

SMLOUVA O DÍLO

uzavřená ve smyslu zákona č. 89/2012 Sb., občanský zákoník, v platném znění
(dále jen „občanský zákoník“)

Níže uvedeného dne, měsíce a roku uzavřeli:

1. Městská část Praha 10

se sídlem: Vinohradská 3218/169, 100 00 Praha 10

IČO: 00063941

DIČ: CZ00063941

zastoupená: Ing. arch. Martinem Valovičem, starostou MČ Praha 10

oprávněn k smluvnímu jednání: Ing. Lukáš Karásek, vedoucí Odboru informatiky

(dále jen „**kupující**“ nebo „**zadavatel**“ na straně jedné)

a

2. NET-Services, s.r.o.

se sídlem: Českobrodská 3/17, Praha 9, 19000

bankovní spojení: Raiffeisen Bank, a.s.

č. účtu: 1161375/5500

IČO: 27909077

DIČ: CZ27909077

zastoupen: Ing. Hanou Černou Vavřincovou – jednatelkou

ID datové schránky: yz2p2at

zapsaný v obchodním rejstříku vedeném u Městského soudu v Praze, oddílu C pod spisovou značkou 125777

(dále jen „**prodávající**“ nebo „**dodavatel**“ na straně druhé)

(kupující a prodávající dále též označováni jako „**smluvní strany**“ nebo „**účastníci smlouvy**“)

tuto kupní smlouvu (dále jen „smlouva“)

I. Úvodní ustanovení

Tato smlouva je uzavřena na základě výsledku řízení zadávaného mimo režim zákona č. 134/2016 Sb. o zadávání veřejných zakázek, v platném znění, k plnění veřejné zakázky malého rozsahu s názvem „Migrace a aktualizace úložiště na distribuovanou SDS“.

II. Předmět smlouvy

1. Předmětem této smlouvy je závazek prodávajícího:

Migrace a aktualizace SW úložiště na distribuované úložiště CEPH. CEPH je vysoce škálovatelné, distribuované SW úložiště s otevřeným zdrojovým kódem, které poskytuje jednotné rozhraní pro blokové, objektové a souborové úložiště, dle technické specifikace se zárukou na dobu 12 měsíců včetně služeb instalace, konfigurace a integrace do ICT prostředí kupujícího. Vše dle požadavků kupujícího vymezených dále v této smlouvě a vyplývajících ze zadávacích podmínek na veřejnou zakázku (dále jen „**dodávka**“ nebo „**dílo**“).

2. Kupující se zavazuje **dílo** převzít a zaplatit prodávajícímu včas kupní cenu ve výši a za podmínek dle této smlouvy.

III. Kupní cena

1. Celková kupní cena za dílo, (dále jen „**cena**“) je sjednána v souladu s cenou, kterou prodávající nabídl v rámci zadávacího řízení na veřejnou zakázku.
2. Celková cena činí: 1.439.870,- Kč bez DPH, tj. 1.742.243,- Kč vč. 21% DPH.
3. Celková cena je sjednána jako závazná a nejvýše přípustná. Ke změně výše ceny může dojít pouze v případě změn příslušných daňových předpisů, tj. při změně výše zákonné sazby DPH v době vzniku zdanitelného plnění.
4. V celkové ceně jsou zahrnuty veškeré náklady prodávajícího nezbytné pro řádnou a včasnou **dodávku** dle této smlouvy, tedy doprava, veškeré služby podpory a aktualizace, poplatky, výkony a další činnosti nutné pro řádné splnění předmětu této smlouvy.
5. Kupující nebude prodávajícímu poskytovat žádné zálohy.

IV. Platební podmínky

1. Kupující se zavazuje zaplatit prodávajícímu cenu za dílo bezhotovostním převodem na bankovní účet prodávajícího uvedený na faktuře, a to na základě faktury vystavené prodávajícím po řádném splnění předmětu plnění dle této smlouvy. Splatnost faktury činí **30 dnů** od jejího prokazatelného doručení kupujícímu.
2. Prodávající vystaví fakturu do 5 kalendářních dnů po převzetí **díla** kupujícím v souladu s čl. V. této smlouvy.
3. Prodávající se touto smlouvou zavazuje, že jím vystavená faktura bude obsahovat všechny náležitosti řádného daňového dokladu dle platné právní úpravy.
4. V případě, že účetní doklady nebudou mít odpovídající náležitosti, je kupující oprávněn zaslat je ve lhůtě splatnosti zpět prodávajícímu k doplnění, aniž se tak dostane do prodlení se splatností. Důvody vrácení sdělí kupující prodávajícímu písemně zároveň s vráceným daňovým dokladem. V závislosti na povaze závady je prodávající povinen daňový doklad včetně jeho příloh opravit nebo vyhotovit nový. Lhůta splatnosti počíná běžet znovu od opětovného zaslání náležitě doplněných či opravených daňových dokladů.
5. Kupní cena se považuje za uhrazenou okamžikem odepsání fakturované ceny z bankovního účtu kupujícího. Pokud kupující uplatní nárok na odstranění vady dodávky nebo její části ve lhůtě splatnosti faktury, není kupující povinen až do odstranění vady dodávky nebo její části uhradit cenu dodávky. Okamžikem odstranění vady dodávky nebo její části začne běžet nová lhůta splatnosti faktury.
6. V případě prodlení kupujícího s úhradou ceny je prodávající oprávněn požadovat po kupujícím zaplacení úroků z prodlení ve výši 0,05% z dlužné částky za každý den prodlení.

V. Termín a způsob plnění

1. Prodávající se zavazuje uskutečnit dílo dle podmínek sjednaných v této smlouvě nejpozději do 6 kalendářních měsíců ode dne účinnosti této smlouvy. Doba realizace díla je členěna následovně:
 - a. Realizace díla - 5 kalendářních měsíců od účinnosti smlouvy.
 - b. Testovací provoz - 1 kalendářní měsíc a ukončení plnění dle odst. 1 písm a) tohoto článku.
2. Kupující nabývá vlastnické právo k dílu okamžikem protokolárního předání a převzetí díla od prodávajícího.
4. Případné vady díla při předání uvede kupující do protokolu. Pokud bude mít dílo nebo jeho jakákoliv část vady, které brání užívání nebo užívání podstatně ztěžují, je kupující oprávněn odmítnout převzetí díla. Bezvadné dílo se kupující zavazuje převzít a zaplatit jeho cenu.

