Smlouva
o dodávce, implementaci a údržbě systému ochrany koncových zařízení (EPP/EDR)

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“) a zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „autorský zákon“),

mezi:

Českou národní bankou

Na Příkopě 28
115 03 Praha 1
zastoupenou: Ing. Milanem Zirnsákem, ředitelem sekce informatiky
a
Ing. Zdeňkem Viriusem, ředitelem sekce správní
IČO: 48136450
DIČ: CZ48136450

(dále jen „zadavatel“ nebo také „ČNB“)

a

T-Mobile Czech Republic a.s.

se sídlem: Tomíčkova 2144/1
148 00 Praha 4
zastoupenou/jednající: Danielem Štefanem, na základě pověření
IČO: 64949681
DIČ: CZ64949681
bankovní spojení/číslo účtu: Komerční banka, a.s, č.ú.: 19-2271190247/0100

(dále jen „dodavatel“)

Preambule

ČNB provozuje systémy ABO, CERTIS a SKD náležející mezi informační systémy kritické informační infrastruktury a je dále provozovatelem významných informačních systémů DMS, eSpis, ISAI, JERRS a KRZR ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZKB“) a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „VKB“). Vzhledem k důležitosti těchto informačních systémů z pohledu naplňování úkolů a fungování ČNB a rovněž i vzhledem k naplňování požadavků výše uvedených právních předpisů v oblasti kybernetické bezpečnosti stanovuje zadavatel dále uvedené požadavky, lhůty, platební podmínky, smluvní pokuty a další smluvní ujednání, které z této důležitosti vycházejí.

Článek I
Předmět, rozsah a místo plnění

1. Předmětem této smlouvy je povinnost dodavatele dodat a implementovat SW a případně HW komponenty systému ochrany koncových zařízení pro nepřetržitou detekci a následnou automatickou nebo manuální reakci na zjištěné bezpečnostní události vzniklé na těchto zařízeních, a to plně dle specifikace uvedené v příloze č. 2 této smlouvy a dalších podmínek stanovených v této smlouvě, zejména pak v čl. II. Dále ve smlouvě bude tento technologický celek včetně všech nabízených licencí a služeb nazýván jako „dílo“ nebo „systém“. Systém musí být použitelný pro 1 800 klientských zařízení a 160 serverových zařízení, z nichž 100 serverů pracuje v rámci RDS farmy Citrix Virtual Apps and Desktops, která poskytuje virtualizovaný desktop pro 950 uživatelů a 40 serverů pracuje v rámci RDS farmy Citrix Virtual Apps and Desktops (Citrix XenApp), která poskytuje virtualizovaný browser pro 1 250 uživatelů. Zadavatel má ve svém prostředí 1 500 uživatelů.
2. Předmětem této smlouvy je dále závazek dodavatele poskytovat zadavateli provozní podporu díla podle čl. VI této smlouvy, a to ode dne podpisu závěrečného akceptačního protokolu oběma smluvními stranami.
3. V případě dodávky HW se dodavatel zavazuje zajistit, že všechny součásti díla budou nové a nepoužité (maximálně zahořelé z výroby, popř. zapnuté pro ověření funkčnosti) a musí být spolu s poskytnutými programovými prostředky (SW) výrobcem určeny pro evropský trh, pakliže výrobce takové určení provádí. Dodavatel je po dobu účinnosti této smlouvy povinen na požádání zadavateli doložit skutečnost, že HW a SW je určen pro evropský trh, pakliže výrobce takové určení provádí, a to do 5 pracovních dnů ode dne doručení požadavku zadavatele.
4. Dodavatel se zavazuje v rámci realizace díla poskytnout zadavateli nejnovější, stabilní verzi software, která bude výrobcem v době plnění uvedena na trh.
5. Místem plnění budou prostory budov v objektech zadavatele na adrese: Na Příkopě 28, 115 03 Praha 1 a Strojírenská 175/25, 155 21 Praha 17.
6. Předmětem této smlouvy je závazek zadavatele poskytnout dodavateli potřebnou součinnost a zaplatit za poskytnutá plnění ceny dle čl. V této smlouvy.
7. Dodavatel bere na vědomí, že mu nebude umožněn vzdálený přístup k žádné součásti dodaného systému (díla).

Článek II
Průběh plnění

Plnění podle čl. I odst. 1 této smlouvy bude realizováno v jednotlivých etapách, přičemž plnění realizovaná v těchto etapách budou předmětem akceptací podle tohoto článku a článku IV této smlouvy. Realizace jednotlivých etap bude probíhat takto:

1. **Etapa 1** – **Ověření přítomnosti deklarovaných technických vlastností**
   Dodavatel v referenčním prostředí dodavatele prokáže, že nabízený systém obsahuje všechny vlastnosti uvedené v příloze č. 2 této smlouvy.

   Pokud se jedná o vlastnost natolik specifickou, že nebude v možnostech dodavatele prokázat funkčnost v referenčním prostředí [např. prokázání plné funkcionality v RDS (Remote Desktop Services) prostředí Citrix XenApp dle požadavků přílohy č. 2 této smlouvy], dostane dodavatel příležitost nakonfigurovat produkt v testovacím prostředí zadavatele. O tuto možnost požádá dodavatel elektronicky, zasláním e-mailu na adresu pověřené osoby zadavatele, ve kterém zdůvodní, proč není možné danou vlastnost

představit v referenčním prostředí dodavatele. Zadavatel bez zbytečného odkladu požadavek schválí nebo se zdůvodněním zamítne, pokud by důvod žádosti nebyl oprávněný. Pokud dojde k zamítnutí požadavku, má dodavatel 5 pracovních dnů na nalezení alternativního řešení, jak zadavateli přítomnost požadované funkcionality doložit. Pokud v této lhůtě věrohodně nedoloží, že dodané řešení požadovanou vlastnost splňuje, je zadavatel opravněn od smlouvy odstoupit dle čl. XII odst. 5 písm. f) této smlouvy.

