimálně předimenzované kapacity nebo naopak poddimenzované výpočetní zdroje, resp. virtuální servery, virtuální disky, síťová připojení, doporučení správného licenčního modelu pro SW z bodu 6.6.).

i. Výkonnostní statistiky v reálném čase. Pro každý vServer:

   I. využití vCPU s následujícími údaji:
      1. Zakoupená kapacita CPU – počet vCPU, celková velikost RAM.
      2. aktuální využití CPU –

   II. využití virtuálních disků s následujícími údaji:
      1. Zakoupená propustnost – zakoupená kapacita jednotlivých disků, s uvedením zakoupených parametrů IOPS a throughput
      2. Aktuální IOPS a throughput s rozdělením In, Out, celkem.

6.6.5. Administrace sítě

a. Interní sítě

b. Interní IP adresy

c. Veřejné IPv4 adresy

d. Virtuální router

e. Virtuální firewall

f. Pravidla NAT

g. VPN Management

6.6.6. Správa SW licencí

6.6.7. Integrovaná funkce fakturace po jednotlivých položkách s funkcí výpočtu služby pro simulaci nákladů projektu.

6.7. SLA Reporty

Jednotky SLA:

Jednotka SLA	Minimální požadovaná hodnota pro splnění 100 % SLA
vCPU – počet jader	dle parametru v Příloze a zakoupené varianty
vRAM – alokovatelná RAM	dle parametru v Příloze a zakoupené varianty
vHDD/vSSD – kapacita	dle parametru v Příloze a zakoupené varianty
vHDD/vSSD – IOPS	dle parametru v Příloze a zakoupené varianty
vHDD/vSSD – throughput	dle parametru v Příloze a zakoupené varianty
konektivita – dosažitelná datová propustnost do NIX	> = 50 Mbps
konektivita – latence od NIX	<30 ms
dostupnost admin portálu	24/7
dostupnost portálu podpory	24/7

6.7.1. Poskytovatel měří dostupnost jednotlivých Jednotek SLA Infrastruktury pro každou Jednotku SLA individuálně pro dané vyhodnocovací období.

6.7.2. Začátkem výpadku je moment, který odpovídá časové značce hlášení v monitorovacím nástroji Poskytovatele, který ohlašuje nedostupnost dané Jednotky SLA. Pokud však Zadavatel prokáže, že Jednotka SLA měla výpadek, tak je irelevantní, když se v logu Poskytovatele nenachází záznam o výpadku a za začátek výpadku je považován čas prokázaný Zadavatelem.

6.7.3. Koncem výpadku je moment, který odpovídá časové značce prvního pravdivého hlášení v monitorovacím nástroji, které ohlašuje dostupnost dané Jednotky SLA. Pokud však Poskytovatel prokáže, že Jednotka SLA byla obnovena, tak je irelevantní, když se v logu Poskytovatele nenachází záznam o obnově a za konec výpadku je považován čas prokázaný Poskytovatelem.

6.7.4. Provozní doba pod SLA se vypočte počtem dní v kalendářním měsíci, za který se vyhotovuje vyhodnocení dostupnosti Infrastruktury vynásobených 24 hodinami převedenými na minuty.

Provozní doba pod SLA = počet dní v kalendářním měsíci × 24 × 60

6.7.5. Doba výpadku je doba mezi začátkem výpadku dle odst. 6.7.2 Technické specifikace a koncem výpadku dle odst. 6.7.3 Technické specifikace uvedená v celých minutách, zaokrouhlených směrem nahoru.

6.7.6. Kumulativní dobou výpadku je součet všech dob výpadku za vyhodnocovaný měsíc.

6.7.7. Vyhodnocení dostupnosti Jednotky SLA se vypočte následujícím způsobem:

a. od provozní doby pod SLA za daný měsíc se odečte kumulativní doba výpadku za daný měsíc,
b. výsledek předešlého kroku je vydělen provozní dobou pod SLA za daný měsíc a
c. výsledek předešlého kroku je vynásoben číslem 100.