VI. Místo plnění

1. Místem plnění je sídlo kupujícího na adrese Vinohradská 3218/169, 100 00 Praha 10, technické místnosti v budově.
2. Kontaktní osobou a odpovědným zaměstnancem kupujícího je pro účely této smlouvy určen Ing. Lukáš Karásek, vedoucí Odboru informatiky, tel.: +420 267 093 642, e-mail: lukas.karasek@praha10.cz.
3. Kontaktní osobou prodávajícího je pro účely této smlouvy určen: [REDACTED]

VII. Odstoupení od smlouvy

1. Kterákoliv smluvní strana může od této smlouvy odstoupit při podstatném porušení smluvních povinností druhou smluvní stranou.
2. Pro účely této smlouvy se za podstatné porušení smluvních povinností považuje takové porušení, u kterého smluvní strana porušující smlouvu měla nebo mohla předpokládat, že při takovémto porušení smlouvy, s přihlédnutím ke všem okolnostem, by druhá smluvní strana neměla zájem smlouvu uzavřít; zejména
 - a) prodlení prodávajícího s dodáním dodávky nebo její jakékoliv části;
 - b) prodlení prodávajícího s řádným a včasným odstraněním vad dodávky nebo jakékoliv její části;
 - c) prodlení kupujícího s úhradou ceny;
 - d) porušení povinnosti prodávajícího stanovené v čl. IX. odst. 2 smlouvy (neudržování pojistné smlouvy v platnosti po celou dobu trvání této smlouvy);
3. Odstoupení od této smlouvy musí mít písemnou formu, musí v něm být přesně popsán důvod odstoupení, podpis odstupující smluvní strany, jinak je odstoupení od této smlouvy neplatné. Tato smlouva zaniká ke dni doručení oznámení odstupující smluvní strany o odstoupení druhé smluvní straně.
4. Odstoupení od této smlouvy se nedotýká práva na náhradu škody vzniklého z porušení smluvní povinnosti ani práva na zaplacení smluvní pokuty a úroku z prodlení.

5. V případě předčasného ukončení smlouvy dohodou, výpovědí či odstoupením jsou smluvní strany povinny provést vypořádání vzájemných práv a povinností v souladu s právními předpisy.

VIII. Sankce

1. Pro případ prodlení prodávajícího s termínem plnění uvedeným v článku V. této smlouvy, se prodávající zavazuje uhradit kupujícímu smluvní pokutu ve výši 5.000 Kč, a to za každý i započatý den prodlení.
2. Pro případ porušení povinností stanovených v článku IX. této smlouvy, se prodávající zavazuje uhradit kupujícímu smluvní pokutu ve výši 2.000 Kč, a to za každý i započatý den prodlení.
3. Uplatněním práv z vad či uplatněním smluvních pokut není dotčeno právo na náhradu újmy v plné výši. Smluvní pokutu je kupující oprávněn započíst oproti pohledávce prodávajícího.
4. Smluvní pokuta je splatná do 15 dnů ode dne doručení výzvy k jejímu zaplacení.
5. Prodávající je povinen nahradit kupujícímu v plné výši újmu, která kupujícímu vznikla vadným plněním nebo jako důsledek porušení povinností a závazků prodávajícího dle této smlouvy.

IX. Pojištění

1. Prodávající je povinen před podpisem této smlouvy předložit kupujícímu pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou prodávajícím třetím osobám, včetně škod způsobených vadou výrobku, při výkonu podnikatelské činnosti, přičemž limit pojistného plnění bude činit minimálně 1 000 000,- Kč.
2. Prodávající je povinen udržovat pojistnou smlouvu dle předchozího odstavce v platnosti po celou dobu trvání této smlouvy a do druhého pracovního dne od vyzvání kupujícího je povinen mu ji předložit k nahlédnutí.

X. Záruka za jakost

Prodávající přejímá záruku na jakost a úplnost dodávky, ve smyslu ustanovení § 2113 až § 2117 občanského zákoníku po dobu trvání smlouvy. Záruční doba neběží po dobu, po kterou kupující nemůže užívat dodávku nebo její jakoukoliv část pro reklamované vady.

XI. Mlčenlivost a ochrana důvěrných informací

1. Vzhledem k tomu, že prodávající bude mít v rámci plnění této smlouvy přístup k informacím, které kupující považuje za důvěrné, sjednávají smluvní strany dohodu o mlčenlivosti, jejímž předmětem je úprava práv a povinností smluvních stran ve vztahu k ochraně důvěrných informací (dále jen „dohoda o mlčenlivosti“).
2. Práva a povinnosti vyplývající z dohody o mlčenlivosti přetrvávají i po skončení této smlouvy, jakož i po ukončení spolupráce mezi smluvními stranami, bez ohledu na stádium ukončení spolupráce.
3. Náležitosti dohody o mlčenlivosti a podrobnější vymezení práv a povinností smluvních stran jsou uvedeny v příloze č. 2 této smlouvy.

4. Za porušení jakékoli povinnosti stanovené v dohodě o mlčenlivosti vzniká prodávajícímu povinnost zaplatit kupujícímu smluvní pokutu ve výši 100.000,- Kč za každý jednotlivý případ porušení. Smluvní pokuta je splatná do 15 dnů od doručení výzvy k úhradě smluvní pokuty. Vznikem nároku na smluvní pokutu, ani jejím zaplacením není dotčen nárok na náhradu újmy v plné výši.