V případě schválení žádosti provede dodavatel s pověřenými osobami zadavatele do 10 pracovních dnů nastavení systému tak, aby vyhovoval technickým požadavkům zadavatele, a poté proběhne ověřovací provoz trvající 5 pracovních dnů. Po uplynutí této doby pověřená osoba zadavatele vyhodnotí, zda byl ověřovací provoz úspěšný nebo neúspěšný.

V případě, že ověřovací provoz bude ze strany zadavatele vyhodnocen jako neúspěšný, dodavatel je povinen do 3 pracovních dnů upravit konfiguraci tak, aby mohl být ověřovací provoz v dalším kole vyhodnocený jako úspěšný. Po úpravě konfigurace bude zopakován ověřovací provoz trvající 5 pracovních dnů. Možnost případné dodatečné úpravy konfigurace dostane dodavatel dvakrát, celkem bude mít tedy tři pokusy nastavit nabízené řešení tak, aby odpovídalo požadavkům zadavatele.

Pokud nebude ověřovací provoz ani ve třetí iteraci akceptačního řízení hodnocen jako úspěšný, je zadavatel oprávněn od smlouvy odstoupit dle čl. XII odst. 5 písm. f) této smlouvy.

V případě, že nabízené řešení dle výsledků akceptačního řízení v rámci Etapy 1 splní všechny vlastnosti požadované zadavatelem, resp. případný ověřovací provoz byl zadavatelem vyhodnocen jako úspěšný, vypracuje zadavatel akceptační protokol č. 1 s názvem „Ověření přítomnosti technických požadavků zadavatele“, jehož základem bude příloha č. 2 této smlouvy. Protokol bude podepsán alespoň jednou z pověřených osob obou smluvních stran.

V případě úspěšného dokončení Etapy 1 má dodavatel možnost předat zadavateli bezplatné testovací licence nabízeného produktu tak, aby zadavatel mohl začít produkt testovat na svých zařízeních před zahájením oficiální implementace díla do provozního prostředí zadavatele.

2. **Etapa 2 – Realizační studie**

Dodavatel se podpisem akceptačního protokolu č. 1 zavazuje vypracovat realizační studii, ve které bude uveden podrobný implementační postup a detailní popis cílového stavu dodávaného díla. Realizační studie bude dodavatelem vypracována ve spolupráci s pověřenými osobami zadavatele.

Realizační studie vypracovaná dodavatelem bude obsahovat minimálně:

a) popis architektury systému dodaného díla, včetně požadovaných integrací s dalšími systémy zadavatele. Popis musí obsahovat adresy a doménová jména všech lokálních nebo vzdálených prvků, spolupracujících prvků systému společně s komunikační maticí uvádějící požadovaný komunikační směr a síťový port;

b) podrobný návrh harmonogramu a postupu implementace všech následných Fází díla do prostředí zadavatele (vznikne na základě spolupráce s pracovní skupinou zadavatele), při respektování lhůt dle čl. III odst. 1 písm. c) a d) této smlouvy;

c) rozdělení zařízení určených k ochraně agentních software do skupin dle jejich priority při nasazení;

d) instalační postup na jednotlivé platformy, který musí být aplikovatelný v prostředí zadavatele pomocí zadavateli dostupných nástrojů, vznikne na základě spolupráce s pověřenými osobami zadavatele; zadavatel v této souvislosti poskytne dodavateli veškerou součinnost nezbytnou pro zpracování této části realizační dokumentace;

e) podrobný návrh organizačního zabezpečení implementace ze strany dodavatele;

f) popis nároků na poskytnutí nezbytné organizační a technické součinnosti ze strany zadavatele pro dodávku, instalaci, konfiguraci a implementaci díla do systémového prostředí zadavatele.

Dodavatel se zavazuje předat řádně zpracovanou realizační studii k akceptaci zadavateli ve lhůtě stanovené v čl. III odst. 1 písm. b) této smlouvy. V případě, že dodavatel tuto lhůtu nedodrží, je zadavatel oprávněn od smlouvy odstoupit dle čl. XII odst. 5 písm. f) této smlouvy.

Řádně zpracovanou realizační studii předá dodavatel zadavateli v jednom vyhotovení v elektronické podobě v českém jazyce, ve formátech DOCX nebo PDF.

Pověřená osoba zadavatele provede vyhodnocení kvality dodané realizační studie do 3 pracovních dnů. V případě, že v realizační studii nalezne nedostatky, předá jejich seznam pověřené osobě dodavatele. Dodavatel má lhůtu 5 pracovních dnů na odstranění vad a předání upravené realizační studie pověřeným osobám zadavatele. Poté se celý výše popsaný proces vyhodnocení a případných úprav zopakuje, a to do okamžiku, kdy pověřená osoba zadavatele neshledá, že realizační studie byla zpracována řádně. V případě, že zadavatel realizační studii neakceptuje pro její nedostatky po třetím vyhodnocení kvality, a to v důsledku vad, které dodavatel odpovídajícím způsobem opakovaně nevypořádal, je zadavatel oprávněn od smlouvy odstoupit dle čl. XII odst. 5 písm. f) této smlouvy.