Výsledkem je Vyhodnocení dostupnosti Jednotky SLA za daný měsíc v procentuální podobě.

Vyhodnocení dostupnosti Jednotky SLA (v %)
=
(provozní doba pod SLA − kumulativní doba výpadku) / (provozní doba pod SLA) × 100

6.7.8. Úrovně podpory Infrastruktury a řešení Požadavků Zadavatele

6.7.8.1. Požadavky jsou rozděleny do následujících úrovní dle závažnosti:

a) **kritická úroveň:** Požadavek souvisí s tím, že Infrastruktura není dostupná nebo vykazuje takové vlastnosti, které ji činí zcela nepoužitelnou. Požadavek vyžaduje okamžitou pozornost Poskytovatele.

b) **střední úroveň:** Infrastruktura je dostupná, avšak se značně zhoršenou odezvou, nebo některé moduly nepracují ve shodě se specifikací / dokumentací. Hlavní funkce organizace Zadavatele, služby mohou na snížené úrovni pokračovat.

c) **nízká úroveň:** Požadavky Zadavatele na změnová řízení služby nebo eskalace, které bezprostředně nemají dopady na chod organizace (např. požadavky na změnu uživatelského rozhraní aplikace).

6.7.9. Reakční doba Poskytovatele na Požadavky Zadavatele činí od okamžiku odeslání Požadavku Poskytovateli:

Požadavek nízké úrovně	Požadavek střední úrovně	Požadavek kritické úrovně
Max. 8 hodin, pouze v pracovní dny	**Max. 4 hodiny, v nepřetržité době 24x7**	**Okamžitě, v nepřetržité době 24x7**

6.7.10. Reakcí na Požadavek se rozumí alespoň informování Zadavatele (a) o zahájení řešení Požadavku, (b) o tom, kdo bude řešitelem Požadavku (přiřazení řešitele) a (c) o tom, jaký způsob Poskytovatel zvolil pro zahájení řešení Požadavku. Reakci musí provést operátor, ne automat.

6.7.11. Doba pro vyřešení Požadavku činí od okamžiku odeslání Požadavku Poskytovateli:

Požadavek nízké úrovně	Požadavek střední úrovně	Požadavek kritické úrovně
Max. 16 hodin, pouze v pracovní dny.	a) **Max. 1 hodina na dodání dočasného řešení nebo náhradního postupu, který vede ke snížení klasifikace Požadavku alespoň o jednu úroveň (například z vysoké na střední) a** b) **max. 12 hodin na trvalé vyřešení Požadavku,** **to vše v nepřetržité době 24 x 7.**	c) **Max. 30 minut na dodání dočasného řešení nebo náhradního postupu, který vede ke snížení klasifikace Požadavku alespoň o jednu úroveň (například z vysoké na střední) a** d) **max. 4 hodiny na trvalé vyřešení Požadavku,** to vše v nepřetržité době 24 x 7.

6.8. Podpora

6.8.1. Pro účely hlášení problémů a zadávání změnových požadavků bude k dispozici ServiceDesk. ServiceDesk bude pracovat v režimu 24x7, kde požadavky bude možné zadávat online nebo případně pomocí e-mailu a/nebo telefonu.

6.9. Zálohování

6.9.1. Služba bude zajišťovat zálohování virtuálních serverů, Záloha serverů bude probíhat jednou denně, čas pro zahájení zálohy bude stanoven Zadavatelem. Obnova dat je pak prováděna vždy na vyžádání ze strany Zadavatele. Vlastní obnovu vServerů zajistí Poskytovatel.

6.9.2. Řešení zálohování umožní připojení zálohy jako virtuálního read only disku k vServeru určeného Zadavatelem, aby bylo možné obnovit ze zálohy i jednotlivé soubory. Připojení zálohy provede Poskytovatel, vlastní obnovu ze zálohy, vyhledání souboru k obnově atd. si zajistí Zadavatel.