XII. Bezpečnostní politika

1. Smluvní strany sjednávají dohodu o bezpečnostní politice a vzdáleném přístupu VPN do interní sítě kupujícího (dále jen „dohoda o bezpečnostní politice“). Dohoda o bezpečnostní politice upravuje pravidla a požadavky pro přístup prodávajícího do interní sítě kupujícího, včetně přístupu prostřednictvím VPN. Obsahuje informace o tom, jaké bezpečnostní politiky a postupy musí prodávající dodržovat, jaké typy přístupů jsou povoleny, jaká bezpečnostní opatření jsou nutná pro ochranu sítě a dat, a jaké jsou postupy v případě bezpečnostních incidentů.
2. Práva a povinnosti vyplývající z dohody o bezpečnostní politice přetrvávají i po skončení této smlouvy, jakož i po ukončení spolupráce mezi smluvními stranami, bez ohledu na stádium ukončení spolupráce.
3. Náležitosti dohody o bezpečnostní politice a podrobnější vymezení práv a povinností smluvních stran jsou uvedeny v příloze č. 3 této Smlouvy.

XIII. Závěrečná ustanovení

1. Tato smlouva nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem zveřejnění v registru smluv, které zajistí kupující.
2. Práva vzniklá z této smlouvy nesmí být postoupena bez předchozího písemného souhlasu druhé smluvní strany. Za písemnou formu nebude pro tento účel považována výměna e-mailových, či jiných elektronických zpráv.
3. Tato smlouva je uzavřena podle práva České republiky. Ve věcech výslovně neupravených touto smlouvou se smluvní vztah řídí občanským zákoníkem.
4. Smluvní strany vylučují uplatnění ustanovení § 1765 odst. 1 a § 1766 občanského zákoníku na svůj smluvní vztah založený touto smlouvou.
5. Nevymahatelnost nebo neplatnost kteréhokoli ustanovení této smlouvy neovlivní vymahatelnost nebo platnost této smlouvy jako celku, vyjma těch případů, kdy takové nevymahatelné nebo neplatné ustanovení nelze vyčlenit z této smlouvy, aniž by tím pozbyla platnosti. Smluvní strany se pro takový případ zavazují vynaložit v dobré víře veškeré úsilí na nahrazení takového neplatného nebo nevymahatelného ustanovení vymahatelným a platným ustanovením, jehož účel v nejvyšší možné míře odpovídá účelu původního ustanovení a cílům této smlouvy.
6. Změna nebo doplnění smlouvy může být uskutečněna pouze písemným dodatkem k této smlouvě podepsaným oběma smluvními stranami (vyjma změny kontaktních osob, kde stačí změnu provést formou e-mailové zprávy s tím, že druhá smluvní strana potvrdí přijetí této e-mailové zprávy).

7. Smluvní strany podpisem této smlouvy potvrzují, že jsou seznámeny s tím, že tato smlouva podléhá povinnosti uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Smluvní strany prohlašují, že žádnou z informací uvedených v nabídce prodávajícího na veřejnou zakázku a v této smlouvě nepovažují za předmět obchodního tajemství ve smyslu § 504 občanského zákoníku, a výslovně souhlasí s tím, aby byl v registru smluv uveřejněn celý obsah smlouvy a aby byla smlouva uvedena v evidenci smluv vedené Úřadem městské části Praha 10. Uveřejnění smlouvy zajistí kupující.
8. Prodávající bere na vědomí, že kupující je povinným subjektem ve smyslu ust. § 2 odst. 1 zák. č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění, a že v důsledku tohoto svého postavení je povinen na žádost poskytnout informace o skutečnostech uvedených v této smlouvě, resp. o jejím samotném uzavření. Pro ten případ prodávající výslovně prohlašuje, že žádný údaj uvedený v této smlouvě ani samotnou skutečnost, že byla uzavřena, nepokládá za své obchodní tajemství.
9. Smlouva je vyhotovena v elektronické podobě v jednom vyhotovení v českém jazyce s elektronickými podpisy obou smluvních stran v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů. V případě, že prodávající nedisponuje elektronickým podpisem, je smlouva vyhotovena ve třech listinných stejnopisech s platností originálu, přičemž kupující obdrží dva stejnopisy a prodávající jeden stejnopis.
10. Přílohy:
PŘÍLOHA ČÍSLO 1 SMLOUVY: TECHNICKÁ SPECIFIKACE
PŘÍLOHA ČÍSLO 2 SMLOUVY: NÁLEŽITOSTI A PODMÍNKY DOHODY O MLČENLIVOSTI
PŘÍLOHA ČÍSLO 3 SMLOUVY: NÁLEŽITOSTI A PODMÍNKY DOHODY O BEZPEČNOSTNÍ POLITICE A VZDÁLENÉM PŘÍSTUPU VPN DO INTERNÍ SÍTĚ ZADAVATELE

V Praze dne:

V Praze dne:

KUPUJÍCÍ:

PRODÁVAJÍCÍ:

Městská část Praha 10
Ing. Lukáš Karásek

NET-Services, s.r.o.
Ing. Hana Černá Vavřincová

PŘÍLOHA ČÍSLO 1 SMLOUVY: TECHNICKÁ SPECIFIKACE

Prodávající vyplňuje pouze pole ve **žlutě** označených sloupcích.

„Migrace a aktualizace úložiště na distribuovanou SDS“

Technická specifikace a popis základní funkcionality SW distribuovaného úložiště CEPH.

Popis prostředí zadavatele:

Zadavatel disponuje tímto HW a SW vybavením:

- 10 ks samostatných HW serverů (v současné době KVM virtualizační boxy s výhledem přechodu na virtualizační platformu Proxmox) – 4U Supermicro, provozovaný OS Linux Debian a MS Windows Server a virtualizační prostředí KVM/Proxmox (6 ks čisté KVM, 4 ks cluster Proxmox)
- 74 ks virtuálních serverů které mají dohromady 126 ks virtuálních HDD
- 4 ks TOR switche S6730-H28Y4C – 2 ks ve stacku v lokalitě 1, 2 ks ve stacku pro lokalitu 2 (lokalita 2 v přípravě), HW servery připojeny redundantně do obou switchů ve stacku 10G linkami

Požadavky instalačních a konfiguračních služeb realizace:

- Dodávka nutného nového hardware, který musí splňovat všechny podmínky výrobce pro použití v České republice a uplatnění případných reklamačních vad a požadavků na servis v místě instalace.
- Součástí HW dodávky zařízení je i veškeré příslušenství (montážní prvky) pro jejich instalaci.
- Instalace a konfigurace spočívají:
 - o Fyzická instalace hardware do současných fyzických serverů.
 - o Upgrade současných serverů do nejvyšší stabilní verze operačního systému Debian pro nasazení aktuálně dostupné verze CEPH, která bude kompatibilní s aktuálně stabilní verzí virtualizační platformy Proxmox (Instalace virtualizační platformy Proxmox není součástí této výzvy).
 - o Konfigurace sítí, úložišť a virtualizačního prostředí.
- Testování a uvedení do provozu:
 - o Komplexní testování všech komponent a systémů.
 - o Odborné předvedení a zaškolení pro min. 2 pracovníky kupujícího.
 - o Zpracování základní technické dokumentace, min. v rozsahu schéma zapojení a popisu topologie.
 - o Uvedení datového centra do plného provozu.
- K páteřnímu propojení jednotlivých komponent musí být použita stávající datová kabeláž, ostatní propojení bude řešeno dodávkou nových patch kabelů od prodávajícího.
- Součástí dodávky HW je požadovaná záruka a podpora od výrobce na dobu minimálně 12 měsíců.
- Žádné z nabízených zařízení/řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze software/firmware, tzn. nelze dodat zařízení/řešení kde je požadovaná funkce teprve zařazené na tzv. roadmapu.

Požadovaná funkcionality/vlastnosti SW distribuovaného úložiště	Splňuje Ano / Ne, případně způsob splnění – doplní uchazeč
Obecné požadavky	
Škálovatelnost: CEPH musí být vysoce škálovatelný, což znamená, že jej můžeme rozšiřovat za běhu bez nutnosti vypnutí služeb. Můžeme snadno přidávat další servery nebo disky a CEPH automaticky integruje tyto nové zdroje do svého clusteru.	Ano
Odolnost vůči selhání: CEPH musí být navržen tak, aby byl vysoce odolný vůči selhání. Používá distribuované replikace nebo erasure coding k zajištění dostupnosti a integrity dat, i když dojde k selhání některých disků nebo serverů nebo celé lokality.	Ano
Vysoká dostupnost (HA): Díky své architektuře bez jediného bodu selhání musí CEPH zajistit vysokou úroveň dostupnosti dat. Data jsou vždy dostupná, i když dojde k výpadku části systému.	Ano
Flexibilita: CEPH nutnost podpory široké škály typů úložišť (SSD, HDD), včetně blokového úložiště, souborového systému a objektového úložiště, což umožňuje používat CEPH pro různé typy pracovních zátěží a aplikací.	Ano
Kontrolní mechanismy CEPH: Je požadována automatická detekce a oprava chyb, což minimalizuje dobu nedostupnosti a potřebu manuálních zásahů.	Ano
Snížení nákladů: Jako software definované úložiště může CEPH výrazně snížit celkové náklady na vlastnictví, protože umožňuje použití komoditního hardware namísto drahých dedikovaných úložných systémů.	Ano
Vylepšená správa dat: Funkce jako thin provisioning, snapshoty a klonování dat poskytují pokročilé možnosti správy dat, které mohou zlepšit efektivitu a flexibilitu.	Ano
Vylepšená výkonnost: Distribuovaná architektura CEPH umožňuje paralelní zpracování dat, což může zlepšit výkonnost úložiště pro náročné aplikace a velké objemy dat.	Ano
Otevřený zdroj: Jako řešení s otevřeným zdrojovým kódem má CEPH silnou komunitní podporu a poskytuje flexibilitu při přizpůsobování a integraci do IT prostředí.	Ano
Síť: Vysokorychlostní síťová infrastruktura s redundancí a podporou moderních protokolů.	Ano
Zabezpečení: Komplexní bezpečnostní řešení zahrnující fyzickou ochranu, síťové zabezpečení, zabezpečení přístupu a šifrování dat.	Ano
Zálohování: Implementace robustního systému zálohování a obnovy dat.	Ano
Architektura SW distribuovaného úložiště	
Monitors: Centrální řídicí jednotka clusteru, která spravuje konfiguraci a stav systému.	Ano
OSD (Object Storage Devices): Fyzická úložná zařízení, která ukládají data.	Ano
Schopnost prodávajícího provést migrační práce – postup migrace	
Instalace CEPH na všechny boxy – servery.	Ano
Instalace separátních síťových karet (oddělení provozu CEPH od provozu úřadu).	Ano
Nastavení boxů – serverů (síť pro CEPH).	Ano
Nastavení switchů Huawei pro CEPH.	Ano

Každý BOX musí být součástí CEPH jako klient – instalace klientských částí.	Ano
Instalace minimálně 5 monitor serverů (monitor server slouží k řízení CEPH).	Ano
Instalace minimálně 2 webových konzolí CEPH.	Ano
Instalace OSD a sestavení CEPH na každém boxu (do CEPH budou jako OSD zařazeny zadavatelem určené pevné disky – již připraveny v BOXech).	Ano
Zařazení BOXu do CEPH clusteru.	Ano
Sestavení CEPH.	Ano
Nepravidelná ruční záloha virtuálních serverů.	Ano
Kontrola dokumentace: pojmenování pevných disků.	Ano
Vypnutí virtuálních strojů.	Ano
Vytvoření blokových zařízení pro jednotlivé virtuální servery na CEPH.	Ano
Připojení nových blokových zařízení z CEPH na BOX, kde jsou data virtuálního serveru.	Ano
Bitová kopie lokálních dat virtuálního serveru do CEPH.	Ano
Odpojení blokových zařízení virtuálního stroje.	Ano
Úprava konfigurace disků virtuálního serveru v Proxmox.	Ano
Spuštění virtuálního serveru z Proxmox.	Ano
Kontrola služeb.	Ano
Kontrola virtualizace (stabilní běh virtuálního serveru).	Ano
Zrušení lokálního úložiště na BOXu.	Ano
Zrušení lokálních diskových polí.	Ano
Začlenění uvolněných disků do CEPH.	Ano
Ukončení migrace a otestování plné funkčnosti.	Ano
Požadovaný HW a jeho instalace	
10 ks síťová karta (S25G-i2S - Dual port 25GbE (SFP28) PCI-E8 (g3) LP)	Ano
20 ks SFP28 (10/ 25Gbps, SM, 1310nm DFB, 10km, 3,3V,LC Duplex, DDM, HUAWEI kompatibilní)	Ano
20 ks SFP28 (10/ 25Gbps, SM, 1310nm DFB, 10km, 3,3V,LC Duplex, DDM, Intel kompatibilní)	Ano
25 ks Patchcord optický (SM OS1/OS2 9/125, LC/PC-LC/PC, 5m)	Ano
Montáž, instalace a konfigurace do stávající ICT infrastruktury objednatele.	Ano
Migrace jednotlivých boxů – serverů je možno provádět jen při úplné provozní odstávce, tedy jen ve dnech pracovního klidu (jen o víkendech).	Ano
Záruka na dodaný HW minimálně 12 měsíců.	Ano