V případě, že zadavatel shledá, že realizační studie je bez vad a kompletní, bude pověřenou osobou zadavatele vypracován akceptační protokol č. 2 s názvem „Akceptace realizační studie“, který bude podepsaný alespoň jednou pověřenou osobou za každou smluvní stranu.

Lhůty uvedené v zadavatelem akceptovaném harmonogramu v realizační studii budou pro dodavatele závazné. Tyto lhůty lze měnit písemnou dohodou pověřených osob smluvních stran (bez povinnosti uzavření dodatku smlouvy). Lhůty však musí být v souladu se lhůtami stanovenými v čl. III odst. 1 písm. c) a d).

3. **Etapa 3 – Kompletní dodávka součástí systému (HW, SW, licence), jejich instalace, konfigurace a implementace v systémovém prostředí zadavatele dle harmonogramu vypracovaného v realizační studii**

V této etapě dojde k postupnému, kompletnímu zprovoznění díla v infrastruktuře zadavatele. Kompletní Etapa 3 v sobě zahrnuje nejméně následující činnosti:

a) v případě dodání HW jeho instalaci a konfiguraci v místech plnění zadavatele;

součástí případné dodávky HW bude minimálně:

- instalace dodaných serverů s kompletním příslušenstvím do racku zadavatele včetně připojení všech potřebných konektorů,

- konfigurace BIOS/UEFI serverů – aktuální stabilní verze doporučovaná výrobcem, včetně optimálního nastavení s ohledem na výkon a provozní power management,
- konfigurace HW komponent serverů, zejména konfigurace lokálně instalovaných SSD disků a síťových rozhraní,
- konfigurace komponent pro vzdálený přístup k serverům z prostředí zadavatele, instalace dodaného operačního systému a potřebných ovladačů HW komponent serveru, včetně případné licence,
- nastavení vzdálených repositářů pro stahování aktualizací SW díla, zdrojů informací o bezpečnostních hrozbách atd.,
- instalace nejnovější stabilní verze potřebného SW,

b) instalaci potřebného SW managementu a řádné zalicencování všech komponent,

c) zřízení a zabezpečení přístupu správců zadavatele do prostředí managementu,

d) přípravu instalačních souborů agentního software na cílové platformy tak, aby odpovídal požadavkům zadavatele v plném rozsahu dle přílohy č. 2 této smlouvy,

e) úpravu konfigurace prostředí managementu a všech zamýšlených koncových zařízení tak, aby odpovídal všem požadavkům zadavatele dle přílohy č. 2 této smlouvy,

f) napojení na Active Directory (AD) zadavatele a manuální import seznamu zařízení mimo AD,

g) finální úpravu definice bezpečnostních politik pro jednotlivé skupiny koncových zařízení dle požadavků zadavatele,

h) po dokončení konfigurace provedení zálohy nastavení díla pro případnou obnovu po havárii díla nebo jeho součásti.

Krok 1

Zprovoznění a zpřístupnění managementu dodaného díla pověřeným zaměstnancům zadavatele. V tomto kroku dojde také k nastavení managementu tak, aby odpovídal všem technickým požadavkům zadavatele podle přílohy č. 2 této smlouvy, včetně definice bezpečnostních politik a požadované integrace s bezpečnostními systémy zadavatele, a to ve lhůtě 10 pracovních dnů od podpisu akceptačního protokolu č. 2.

Po zprovoznění a zpřístupnění managementu provede zadavatel vyhodnocení nastavení díla. V případě, že je zadavatelem identifikovaný vážný nedostatek systému, tj. nedostatek bránící užívání díla, mající vliv na stabilitu chráněného systému nebo spočívající v selhání ochranných funkcí, dodavatel je povinen do 5 pracovní dnů upravit nastavení systému tak, aby dílo mohlo být použitelné v souladu s požadavky stanovenými v této smlouvě. V případě potřeby poskytnou pověřené osoby zadavatele k tomu nezbytnou součinnost. Možnost případného dodatečného nastavení systému dostane dodavatel dvakrát, tudíž má ve výsledku 3 pokusy na nastavení díla tak, aby odpovídalo požadavkům stanoveným v této smlouvě.

V případě, že dodavatel není schopný vážné nedostatky odstranit, je zadavatel oprávněn od smlouvy odstoupit dle čl. XII odst. 5 písm. f) a požadovat po dodavateli smluvní pokutu dle čl. X odst. 7.

V případě, že je pověřenou osobou zadavatele identifikovaný drobný (jiný než vážný) nedostatek systému, vyzve e-mailovou zprávou pověřené osoby dodavatele k provedení opravy tohoto nedostatku, a to do 10 pracovních dnů ode dne doručení této výzvy.

V případě, že ze strany dodavatele nedojde k odstranění tohoto nedostatku v uvedené lhůtě, je zadavatel oprávněn požadovat po dodavateli smluvní pokutu dle čl. X odst. 11 za každý pracovní den prodlení.

V případě, že je dílo nastaveno tak, že odpovídá požadavkům stanoveným v této smlouvě, s výjimkou drobných vad, potvrdí pověřená osoba zadavatele pověřené osobě dodavatele e-mailovou zprávou akceptaci Kroku 1. Toto potvrzení zároveň slouží jako pokyn pro přechod ke Kroku 2.

Krok 2

Zařízení zadavatele určená k ochraně prostřednictvím agentního software budou rozdělena do 3 skupin. Členství konkrétních zařízení v příslušné skupině bude určeno v realizační studii (Etapa 2), a to na základě podkladů zadavatele, na základě nichž bude dodavatelem vypracován časový harmonogram nasazení agentního software na konkrétní skupinu zařízení.