6.9.3. Zálohy budou denní celých virtuálních serverů (Recovery Point Objective 24 hodin) s definovanou retencí záloh (minimálně 30 dní). Garantovaná obnova dat (Recovery Time Objective) bude maximálně do 8 hodin. Dále jen RPO24h/RET30.

6.10. Kompatibilita a interoperabilita

6.10.1. Webová rozhraní nabízených systémů a zařízení musí být funkční v obvyklých internetových prohlížečích – min. Edge, Chrome, Safari v aktuálních verzích bez potřeby instalace speciálních doplňků či plug-in modulů.

6.11. Dokumentace

6.11.1. Veškerá dokumentace vytvořená v rámci realizace zakázky, musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě na datovém nosiči ve standardních editovatelných formátech MS Office nebo formátu PDF. Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena Zadavatelem.

6.11.2. Poskytovatel zpracuje provozní dokumentaci, která bude popisovat konfiguraci zhotoveného díla.

6.11.3. Součástí provozní dokumentace bude popis úkonů doporučené údržby a specifikace intervalů jejich provádění.

6.11.4. Poskytovatel uvede do dokumentace kompletní podmínky pro zajištění provozu dodaných prvků a své virtuální infrastruktury, včetně požadavků na aktualizace software (maintenance) a proces Poskytovatele, kterým bude tyto aktualizace provádět a kontrolovat. Toto se netýká routerů Zadavatele, které budou sloužit pro propojení s DC Poskytovatele; jejich správa a údržba je zodpovědností Zadavatele.

6.11.5. Správnost a úplnost veškeré dokumentace je Poskytovatelem kontrolována a aktualizována minimálně 1x ročně a dále nejdříve dva měsíce a nejpozději týden před skončením platnosti Smlouvy.

6.11.6. Poskytovatel o kontrole a aktualizaci dokumentace vytvořil protokol, který obsahuje minimálně:

a. Datum aktualizace dokumentace.

b. Seznam kontrolovaných dokumentů a jejich umístění.

c. Pro každý dokument souhrn, v čem aktualizace spočívala.

6.12. Školení

6.12.1. Poskytovatel zajistí školení pracovníků Zadavatele – administrátorů– na zařízení a systémy dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu předávané provozní dokumentace.

6.12.2. Školení zajistí seznámení pracovníků Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin a pracovníkům bude vystaveno osvědčení o školení s uvedením rozsahu školení. Budou provedena tato školení:

a) Školení administrátorů a správců cloud platforem – minimální rozsah školení je 8 hodin; předpokládá se účast max. 3 účastníků, školení bude probíhat v sídle Zadavatele

6.13. Právní a další předpisy

6.13.1. Poskytovatel při vytváření systému a poskytování služeb dodržuje právní předpisy a interní předpisy Zadavatele. Zadavatel upozorňuje zejména na:

a. Nařízení (EU) 2016/679 (GDPR). Poskytovatel vzal na vědomí a respektuje, že Zadavatel pracuje se zvláštní kategorií osobních údajů.

b. Směrnice (EU) 2002/58/ES (Nařízení o soukromí a elektronických komunikacích) a Nařízení, které ji nahrazuje (ePrivacy).

c. Zák. č. 480/2004, zákon o některých službách informační společnosti a o změně některých zákonů, zejména §7.

d. Zákon 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

e. Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

f. Minimální smluvní podmínky smlouvy na dodávku služby cloud computingu vydané MV ČR Projekt eGovernment cloud (eGC) verze 2.1 z 1/6/2022

6.14. Organizace bezpečnosti informací

6.14.1. Poskytovatel prohlašuje, že má zaveden systém řízení bezpečnosti informací minimálně s těmito parametry:

a) Rozsah systému řízení bezpečnosti informací zahrnuje organizační jednotky Poskytovatele, lokality a procesy využívané k poskytování služby cloud computingu.

b) Poskytovatel dokumentuje zavedená opatření pro nastavení, implementaci, údržbu a neustálé zlepšování systému řízení bezpečnosti informací.

c) Dokumentace obsahuje rozsah systému řízení bezpečnosti informací a prohlášení o aplikovatelnosti, ve kterém je uvedeno, jaká bezpečnostní opatření byla vybrána pro potlačení rizik, a výsledky posledního auditu systému řízení bezpečnosti informací Poskytovatele.