PŘÍLOHA ČÍSLO 2 SMLOUVY: NÁLEŽITOSTI A PODMÍNKY DOHODY O MLČENLIVOSTI

1 DŮVĚRNÉ INFORMACE

- 1.1 Za „*Důvěrné informace*“ se ve smyslu Smlouvy a této přílohy považují veškeré informace, údaje a dokumenty, poskytnuté Zadavatelem Dodavateli v souvislosti se Smlouvou a plněním závazků z ní vyplývajících, pokud tyto informace, údaje a dokumenty nebyly Zadavatelem dosud zveřejněny. Na charakter Důvěrných informací nemá vliv skutečnost, zda jsou či budou poskytovány v písemné, ústní či elektronické podobě, ani skutečnost, zda byly poskytnuty přímo Zadavatelem, či jeho poradci, zástupci, zaměstnanci, a současně zda již byly poskytnuty před uzavřením této Smlouvy nebo poté.
- 1.2 Důvěrnými informacemi je zejména veškeré know-how, obchodní tajemství, předměty duševního vlastnictví (ochranné známky, loga, obchodní značky, počítačový software, data apod.), zdrojové kódy, a to i včetně veškerého know-how a koncepcí, které z jednotlivých Důvěrných informací tak, jak jsou uvedeny výše, vyplývají nebo mohou vyplývat
- 1.3 Za Důvěrné informace se nepovažují informace a údaje:
- a. které jsou nebo se stanou obecně známými bez zavinění Dodavatele; nebo
 - b. které Dodavatel bez porušení smluvní či zákonné povinnosti získal dříve, než je obdržel od Zadavatele; nebo
 - c. které byly Dodavateli bez porušení smluvní či zákonné povinnosti zpřístupněny jinou oprávněnou osobou; nebo
 - d. jejichž sdělení (či zpřístupnění) je vyžadováno dle obecně závazných právních předpisů, a to pouze v nezbytně nutné míře stanovené obecně závazným právním předpisem; nebo
 - e. které byly zveřejněny se souhlasem Zadavatele; nebo
 - f. které jsou všeobecně známé (například z odborných publikací, jako součást vědeckého poznání apod.); nebo
 - g. které jsou vyžádány soudem nebo jiným orgánem veřejné moci na základě zákona a jsou použity pouze k tomuto účelu.

2 PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

- 2.1 Dodavatel se zavazuje využívat Důvěrné informace výhradně za účelem plnění svých závazků vyplývajících ze Smlouvy (dále jen „*Účel*“), k činnostem směřujícím k plnění Účelu

či s ním souvisejícím, není-li na základě výslovného písemného souhlasu Zadavatele sjednáno jinak.

- 2.2 Důvěrné informace nesmí být Dodavatelem bez předchozí souhlasu Zadavatele žádným způsobem sděleny nebo zpřístupněny jakékoliv třetí osobě s výjimkou zaměstnanců Dodavatele, konzultantů nebo odborných poradců, příp. subdodavatelů, kteří poskytují poradenství Přijímající straně týkající se Účelu (dále jen „**Poradci**“), a to pouze za předpokladu, že tyto osoby potřebují být s konkrétní Důvěrnou informací seznámeni vzhledem k plnění Účelu. Tyto osoby budou zavázány povinností mlčenlivosti minimálně v takovém rozsahu, v jakém je zavázán Dodavatel na základě této přílohy.
- 2.3 Dodavatel je povinen nakládat se všemi Důvěrnými informacemi jako s důvěrnými, chránit jejich vyjádření, zajistit bezpečnost Důvěrných informací a chránit Důvěrné informace před neoprávněným přístupem, poskytnutím, předáním, zpracováním, uveřejněním a použitím a za tím účelem přijmout veškerá rozumně očekávatelná organizační a technická opatření.
- 2.4 Dodavatel se zavazuje žádné Důvěrné informace, poznatky z Důvěrných informací vyplývající ani závěry na Důvěrných informacích založené nevyužít ve svůj prospěch ani ve prospěch třetí osoby.
- 2.5 Dodavatel nesmí pořizovat kopie Důvěrných informací, ledaže je to nezbytné pro plnění Účelu a za předpokladu, že všechny tyto kopie jsou označeny jako důvěrné a bez zbytečného odkladu po naplnění Účelu budou zlikvidovány.
- 2.6 Dodavatel po skončení Smlouvy nebo naplnění Účelu vrátí nebo zničí, podle pokynů Zadavatele, veškeré hmotné materiály (mimo jiné včetně listin, disků, CD nebo jiných médií umožňujících zápis) originály nebo kopie dokumentů obsahujících Důvěrné informace, které mu Zadavatel poskytl nebo které Dodavatel získal na základě činnosti dle Smlouvy, a poskytne Zadavateli důkaz o jejich zničení.
- 2.7 Dodavatel je povinen bez zbytečného odkladu informovat Zadavatele o existenci jakékoli skutečnosti, která by mohla přímo nebo nepřímo ohrozit existenci, trvání, vyjádření nebo hodnotu Důvěrných informací a přijmout opatření k jejich ochraně, jakož i poskytnout Zadavateli součinnost k tomu, aby nemohlo dojít k přímému nebo nepřímému ohrožení existence, trvání, vyjádření nebo hodnoty Důvěrných informací.
- 2.8 V případě, že má být Důvěrná informace zpřístupněna v souladu s touto přílohou, je Dodavatel povinen o této skutečnosti před samotným zpřístupněním informovat Zadavatele, jakož i o všech okolnostech a rozsahu zpřístupnění.