Nestanoví-li realizační studie po dohodě smluvních stran jinak:

Skupina 1 bude obsahovat 25 zařízení - jedná se o testovací skupinu pro prvotní nasazení systému do produkčního prostředí zadavatele.

Skupina 2 bude obsahovat 200 zařízení - jedná se o rozšířenou testovací skupinu před kompletním nasazením systému do produkčního prostředí zadavatele.

Skupina 3 bude obsahovat všechna ostatní zamýšlená zařízení, až do výše poptávaných licencí.

Postup pro všechny skupiny bude probíhat podle popisu níže.

Správci zadavatele nainstalují agentní software na všechna zařízení spadající do konkrétní skupiny zmíněné výše, a to dle postupu navrženého dodavatelem v realizační studii. V případě nefunkčnosti, nemožnosti připojení k managementu, problémům s kompatibilitou, nutnosti definice výjimek nebo jiného problému s provozem agentního software na koncovém zařízení zadavatele zajistí dodavatel odstranění vzniklého problému vlastními silami. Po úspěšném zprovoznění na všech zařízeních příslušné skupiny bude na příslušné bezpečnostní politice nastaven detekční režim pro všechny funkcionality požadované zadavatelem dle přílohy č. 2 této smlouvy a zahájí se ověřovací provoz. V případě částí plnění týkajících se zařízení Skupiny 1 a poté i Skupiny 2 budou ověřovací provozy v každém případě probíhat po dobu 10 pracovních dnů. V případě plnění týkajícího se zařízení Skupiny 3 bude ověřovací provoz probíhat po dobu 15 pracovních dnů. Cílem ověřovacích provozů bude ověřit stabilitu a provozní spolehlivost díla.

Po ukončení příslušného ověřovacího provozu provede zadavatel vždy jeho vyhodnocení. V případě, že je v rámci ověřovacího provozu zadavatelem identifikovaný vážný nedostatek systému, dodavatel je povinen do 5 pracovních dnů upravit nastavení systému tak, aby dílo mohlo být v souladu s požadavky stanovenými v této smlouvě, v případě potřeby k tomu pověřené osoby zadavatele poskytnou nezbytnou součinnost. Poté bude zopakován ověřovací provoz v rozsahu 10 (v případě Skupiny 3 v rozsahu 15) pracovních dnů. Možnost dodatečného nastavení systému dostane dodavatel dvakrát, tudíž má ve výsledku 3 pokusy na nastavení díla tak, aby odpovídalo požadavkům stanoveným v této smlouvě. O úspěšném provedení ověřovacího provozu bude vždy vyhotoven protokol podepsaný minimálně jednou pověřenou osobou obou smluvních stran.

V případě, že dodavatel nebude schopný vážné nedostatky odstranit, je zadavatel oprávněn

od smlouvy odstoupit dle čl. XII odst. 5 písm. f) a požadovat po dodavateli smluvní pokutu dle čl. X odst. 7.

V případě, že je zadavatelem identifikovaný drobný nedostatek systému, vyzve dodavatele k provedení opravy tohoto nedostatku, a to do 10 pracovních dnů ode dne doručení této výzvy. V případě, že ze strany dodavatele nedojde k odstranění tohoto nedostatku v uvedené lhůtě, je zadavatel oprávněn požadovat po dodavateli smluvní pokutu dle čl. X odst. 11 za každý pracovní den prodlení.

Pokud zadavatel v rámci ověřovacího provozu konkrétního kroku neidentifikuje vážný nedostatek, bude pověřenou osobou zadavatele potvrzeno úspěšné ukončení implementace pro tuto skupinu zařízení prostřednictvím e-mailové zprávy pověřeným osobám dodavatele.

Toto potvrzení bude zároveň sloužit jako pokyn ke změně režimu této skupiny z Detekce na Protekce u všech funkcionalit a přechod k dalšímu Kroku této Etapy, a to podle harmonogramu vypracovaného v realizační studii.

Ověřovací provoz pro další skupinu zařízení bude vždy kumulovat i všechny předchozí skupiny zařízení, kde bude vzhledem ke změně režimu z Detekce na Protekce potřeba znovu ověřit bezproblémový provoz na koncových zařízeních zadavatele po této změně.

Krok 3

V případě úspěšného provedení všech ověřovacích provozů v Kroku 2 vypracuje pověřená osoba zadavatele akceptační protokol č. 3 s názvem „Implementace díla do provozního prostředí“. Tento protokol podepíše alespoň jedna pověřená osoba za každou smluvní stranu.

4. **Etapa 4 – ověřovací provoz celého díla, zaškolení správců a analytiků zadavatele, tvorba dokumentace**

Po dobu 20 pracovních dnů od podpisu akceptačního protokolu č. 3 bude bez přerušení probíhat ověřovací provoz v režimu standardního pracovního provozu zadavatele. Cílem je ověřit v delším časovém horizontu stabilitu a provozní spolehlivost celého díla.

Po ukončení ověřovacího provozu provede zadavatel jeho vyhodnocení.

V případě, že bude v rámci ověřovacího provozu zadavatelem identifikovaný vážný nedostatek systému, je dodavatel povinen do 5 pracovních dnů upravit konfiguraci díla tak, aby dílo nevykazovalo žádné nedostatky, v případě potřeby k tomu pověřené osoby zadavatele poskytnou nezbytnou součinnost. Poté bude zopakován ověřovací provoz v rozsahu 20 pracovních dnů. Možnost dodatečného nastavení systému dostane dodavatel dvakrát, tudíž má ve výsledku 3 pokusy na nastavení a vyladění systému tak, aby odpovídal požadavkům stanoveným v této smlouvě.