6.14.2. Infrastruktura se řídí politikou bezpečnosti informací Poskytovatele, sdílenou a sdělovanou všem zaměstnancům, externím pracovníkům a subdodavatelům Poskytovatele, dokumentovanou, verzovanou, kontrolovanou a schválenou vrcholovým vedením Poskytovatele. Politika bezpečnosti informací popisuje význam bezpečnosti informací, bezpečnostní cíle, úroveň zabezpečení Infrastruktury, nejvýznamnější aspekty bezpečnostní strategie k dosažení stanovených cílů a organizační strukturu Poskytovatele v rozsahu systému řízení bezpečnosti informací.

6.14.3. Poskytovatel prohlašuje, že na základě politiky bezpečnosti informací zavádí přiměřená bezpečnostní opatření, která jsou v souladu s požadavky Zadavatele.

6.14.4. Poskytovatel se zavazuje jednoznačně identifikovat, dokumentovat a udržovat aktuální veškeré relevantní povinnosti vyplývající z právních předpisů a Smlouvy, kladené na Poskytovatele a týkající se bezpečnosti informací služby cloud computingu. Poskytovatel dokumentuje způsob, jakým tyto povinnosti dodržuje.

6.14.5. Ve vztahu ke službě cloud computingu je Poskytovatelem jednou ročně nebo na základě opakujících se kybernetických bezpečnostních incidentů nebo v případě rozporu vůči deklarovaným parametrům umožněno NÚKIB zdarma provedení kontroly splnění požadavků podle zákona č. 255/2012 Sb., kontrolní řád, ve znění pozdějších předpisů, na všech místech a zařízeních souvisejících s poskytováním služby cloud computingu. Poskytovatel zároveň poskytne NÚKIB veškerou potřebnou součinnost, vyjma zpřístupnění či předání zákaznických dat bez souhlasu Zadavatele.

6.15. Fyzická bezpečnost budov a prostor

6.15.1. V datových centrech, ve kterých dochází k poskytování služby cloud computingu, Poskytovatel navrhl a aplikuje fyzickou ochranu proti přírodním katastrofám, úmyslnému útoku nebo haváriím.

6.15.2. Služba cloud computingu je Poskytovatelem poskytována alespoň ze dvou datových center, která jsou od sebe oddělena dostatečnou vzdáleností k zajištění vzájemné provozní zastupitelnosti a odolnosti v poskytování služby cloud computingu.

6.15.3. Primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby cloud computingu poskytované z primárního datového centra, jsou v dostatečné vzdálenosti od přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka vedoucích k narušení nebo omezení poskytování služby cloud computingu nebo bezpečnosti informací nebo Poskytovatel přijal adekvátní bezpečnostní opatření, nebo se primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby cloud computingu poskytované z primárního datového centra, nacházejí ve vzájemné vzdálenosti nejméně 50 km.

6.15.4. U budov a prostor vztahujících se k poskytování služby cloud computingu, včetně vstupu to těchto budov a prostor, Poskytovatel prokazatelně zavedl bezpečnostní opatření vhodná k včasné detekci a zabránění neoprávněnému či neautorizovanému přístupu k technickým aktivům, nebo k zákaznickým datům a provozním údajům, nebo poškození a neoprávněným zásahům do technických aktiv, zákaznických dat nebo provozních údajů.

6.16. Zajištění provozu Infrastruktury

6.16.1. Zákaznická data Poskytovatel bezpečně a striktně odděluje od jiných dat, která jsou uložená a zpracovávaná na sdílených virtuálních a fyzických zdrojích využívaných k poskytování služby cloud computingu tak, aby byla zajištěna důvěrnost a integrita zákaznických dat.