- 2.9** V případě, že se Dodavatel dozví o jakémkoli neoprávněném zpřístupnění Důvěrné informace, je povinna okamžitě informovat Zadavatele, sdělit mu všechny podstatné okolnosti a přijmout všechna opatření nezbytná k zabránění vzniku újmy nebo omezení rozsahu újmy již vzniklé a k zamezení dalšímu šíření Důvěrné informace.
- 2.10** Důvěrné informace zůstávají vlastnictvím Zadavatele i po jejich zpřístupnění.
- 2.11** Pokud Dodavatel zveřejní či zpřístupní Důvěrné informace Poradci nebo jakékoliv jiné osobě, odpovídá za jednání či opomenutí těchto osob, které spočívá v neoprávněném rozšiřování, užití a/nebo zveřejnění takovéto Důvěrné informace, resp. za jakékoliv porušení povinností vyplývajících z této přílohy ze strany těchto osob.
- 2.12** Dodavatel je srozuměn s tím, že není oprávněn užít či dále zpřístupnit Důvěrné informace nabyté během trvání Smlouvy jiným způsobem a k jinému účelu, než jak je předpokládáno touto přílohou.
- 2.13** Pokud Dodavatel poruší jakýkoli závazek plynoucí z této přílohy, je povinen se neprodleně takového jednání na základě výzvy Zadavatele zdržet, informovat o tom Zadavatele a okamžitě učinit opatření směřující k odstranění a náhradě veškeré újmy způsobené Zadavateli či jeho smluvním partnerům tímto jednáním a uvedení do původního stavu, bude-li to možné.

3 ZÁVĚREČNÁ USTANOVENÍ

- 3.1** Jakékoliv porušení práv a povinností vyplývajících z této přílohy představuje též závažné porušení Smlouvy.
- 3.2** Pokud se ukáže některé ustanovení této přílohy neplatné, neúčinné nebo nevymahatelné, zbývající části zůstávají v platnosti. Ohledně neplatného, neúčinného nebo nevymahatelného ustanovení se Smluvní strany zavazují, že je buď dodatkem upraví tak, aby byla zajištěna jeho platnost, účinnost a vymahatelnost, a to při co největším zachování původních záměrů smluvních stran nebo, pokud to není možné, budou vykládat toto ustanovení způsobem, jako by neplatná, neúčinná nebo nevymahatelná část nebyla nikdy v této příloze obsažena.

PŘÍLOHA ČÍSLO 3 SMLOUVY: NÁLEŽITOSTI A PODMÍNKY DOHODY O BEZPEČNOSTNÍ POLITICE A VZDÁLENÉM PŘÍSTUPU VPN DO INTERNÍ SÍTĚ ZADAVATELE

3 ÚVODNÍ USTANOVENÍ

- 1.4** Tato příloha stanoví práva a povinnosti Zadavatele a Dodavatele týkající se bezpečnostních opatření při plnění Smlouvy a dodržování bezpečnostní politiky Zadavatele.
- 1.5** Tato příloha dále stanoví pravidla a požadavky pro bezpečný vzdálený přístup Dodavatele do Interní sítě prostřednictvím VPN (Virtuální Privátní Síť).
- 1.6** Cílem této přílohy je zajistit ochranu Interní sítě a dat Zadavatele před neautorizovaným přístupem a potenciálními bezpečnostními hrozbami.

2 DEFINICE POJMŮ

- 2.1** Pro účely této přílohy mají následující pojmy níže popsany význam, není-li v konkrétním případě stanoveno jinak:
- 2.1.1** „*Interní síť*“ se rozumí veškerá síťová infrastruktura Zadavatele, včetně, ale neomezeno na, servery, pracovní stanice, virtuální stanice a servery, databáze.
- 2.1.2** „*VPN*“ se rozumí virtuální privátní síť umožňující zabezpečený vzdálený přístup do Interní sítě.
- 2.1.3** „*Dat*“ se rozumí veškeré informace, údaje a dokumenty, k nimž získá Dodavatel přístup na základě přístupu do Interní sítě.
- 2.1.4** „*Interním bezpečnostním řádem*“ se rozumí interní předpis, směrnice nebo jiný dokument na straně Dodavatele, který stanovuje pravidla, politiky a postupy týkající se ochrany informací, dat a infrastruktury organizace před interními i externími hrozbami. Cílem tohoto řádu je zajištění základních pravidel kybernetické bezpečnosti a také integrity, dostupnosti a důvěrnosti všech informačních aktiv.
- 2.1.5** „*Zařízením*“ se rozumí jakýkoli hardwarový komponent nebo soubor hardwarových komponent, které jsou využívány k přístupu do Interní sítě nebo správě, zpracování a ukládání Dat. To zahrnuje, ale není omezeno na, koncová zařízení (počítače, notebooky, mobilní telefony, tablety a další), servery, síťové komponenty a další periferní zařízení používaná v kontextu plnění Smlouvy.
- 2.1.6** „*Komplexita hesla*“ je stanovena tak, že heslo běžného uživatelského účtu, který je chráněn vícefaktorovou autentizací (MFA) musí mít minimálně 8 znaků. Běžný

uživatelský účet, který není chráněn MFA musí mít alespoň 12 znaků. Privilegovaný účet, bez ohledu na MFA, musí mít alespoň 17 znaků. Technický nebo systémový účet musí mít alespoň 22 znaků. Hesla k šifrování a ochraně souborů musí mít alespoň 10 znaků. Všechna hesla musí zároveň splňovat minimálně tři ze čtyř následujících kritérií: obsahuje alespoň jedno malé písmeno, jedno velké písmeno, jednu číslici a jeden speciální znak.