V případě, že dodavatel nebude schopný zjištěný nedostatek nebo nedostatky odstranit, je zadavatel oprávněn od smlouvy odstoupit dle čl. XII odst. 5 písm. f) a požadovat po dodavateli smluvní pokutu dle čl. X odst. 7.

V případě, že je zadavatelem identifikovaný drobný nedostatek systému, vyzve dodavatele k provedení opravy tohoto nedostatku, a to do 10 pracovních dnů ode dne doručení této výzvy. V případě, že ze strany dodavatele nedojde k odstranění tohoto nedostatku v uvedené lhůtě, je zadavatel oprávněn požadovat po dodavateli smluvní pokutu dle čl. X odst. 11 za každý pracovní den prodlení.

Za funkční dílo považuje zadavatel stav, kdy byl úspěšně dokončen ověřovací provoz díla jako celku v rámci Etapy 4 a kdy dílo splňuje všechny technické požadavky zadavatele dle přílohy č. 2 této smlouvy. O úspěšném provedení ověřovacího provozu celého díla bude vyhotoven protokol podepsaný minimálně jednou pověřenou osobou obou smluvních stran.

V Etapě 4 je dodavatel dále povinen provést zaškolení správců a analytiků zadavatele, a to nejpozději do 10 pracovních dnů od úspěšného ukončení ověřovacího provozu v takovém rozsahu, aby byli schopni systém samostatně spravovat a využít dostupné informace k vyšetřování bezpečnostních událostí.

Zaškolení správců a analytiků zadavatele bude provedeno v rozsahu umožňujícím provádět minimálně:

- běžný rutinní provoz a údržbu dodávaného díla,
- řešení obvyklých problémů,
- správu uživatelských účtů a oprávnění,
- monitoring stavu dodaného díla,
- zálohování a obnovu konfigurace,
- tvorbu vlastních pohledů, reportů, dashboardů apod.,
- investigaci, vyhodnocování a reakci na bezpečnostní události.

Dodavatel je dále povinen zadavateli do 10 pracovních dnů od úspěšného ukončení ověřovacího provozu zaslat dokumentaci skutečného stavu díla, a to v elektronické podobě, ve formátech DOCX nebo PDF, zahrnující minimálně:

- popis funkčního schématu dodaného díla, včetně zapojení a konfigurace prvků, seznam kompletních komunikačních matic vzdálených i lokálních cílů,
- postup implementace díla do prostředí zadavatele,
- postupy pravidelné údržby díla,
- postupy diagnostiky a monitorování stavu díla,
- postupy řešení havarijních stavů celého díla,
- postupy zálohování, archivace a obnovy konfigurace systému díla a dat.

Po úspěšném ukončení ověřovacího provozu, zaškolení pracovníků a zaslání dokumentace skutečného stavu díla v rámci Etapy 4 bude zadavatelem sepsán závěrečný akceptační protokol, který bude podepsán alespoň jednou pověřenou osobou za každou smluvní stranu. Na základě tohoto protokolu bude dílo zadavateli předáno.

Článek III
Lhůty plnění, součinnost, pověřené osoby

1. Dodavatel se zavazuje ukončit jednotlivé etapy díla a dílo předat zadavateli v následujících lhůtách:

   a) plnění v rámci Etapy 1 dle čl. II odst. 1 této smlouvy je dodavatel povinen ukončit **nejpozději do 10 pracovních dnů** ode dne účinnosti této smlouvy;

   b) plnění v rámci Etapy 2 dle čl. II odst. 2 této smlouvy je dodavatel povinen ukončit **nejpozději do 20 pracovních dnů** ode dne podpisu akceptačního protokolu Etapy 1;

   c) plnění v rámci Etapy 3 dle čl. II odst. 3 této smlouvy je dodavatel povinen ukončit nejpozději **do 90 pracovních dnů** ode dne podpisu akceptačního protokolu Etapy 2;

d) plnění v rámci Etapy 4 dle čl. II odst. 4 této smlouvy je dodavatel povinen ukončit a předat dílo zadavateli v souladu s čl. IV odst. 4 této smlouvy nejpozději **do 30 pracovních dnů** ode dne podpisu akceptačního protokolu Etapy 3.

V případě, že v průběhu plnění v rámci jednotlivých etap dojde v případech výslovně uvedených v čl. II k potřebě úprav systému, opakovaného provedení ověřovacích provozů, nalezení alternativních řešení apod., a v důsledku toho ke stanovení dodatečné lhůty pro nápravu v rozsahu uvedeném v příslušném ustanovení, lhůta pro ukončení příslušné etapy stanovená v čl. III odst. 1 se o tuto lhůtu automaticky prodlužuje (tj. bez povinnosti uzavření dodatku).

2. Lhůtu(y) uvedenou(é) v čl. III odst. 1 je dále oprávněna kterákoliv z pověřených osob zadavatele, na písemnou a odůvodněnou žádost dodavatele, přiměřeně okolnostem prodloužit, pokud dodavatel objektivně nemohl pokračovat v plnění dle této smlouvy z důvodu, že mu zadavatel neposkytl povinnou a nezbytnou součinnost, nebo z důvodu skutečností stojících na straně dodavatele, které ani dodavatel jednající s náležitou péčí nemohl předvídat a které sám nezpůsobil (včetně např. výpadku či zdržení v dodavatelsko-odběratelském řetězci, výpadku v pracovní síle dodavatele z důvodu opatření uložených orgány veřejné moci, nikoli v důsledku protiprávního jednání dodavatele, zdržení v plnění jiných smluvních partnerů zadavatele, které se plnění dle této smlouvy dotýká a které nebylo způsobeno zadavatelem). Písemná žádost dodavatele musí obsahovat i návrh prodloužení lhůt(y), ten však není pro pověřené osoby zadavatele závazný. Úprava lhůt(y) bude provedena formou dodatku k této smlouvě.