6.16.2. Zákaznická data a data nezbytná pro poskytování služby cloud computingu Poskytovatel zálohuje do lokality v dostatečné vzdálenosti. Při přenosu do této lokality i při uložení v této lokalitě Poskytovatel zákaznická data a data nezbytná pro poskytování služby cloud computingu šifruje v souladu s uznávanými nejmodernějšími požadavky v oblasti kryptografických prostředků nebo alespoň v souladu s doporučením NÚKIB v oblasti kryptografických prostředků zveřejněným na internetových stránkách NÚKIB.

6.16.3. Provozní údaje se vztahem ke službě cloud computingu Poskytovatel shromažďuje zejména o událostech:

a. přihlašování a odhlašování u všech účtů, a to včetně neúspěšných pokusů,

b. činnosti provedené administrátory na straně Poskytovatele zejména pokud zaměstnanci nebo externí pracovníci Poskytovatele čtou nebo zapisují nešifrovaná zákaznická data nebo specifické provozní údaje zpracovávané ve službě cloud computingu nebo k nim přistupují bez předchozího souhlasu Zadavatele,

c. úspěšné i neúspěšné manipulace s účty, oprávněními a přístupovými právy,

d. neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,

e. činnosti uživatelů a administrátorů na straně Zadavatele, které mohou mít vliv na bezpečnost informací ve službě cloud computingu,

f. zahájení a ukončení činností technických aktiv,

g. kritická i chybová hlášení technických aktiv a

h. pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí.

6.16.4. Provozní údaje zaznamenané podle výše uvedeného pravidla obsahují zejména:

a. datum a čas, včetně specifikace časového pásma,

b. typ činnosti,

c. identifikaci technického aktiva, které činnost zaznamenalo,

d. jednoznačnou identifikaci účtu, pod kterým byla činnost provedena,

e. jednoznačnou síťovou identifikaci zařízení původce a

f. úspěšnost nebo neúspěšnost činnosti.

6.16.5. Poskytovatel zajistí nástroj pro monitorování a zaznamenávání, sledování a vyhodnocování kybernetických bezpečnostních událostí a přístup Zadavatele k informacím o stavu zabezpečení, zejména k informacím vyplývajícím ze shromážděných provozních údajů. Nové události zpřístupní Poskytovatel Zadavateli okamžitě po vzniku události, nejpozději však do 24 hodin. Shromážděné nebo vygenerované provozní údaje bude Poskytovatel uchovávat alespoň po dobu 12 měsíců od jejich vytvoření ve vhodné, neměnné a sdružené formě bez ohledu na jejich zdroj tak, aby bylo možné centrální autorizované vyhodnocení dat.

6.16.6. Na žádost Zadavatele poskytne Poskytovatel Zadavateli bezodkladně vyžádané provozní údaje o činnostech uživatelů, a to v elektronickém, strukturovaném, běžně používaném, strojově čitelném a interoperabilním formátu tak, aby mohl Zadavatel provést analýzu jakéhokoliv kybernetického bezpečnostního incidentu.

6.16.7. Mezi technickým aktivem shromažďujícím provozní údaje a technickým aktivem, na němž jsou provozní údaje vytvářeny, Poskytovatel provádí ověřování identity. Poskytovatel zajistí, aby přenos mezi technickým aktivem shromažďujícím provozní údaje a technickými aktivy, na nichž jsou provozní údaje vytvářeny, probíhal zabezpečeným aktuálně odolným šifrováním nebo po sítích pod kontrolou Poskytovatele.

6.17. Řízení přístupu Poskytovatele

6.17.1. Poskytovatel v rámci své organizace řídí přístupy k informačnímu systému využívanému k poskytování služby cloud computingu Zadavateli.

6.17.2. Přístupová práva Poskytovatel přiděluje konkrétním administrátorům na straně Poskytovatele podle principu nutnosti vědět (need-to-know principle) a časově je omezuje na základě hodnocení rizik Poskytovatele.