3 BEZPEČNOSTNÍ POLITIKY A POSTUPY

3.1 Bezpečnost informací a dodržování bezpečnostní politiky Zadavatele

- 3.1.1 Dodavatel se zavazuje dodržovat bezpečnostní standardy a opatření týkající se přístupu a používání Interní sítě Zadavatele. Dodavatel se dále zavazuje k odpovědnému chování při manipulaci s Daty a systémy Zadavatele a k zajištění, že jeho činností nedojde úmyslně ani neúmyslně k poškození Interní sítě, Dat nebo operací Zadavatele.
- 3.1.2 Dodavatel se zavazuje zavést a dodržovat svůj Interní bezpečnostní řád, který zajistí řádnou technickou a organizační ochranu Dat Zadavatele, což zahrnuje implementaci odpovídajících bezpečnostních opatření a postupů, které zabraňují neoprávněnému přístupu, úniku, ztrátě nebo jakékoliv jiné kompromitaci dat. Tyto opatření musí být v souladu s platnými zákony a normami pro ochranu dat a informační bezpečnost. Interní bezpečnostní řád musí obsahovat politiky pro správu přístupových práv a požadavky na hesla, šifrování, zabezpečení komunikace, aktualizace softwaru, záplatování zranitelností a postupy v případě bezpečnostních incidentů.
- 3.1.3 Dodavatel je povinen zajistit pravidelnou aktualizaci veškerých Zařízení a softwaru, který používá pro přístup do Interní sítě nebo pro práci s Daty. Všechna koncová Zařízení musí obsahovat alespoň ochranu proti virům a malware, která je pravidelně aktualizována. Přístup ke koncovým zařízením musí být chráněn biometrickým ověřením nebo heslem splňujícím požadavky na minimální komplexitu.
- 3.1.4 Dodavatel je povinen zajistit, že veškeré přístupové údaje a hesla k Zařízení, síti VPN nebo jiným systémům, která mají přístup do Interní sítě nebo k Datům, budou uchovávány v tajnosti, přiděleny pouze jedné osobě a nebudou sdíleny s jinými uživateli nebo neautorizovanými osobami.
- 3.1.5 Dodavatel je povinen používat šifrování pro veškerá Data přenášená mezi Dodavatelem a Zadavatelem, aby zajistil jejich ochranu. Pro Data uložená na

pevných discích Zařízeních a jiných přenosných úložištích se musí použít šifrování s minimálně 256-bitovým AES standardem nebo jiným, který dosahuje srovnatelné úrovně zabezpečení. Pro data přenášená mezi sítěmi musí být zajištěno šifrování prostřednictvím protokolů, které splňují standardy TLS 1.2 nebo vyšší. Dodavatel dále zaručuje, že klíče pro šifrování a dešifrování budou spravovány v souladu s přísnými bezpečnostními postupy, aby se předešlo jakékoli možnosti neoprávněného přístupu nebo zneužití. Případná hesla musí splňovat minimální Komplexitu hesla.

- 3.1.6 Dodavatel se zavazuje zavést bezpečné komunikační kanály pro přenos dat mezi svými systémy a systémy Zadavatele. Je vyžadováno používání šifrovacích metod (TLS/SSL certifikáty) s nejvyšší možnou mírou zabezpečení všude tam, kde je to technicky možné. Stejně pravidlo se uplatní i pro webové technologie a jiné online transakce.
- 3.1.7 Data je zakázáno nahrávat na veřejná uložště, a to i v případě, že jsou šifrována. Data je zakázáno sdílet s jinými subjekty bez předchozího prokazatelného souhlasu Zadavatele.
- 3.1.8 Dodavatel se zavazuje zajistit adekvátní fyzickou bezpečnost všech Zařízeních a datových center, která jsou využívána k poskytování služeb Zadavateli. Dodavatel zajišťuje kontrolu přístupů, využívá bezpečnostní karty, biometrické systémy a kódované zámky, které omezují vstup pouze autorizovaným osobám. Datová centra využívaná Dodavatelem pro poskytování služeb Zadavateli musí být vybavena bezpečnostními kamerami, alarmy pro detekci a reakci na neoprávněný přístup nebo jiné bezpečnostní incidenty jako je například požár nebo povodeň.
- 3.1.9 V případě, že Dodavatel poskytuje Zadavateli službu, která může být ohrožena útoky typu Denial of Service (DoS) nebo Distributed Denial of Service (DDoS), tak se zavazuje implementovat efektivní protiopatření k ochraně síťové infrastruktury za použití pokročilých detekčních a filtračních systémů, které identifikují a izolují neobvyklý nebo škodlivý síťový provoz. Dodavatel dále implementuje síťové bariéry a firewally s pravidly pro dynamické blokování adres, které se pokoušejí provádět tyto útoky. Pro zvýšení odolnosti proti těmto hrozbám musí být veškerá Zařízení pravidelně aktualizována.
- 3.1.10 Dodavatel se zavazuje zajistit pravidelné školení a osvětu v oblasti kybernetické bezpečnosti u všech svých zaměstnanců, kteří poskytují nebo se podílí na poskytování služeb Zadavateli. Dodavatel zajistí obeznámení zaměstnanců s

aktuálními hrozbami a postupy v oblasti kybernetické bezpečnosti. Školení musí absolvovat každý zaměstnanec, který poskytuje službu Zadavateli alespoň jednou ročně.

- 3.1.11 Dodavatel se zavazuje spolupracovat se Zadavatelem na zvýšení kybernetické bezpečnosti Interní sítě. Pokud Zadavatel upozorní Dodavatele na jakoukoliv bezpečnostní zranitelnost spojenou se službami, které Dodavatel poskytuje, je Dodavatel povinen bezodkladně, a nejpozději do 30 dnů od oznámení přijmout nápravná opatření.
- 3.1.12 Dodavatel musí získat výslovný souhlas Zadavatele před jakýmkoli zásahem nebo změnou v Datech, na Interní síti, v systémech nebo jiných službách používaných v produkčním prostředí Zadavatele. Bez tohoto souhlasu nesmí Dodavatel provádět žádné akce. Výjimky z tohoto pravidla jsou povoleny pouze v případech, kdy by nečinnost mohla vést k majetkové nebo nemajetkové újmě na straně Zadavatele nebo Dodavatele, například v případě kybernetických incidentů.
- 3.1.13 Dodavatel bere na vědomí, že veškeré aktivity Dodavatele a jeho plnění realizované v prostředí Zadavatele může být monitorováno a vyhodnocováno.
- 3.1.14 V případě ukončení spolupráce mezi Dodavatelem a Zadavatelem je Dodavatel povinen předat veškerá data a provozní údaje nastupujícímu dodavateli nebo Zadavateli, a to včetně veškeré dokumentace spojené s provozem systému. Dále je Dodavatel povinen poskytnout veškerou nezbytnou součinnost novému dodavateli během přechodného období, včetně předání know-how.