3. Zadavatel se zavazuje vytvořit dodavateli k instalaci a implementaci HW a SW dle této smlouvy potřebné podmínky, zejména:

   a) zajistit přístup odborným pracovníkům dodavatele ke klientskému zařízení, z něhož bude realizována implementace SW,

   b) připravit pro instalaci HW a SW potřebné technické a organizační prostředky (konkrétní požadavky nadefinuje dodavatel v rámci realizační studie).

4. Pověřenými osobami jsou:

   a) za zadavatele:

   [redacted]

   b) za dodavatele:

   [redacted]

   V případě změny pověřených osob smluvních stran nebo jejich kontaktních údajů jsou smluvní strany povinny nahlásit změnu následující pracovní den po provedení změny na e-mailové adresy pověřených osob druhé smluvní strany. Změna osob je účinná dnem jejího oznámení druhé smluvní straně, a to bez povinnosti uzavírat dodatek k této smlouvě.

Článek IV
Akceptace díla

1. V případě, že zadavatel v Etapě 1 shledá, že nabízený produkt splňuje všechny technické vlastnosti dle přílohy č. 2 této smlouvy, připraví akceptační protokol č. 1 „Ověření

přítomnosti technických požadavků zadavatele“, který svým podpisem potvrdí pověřené osoby obou smluvních stran. V případě, že zadavatel odmítne z důvodu nesplnění výše zmíněných technických vlastností plnění v rámci Etapy 1 akceptovat, vyhrazuje si právo na odstoupení od smlouvy dle čl. XII odst. 5 písm. f).

2. Poté, co dodavatel vypracuje v rámci Etapy 2 realizační studii dle čl. II odst. 2 této smlouvy, provede pověřená osoba zadavatele do 3 pracovních dnů její vyhodnocení. V případě, že bude zpracována řádně, vypracuje pověřená osoba zadavatele akceptační protokol č. 2 „Akceptace realizační studie“, který bude podepsán pověřenými osobami obou smluvních stran.

   Zadavatel realizační studii akceptuje, pokud bude obsahovat všechny náležitosti stanovené v čl. II odst. 2 této smlouvy a návrh implementace díla popsaný v realizační studii bude splňovat všechny podmínky stanovené v této smlouvě, včetně požadavků stanovených v přílohách č. 1 a 2 této smlouvy.

   Do okamžiku akceptace Etapy 2 je zadavatel oprávněn od smlouvy kdykoliv odstoupit uhrazením odstupného v souladu s čl. XII odst. 11 této smlouvy.

3. Po dokončení implementace v rámci Kroku 1 a Kroku 2 v Etapě 3 podle čl. II odst. 3 této smlouvy předloží dodavatel zadavateli k akceptaci implementaci díla (Krok 3). Akceptační řízení bude zadavatelem provedeno do 3 pracovních dnů od předložení Etapy 3 díla k akceptaci. V případě akceptace Etapy 3 bude zadavatelem sepsán akceptační protokol č. 3 s názvem „Implementace díla do provozního prostředí“, který bude podepsán pověřenými osobami obou smluvních stran.

4. Po úspěšném ukončení ověřovacího provozu, provedení zaškolení pracovníků zadavatele a zaslání dokumentace skutečného stavu díla dle článku II. odst. 4 v rámci Etapy 4 bude zadavatelem sepsán závěrečný akceptační protokol, který bude podepsán pověřenými osobami obou smluvních stran. Na základě tohoto protokolu bude dílo zadavateli předáno.

5. Zadavatel převezme dílo pouze tehdy, pokud:

   a) dodavatel dodal, nainstaloval a implementoval veškeré HW (v případě, že řešení dodavatele zahrnuje jeho dodání) a SW komponenty včetně jejich konfigurace;

   b) byly splněny veškeré požadavky zadavatele uvedené v příloze č. 2 této smlouvy;

   c) dodavatel řádně zajistil licence všech součástí díla;

   d) dodavatel odstranil veškeré nedostatky, které mu zadavatel ohlásil v rámci všech předchozích etap a nedostatky zjištěné v průběhu Etapy 4, s výjimkou drobných nedostatků;

   e) dodavatel provedl dílo v souladu s akceptovanou realizační studií, nebylo-li smluvními stranami dohodnuto jinak;

   f) dodavatel zaškolil pracovníky zadavatele dle požadavků stanovených v čl. II odst. 4;

   g) dodavatel předal zadavateli kompletní dokumentaci skutečného stavu díla.

6. Dodavatel plně odpovídá za to, že dodané dílo bude plně funkční a schopno použití v prostředí zadavatele.

Článek V
Cena plnění a platební podmínky

1. Cena za instalaci a implementaci díla podle čl. I odst. 1 je stanovena jednorázově a činí celkem **670 000 Kč bez DPH**. Cena za zaškolení činí navíc **105 000 Kč bez DPH.**