6.17.3. Poskytovatel vyhotovuje záznam o přístupu jeho interních a externích pracovníků k nezašifrovaným datům Zadavatele, ke kterému došlo bez přechozího svolení Zadavatele v daném případě. Tento záznam musí obsahovat alespoň důvod, čas, trvání, typ a rozsah přístupu a dostatek dalších údajů potřebných k tomu, aby mohl Zadavateli vyhodnotit rizikovost tohoto přístupu. Poskytovatel o záznamu Zadavatele informuje ihned po přístupu k datům Zadavatele a umožní Zadavateli přístup k záznamu alespoň po dobu 1 roku zpětně.

6.18. Šifrování zákaznického obsahu a zabezpečení komunikace

6.18.1. Poskytovatel zavedl procesy a technická opatření s aktuálně odolným šifrováním a ověřením identity pro zabezpečení přenosu zákaznického obsahu po sítích mimo kontrolu Poskytovatele.

6.18.2. Poskytovatel zavedl procesy a technická opatření pro aktuálně odolné šifrování zákaznického obsahu během jeho uchovávání.ne

6.18.3. Zákaznický obsah Poskytovatel při přenosu a v úložištích ve službě cloud computingu šifruje v souladu s uznávanými nejmodernějšími požadavky v oblasti kryptografických prostředků nebo alespoň pomocí některého z algoritmů uvedeného v doporučení NÚKIB v oblasti kryptografických prostředků zveřejněném na internetových stránkách NÚKIB, případně Poskytovatel umožní Zadavateli využití vlastního šifrovacího klíče (BYOK). Poskytovatel musí kdykoliv na vyžádání Zadavatele umožnit import či export dat Zadavatele prostřednictvím zaslání šifrovaných paměťových médií, a to i v objemu větším než 2 TB.

6.18.4. Zákaznická data přenášená do služby cloud computingu Poskytovatel chrání proti neoprávněnému zásahu, kopírování, úpravě, přesměrování nebo vymazání v souladu s požadavky Zadavatele na zajištění bezpečnosti informací.

6.18.5. Zákaznická data přenášená ze služby cloud computingu Poskytovatel chrání proti neoprávněnému zásahu, kopírování, úpravě, přesměrování nebo vymazání v souladu se zavedenou politikou bezpečnosti informací Poskytovatele.

6.19. Dokumentace bezpečnosti vstupů a výstupů

6.19.1. Poskytovatel zajistil, že služba cloud computingu je přístupná pro jiné služby cloud computingu nebo IT systémy Zadavatele skrze zdokumentované rozhraní příchozích a odchozích zákaznických dat tak, aby z nich Zadavatel mohl v případě potřeby získat zákaznická data, a to pokud se jedná o služby cloud computingu, které zákaznická data ukládají ve stavu neaktivních dat. Poskytovatel na vyžádání Zadavatele zpřístupní příslušnou dokumentaci.

6.20. Nákup, vývoj a úprava informačních systémů

6.20.1. Bude-li zřízeno za účelem plnění Smlouvy testovací prostředí, Provozní prostředí Infrastruktury je Poskytovatelem fyzicky nebo logicky odděleno od testovacího nebo vývojového prostředí, aby se zabránilo neautorizovanému přístupu k zákaznickým datům, šíření škodlivého kódu nebo změnám technických aktiv. Z důvodu ochrany důvěrnosti dat data obsažená v provozním prostředí Poskytovatel nepoužívá v testovacím ani v jakémkoliv jiném prostředí.

6.21. Audity a inspekce

6.21.1. Zadavatel je oprávněn provést audit nebo inspekci souladu systému řízení bezpečnosti informací Poskytovatele s právem České republiky nebo podmínkami této Smlouvy, dodržování politik Poskytovatele a plnění povinností týkajících se zpracování osobních údajů. Audity a inspekce se řídí následujícími pravidly:

1. Poté, co Poskytovatel obdrží žádost Zadavatele o audit nebo inspekci se Strany dopředu dohodnou na: (a) možném termínu provedení auditu, bezpečnostních opatřeních a způsobu zajištění dodržení závazků mlčenlivosti během auditu, (b) předpokládaném začátku, rozsahu a době trvání inspekce, bezpečnostních opatřeních a způsobu zajištění dodržení závazků mlčenlivosti během inspekce.