3.2 Oprávnění užívat Data

- 3.2.1 Dodavatel je povinen implementovat a dodržovat systém řízení přístupu pro své zaměstnance, pracovníky či subdodavatele, který zajistí minimalizaci přístupu k Datům a do Interní sítě Zadavatele na nezbytně nutnou úroveň pro efektivní plnění Smlouvy. Uvedený systém přístupu zajistí, že každý přistupuje jen k těm Datům a prostředkům, která jsou nezbytná pro jeho práci, čímž je zajištěna ochrana před neoprávněným přístupem a zneužitím.
- 3.2.2 Dodavatel není oprávněn nahlížet do, přistupovat k, stahovat, kopírovat, ani jinak zpřístupňovat jakákoli Data, která nejsou přímo potřebná pro plnění smluvních povinností, bez předchozího prokazatelného souhlasu Zadavatele.

- 3.2.3 Pro přístup Dodavatele k Datům nebo do Interní sítě je zpravidla využíváno připojení VPN, které je chráněno vícefaktorovou autentizací (MFA). V případě, že Dodavatel využívá i jinou formu přístupu k Datům nebo do Interní sítě, tak je povinen zajistit použití MFA u všech uživatelů tak, aby zajistil ochranu těchto aktiv před přístupem neautorizovaných osob. Výjimka z povinnosti použití MFA je možná pouze v případech, kdy její implementace není technicky možná.

3.3 Kontrola a audit Dodavatele

- 3.3.1 Zadavatel má právo provádět zákaznický audit Dodavatele, který může zahrnovat kontrolu dodržování smluvních podmínek, bezpečnostních pravidel, Interního bezpečnostního řádu a dalších aspektů souvisejících s plněním Smlouvy.
- 3.3.2 Audit může být prováděn až dvakrát ročně nebo častěji v případě závažných obav nebo incidentů. Audity budou prováděny po předchozím oznámení s předstihem nejméně 30 dnů, ledaže neoprávněný přístup nebo jiné bezpečnostní hrozby vyžadují bezodkladné jednání.
- 3.3.3 Audit může zahrnovat fyzickou inspekci Zařízení, přehledy bezpečnostních protokolů, analýzu správy Dat a přístupových práv a kontrolu dodržování relevantních právních a smluvních požadavků. Zadavatel má právo požadovat od Dodavatele veškerou relevantní dokumentaci a záznamy související s auditovanými oblastmi.
- 3.3.4 V případě zjištění nedostatků během auditu je Dodavatel povinen tyto nedostatky odstranit do stanovené lhůty, obvykle do 30 dnů od doručení zprávy o auditu. Zadavatel má právo požadovat nápravné opatření nebo přijmout další kroky, včetně uplatnění smluvních sankcí, v závislosti na závažnosti zjištěných nedostatků.

3.4 Řízení subdodavatelů

- 3.4.1 Dodavatel je povinen zajistit, že jakýkoli jeho subdodavatel, který bude mít jakýmkoli způsobem přístup k Datům nebo do Interní sítě, bude dodržovat veškeré povinnosti a standardy, které vyplývají pro Dodavatele na základě této přílohy.

3.5 Informační povinnost Dodavatele

- 3.5.1 Dodavatel je povinen předložit Zadavateli kopii Interního bezpečnostního řádu podle článku 3.1.2 této přílohy na vyžádání Zadavatele.

3.5.2 Dodavatel je povinen bezodkladně informovat Zadavatele o jakýchkoli bezpečnostních incidentech, které mohou mít vliv nebo se přímo týkají Interní sítě nebo Dat.

3.5.3 Dodavatel je povinen neprodleně informovat Zadavatele o jakémkoli ukončení pracovního poměru nebo změně ve statutu zaměstnance, který měl přístup k VPN nebo jiným systémům Zadavatele. Zadavatel zajistí odebrání přístupů tohoto zaměstnance k systémům a do Interní sítě. Dodavatel je povinen zajistit znepřístupnění, zabezpečení a ochranu Dat, ke kterým měl zaměstnanec přístup.

3.6 Pravidla pro likvidaci Dat

3.6.1 Dodavatel se zavazuje neprodleně předat Zadavateli veškerá Data, která již nejsou potřeba pro poskytování služeb. Případné kopie všech těchto dat je Dodavatel povinen odstranit.

3.6.2 Dodavatel je povinen zajistit odstranění Dat takovým způsobem, který zabraňuje možnosti obnovy nebo zneužití.

4 PRAVIDLA PRO VZDÁLENÝ PŘÍSTUP DODAVATELE PROSTŘEDNICTVÍM VPN

4.1 Dodavatel je povinen využívat vzdálený přístup VPN pouze pro účely plnění svých závazků dle Smlouvy a v rozsahu nezbytném pro plnění svých závazků dle Smlouvy.

4.2 Dodavatel není oprávněn bez předchozího písemného souhlasu Zadavatele jakýmkoli způsobem využívat Interní síť pro jiné účely než pro účely plnění svých závazků dle Smlouvy nebo v jiném rozsahu než v rozsahu nezbytném pro plnění svých závazků dle Smlouvy.

5 ZÁVĚREČNÁ USTANOVENÍ

5.1 Jakékoli porušení práv a povinností vyplývajících z této přílohy představuje též závažné porušení Smlouvy.

5.2 Pokud se ukáže některé ustanovení této přílohy neplatné, neúčinné nebo nevymahatelné, zbývající části zůstávají v platnosti. Ohledně neplatného, neúčinného nebo nevymahatelného ustanovení se Smluvní strany zavazují, že je buď dodatkem upraví tak, aby byla zajištěna jeho platnost, účinnost a vymahatelnost, a to při co největším zachování původních záměrů smluvních stran nebo, pokud to není možné, budou vykládat toto ustanovení způsobem, jako by neplatná, neúčinná nebo nevymahatelná část nebyla nikdy v této příloze obsažena.