2. Cena za dodávku programových prostředků, včetně licencí pro 1 800 klientských zařízení, 160 serverových zařízení [včetně licencí pro sessiony virtualizovaných desktopů pro 950 uživatelů a licencí pro sessiony virtualizovaných browserů pro 1 250 uživatelů v rámci provozních RDS farem Citrix Virtual Apps and Desktops (Citrix XenAPP), pokud jsou licencovány samostatně], případně licencí pro 1 500 uživatelů, dle specifikace uvedené v příloze č. 2 této smlouvy, činí **1 826 880 Kč bez DPH ročně**.
3. Cena za podporu SW výrobcem podle čl. VI odst. 1 písm. b) a podporu dle písm. d) této smlouvy je stanovena paušálně a činí ročně **120 000 Kč bez DPH.**
4. Cena za podporu dodavatele v místě plnění pro 1. rok provozu dle čl. VI odst. 1 písm. c) této smlouvy v rozsahu 12 MD ročně je stanovena paušálně a činí **209 400** K**č bez DPH.**
5. Cena za podporu dodavatele v místě plnění pro 2. a další následující roky provozu dle čl. VI odst. 1 písm. c) této smlouvy v rozsahu 6 MD ročně je stanovena paušálně a činí ročně **104 700 Kč bez DPH.**
6. Cena za podporu dodavatele v místě plnění dle čl. VI odst. 1 písm. c) této smlouvy nad limit stanovený v odst. 4 nebo 5 tohoto článku bude stanovena jako součin počtu skutečně odpracovaných hodin a hodinové sazby, která činí **2 200 Kč bez DPH.**
7. K cenám uvedeným v odstavcích 1 až 6 tohoto článku bude účtována DPH v sazbě platné v den uskutečnění zdanitelného plnění. Ceny zahrnují veškeré náklady dodavatele spojené s plněním podle této smlouvy (včetně nákladů na náhradní díly HW dodávaných v rámci podpory, dopravy a ztráty času techniků na cestě).
8. Dodavatel může vystavit 1. zálohovou fakturu na základě reálně spotřebovaného počtu licencí po úspěšném ukončení ověřovacího provozu týkající se Skupiny 1 v rámci Kroku 2 Etapy 3. Výše zálohy bude odpovídat ceně použitých licencí a bude odpovídat částce za 1 rok provozu těchto licencí.
9. Dodavatel může vystavit 2. zálohovou fakturu na základě reálně spotřebovaného počtu licencí po úspěšném ukončení ověřovacího provozu týkající se Skupiny 2 v rámci Kroku 3 Etapy 3 zadavatelem. Výše zálohy bude odpovídat ceně použitých licencí a bude odpovídat částce za 1 rok provozu těchto licencí.
10. Dodavatel může vystavit 3. zálohovou fakturu na základě reálně spotřebovaného počtu licencí po úspěšném ukončení ověřovacího provozu týkající se Skupiny 3 v rámci Kroku 4 Etapy 3 zadavatelem. Výše zálohy bude odpovídat ceně použitých licencí a bude odpovídat částce za 1 rok provozu těchto licencí.
11. Daňový doklad na cenu díla, resp. plnění podle odstavce 1 a cenu licencí za 1 rok provozu dle odstavce 2 tohoto článku, je dodavatel oprávněn vystavit po podpisu závěrečného akceptačního protokolu zadavatelem, přičemž v tomto daňovém dokladu bude odečtena výše záloh poskytnutých dle odstavce 8–10 tohoto článku.
12. Úhrada paušálních cen licencí pro další roční období dle odstavce 2 tohoto článku bude zadavatelem hrazena vždy na základě daňového dokladu vystaveného dodavatelem nejdříve 14 dnů před ukončením platnosti předplacených licencí z předešlého období.
13. Úhrada paušálních cen podpory dle odstavce 2–5 tohoto článku bude zadavatelem hrazena předem následovně:
    a) první daňový doklad je dodavatel oprávněn vystavit po podpisu závěrečného akceptačního protokolu pověřenými osobami obou smluvních stran dle čl. IV odst. 4, a to za celý první rok poskytování podpory;
    b) další daňové doklady je dodavatel oprávněn vystavit vždy nejdříve 14 dnů

před koncem předplacené doby podpory z předešlého období.

14. Cena za podporu na místě dle odst. 6 tohoto článku nad limit stanovený v odst. 4 a 5 tohoto článku bude zadavatelem hrazena na základě daňového dokladu vystaveného dodavatelem nejdříve poslední den uplynulého kalendářního měsíce, ve kterém bylo příslušné plnění řádně poskytnuto. Kopie výkazu práce dle čl. VI odst. 12 podepsaného zadavatelem bude tvořit nedílnou přílohu daňového dokladu.

15. Doklad k úhradě (fakturu) zašle dodavatel elektronicky jako přílohu e-mailové zprávy na adresu faktury@cnb.cz ve formátu ISDOC. Pokud není možné vytvořit doklad ve formátu ISDOC, je možné zasílat jej ve formátu PDF. V jedné e-mailové zprávě smí být pouze jeden doklad k úhradě. Mimo vlastní doklad k úhradě může být přílohou e-mailové zprávy jedna až sedm příloh k dokladu ve formátech PDF, DOC, DOCX, XLS, XLSX. Přijaty budou i doklady k úhradě v jiném formátu, který bude v souladu s evropským standardem elektronické faktury. Nebude-li možné zaslat doklad k úhradě elektronicky, zašle jej dodavatel v analogové formě na adresu:

    Česká národní banka
    sekce rozpočtu a účetnictví
    odbor účetnictví
    Na Příkopě 28
    115 03 Praha 1

16. Doklad k úhradě bude obsahovat údaje podle § 435 občanského zákoníku a bankovní účet, na který má být placeno a který je uveden v záhlaví této smlouvy nebo který byl později aktualizován dodavatelem (dále jen „určený účet“). Daňový doklad bude nadto obsahovat náležitosti stanovené v zákoně o dani z přidané hodnoty. Nezbytnou náležitostí každého dokladu je také číslo této smlouvy (ve formátu ISDOC v poli ID ve skupině Contract References), nebo číslo objednávky (ve formátu ISDOC v poli External_Order_ID ve skupině OrderReference), jsou-li objednávky v rámci smlouvy vystavovány. Pokud doklad bude postrádat některou ze stanovených náležitostí nebo bude obsahovat chybné údaje, je zadavatel oprávněn jej vrátit dodavateli, a to až do lhůty splatnosti. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného dokladu.