2. Nedohodnou-li se Strany v souladu s bodem 1 výše na všech potřebných náležitostech auditu nebo inspekce do 14 dnů ode dne, kdy Poskytovatel obdržel žádost Zadavatele, stanoví termín, průběh a další náležitosti auditu nebo inspekce Zadavatel s přihlédnutím ke spravedlivým zájmům Poskytovatele.

3. Pro účely auditu nebo inspekce Poskytovatel zpřístupní Zadavatell nebo Zadavatelem pověřenému auditorovi veškeré prostory, zařízení, úložiště a systémy, které se týkají

systému řízení bezpečnosti informací, bezpečnostních politik Poskytovatele nebo kde dochází ke zpracování osobních údajů pro Zadavatele, pokud tím nedojde k porušení zákonných povinností Poskytovatele.

4. Poskytovatel může vznést písemné námitky proti jakémukoliv auditorovi, který byl pověřen Zadavatelem, pokud není auditor podle názoru Poskytovatele dostatečně kvalifikován, není nezávislý, je v soutěžním postavení vůči Poskytovateli nebo je jinak zjevně nevhodný. Vznesené námitky Zadavatel posoudí a pokud je shledá důvodnými, zvolí jiného auditora nebo provede audit sám.

5. Náklady spojené s auditem nebo inspekcí si každá Strana nese sama. Odměnu auditora pověřeného Zadavatelem hradí Zadavatel. Pokud by však audit nebo inspekce odhalily porušení Smlouvy ze strany Poskytovatele, uhradí odměnu auditora Poskytovatel.

6. Tato pravidla se použijí také na audity a inspekce prováděné u subdodavatelů Poskytovatele, zapojených do systému řízení bezpečnosti nebo majících vliv na bezpečnost informací a bezpečnostní politiky Poskytovatele, a dalších zpracovatelů osobních údajů.

7. Audit nebo inspekci je možné konat maximálně jednou za 6 měsíců.

6.22. Akceptace

a. V rámci etapy 1.5. provede Zadavatel akceptační testy. Poskytovatel mu poskytne potřebnou součinnost.

   i. Poskytovatel prokáže kompletnost dodávky a splnění povinných i hodnocených požadavků.

   ii. Poskytovatel prokáže aktivaci software (i hardware) aktivačními klíči či jinými prostředky, je-li aktivace potřebná.

   iii. Zadavatel provede test administrátorského rozhraní a možnost přidělení jednotlivých požadovaných rolí a ověření funkcí požadovaných ZD

   iv. Zadavatel provede výkonové testy prokazující shodu s požadovanými výkonnostními parametry:

      1. Výkon virtuálních serverů dle specifikace (vCPU, RAM)

      2. Výkon virtuálních disků: IOPS, throughput

   v. Testy s ohledem na použitelnost řešení v rutinním provozu

      1. Výkon/odezva databázového serveru

2. Odezva uživatelských rozhraní aplikací a softwarových rozhraní

b. O provedení akceptace a jejím výsledku je vyhotoven písemný akceptační protokol.

c. Poskytovatel zajistí zkušební (testovací neplacený) provoz dle 1.3. včetně technické podpory minimálně 1 specialisty na dodané řešení s odezvou do 1 hodiny od nahlášení požadavku v pracovní den v době od 8 h do 17 h.

d. Při předávání díla po částech bude po předání jednotlivých částí a dokončení díla jako celku následovat, akceptační řízení v plném rozsahu a předání celého díla.

e. Přechodem do plného provozu se rozumí okamžik akceptace díla v plném rozsahu včetně vypořádání všech vad a nedodělků.