17. V případě, že bude v dokladu k úhradě uveden jiný než určený účet, je pověřená osoba dodavatele povinna na základě výzvy zadavatele sdělit na e-mailovou adresu, ze které byla výzva odeslána, zda má být zaplaceno na bankovní účet uvedený v dokladu, nebo na určený účet. V tomto případě se doklad k úhradě nevrací s tím, že lhůta splatnosti začíná běžet až dnem doručení sdělení dodavatele podle předchozí věty.

18. Splatnost daňového dokladu je 14 dnů od doručení zadavateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu zadavatele ve prospěch účtu dodavatele.

19. Smluvní strany se dohodly, že zadavatel je oprávněn započíst jakoukoli svou peněžitou pohledávku za dodavatelem, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce dodavatele za zadavatelem, ať splatné či nesplatné.

20. Dodavatel je oprávněn navrhnout změnu paušální ceny licencí dle odst. 2 tohoto článku v návaznosti na vývoj indexu cen tržních služeb, stejné období předchozího roku = 100, konkrétně index „J62“ – „Služby v oblasti programování a poradenství a související služby“, sloupec „Průměr od počátku roku“, a to průměr za předchozí kalendářní rok, který vyhlašuje Český statistický úřad. Ceny mohou být zvýšeny maximálně o částku odpovídající předmětné roční inflaci. Úprava ceny bude provedena formou dodatku ke smlouvě. První úpravu cen může dodavatel navrhnout nejdříve po ukončení platnosti

licencí třetího ročního období, a to za účelem navýšení paušální ceny pro následující roční období.

21. Dodavatel je oprávněn navrhnout změnu paušálních cen podpory dle odst. 3 a 5 tohoto článku či hodinové sazby za podporu dle odst. 6 tohoto článku v návaznosti na vývoj indexu cen tržních služeb, stejné období předchozího roku = 100, konkrétně index „J62" – „Služby v oblasti programování a poradenství a související služby", sloupec „Průměr od počátku roku", a to průměr za předchozí kalendářní rok, který vyhlašuje Český statistický úřad. Ceny mohou být zvýšeny maximálně o částku odpovídající předmětné roční inflaci. Úprava ceny bude provedena formou dodatku ke smlouvě. První úpravu cen může dodavatel navrhnout nejdříve 1 měsíc před uplynutím 1. roku od zahájení podpory dle čl. I odst. 2 této smlouvy.

Článek VI
Podpora

1. Podpora díla dle čl. I odst. 2 této smlouvy zahrnuje:
   a) odstraňování jakýchkoliv vad dodaného HW, pokud byl dodaný jako součást díla,
   b) poskytování veškerých aktualizací dodaného SW (nové verze, opravné verze, bezpečnostní záplaty),
   c) podporu dodavatelem v místě plnění, která bude spočívat zejména v následujících činnostech:
      - řešení/odstraňování závad, poruch nebo /problémů dodaného SW pro koncová zařízení nebo managementu a HW prostředků díla,
      - implementace aktualizací dodaného SW pro koncová zařízení nebo management díla,
      - konzultace v místě plnění, zejména k problematice úpravy konfigurace chráněných zařízení, včetně doporučení k optimalizaci využití zdrojů chráněných zařízení, zvýšení bezpečnosti díla, interpretaci analytických výstupů apod.,
   d) podporu výrobce, nejméně formou e-mailové komunikace. Zaručuje pověřeným osobám zadavatele možnost zadávat servisní požadavky prostřednictvím ServiceDesku výrobce. Přijetí požadavku výrobcem je vždy potvrzeno zasláním e-mailu na adresu jedné nebo více pověřených osob zadavatele. Přístup do systému výrobce zprostředkuje pověřeným osobám zadavatele dodavatel. Požadavek na dostupnost podpory výrobce je minimálně v režimu 8x5/NBD.
2. Dodavatel je povinen reagovat a odstranit každou takto oznámenou vadu podle její priority do doby uvedené v tabulce:

Kategorie	Reakční doba	Doba do finálního vyřešení (odstranění) vady
Priorita 1	2 pracovní hodiny	8 pracovních hodin od ohlášení
Priorita 2	2 pracovní hodiny	48 pracovních hodin od ohlášení
Priorita 3	2 pracovní hodiny	72 pracovních hodin od ohlášení
Priorita 4	2 pracovní hodiny	Příští update SW (agent i management)

O zařazení vady do příslušné kategorie rozhoduje zadavatel, resp. pověřená osoba zadavatele. Pracovní hodinou se rozumí hodina spadající pod pracovní dobu zadavatele (7:45 – 16:00 hod.).

3. Vady kategorizované jako Priorita 1 se týkají kritického selhání díla. Spadají sem události jako nedostupný management díla (HW i SW poruchy), nefunkční agentní software na více než 100 koncových zařízeních a jiné závažné poruchy, které znemožňují zadavateli plnohodnotně využívat funkcionalitu díla a mají kritický dopad na bezpečnost prostředí nebo kontinuitu činností zadavatele.
4. Vady kategorizované jako Priorita 2 se týkají závažného selhání díla, kdy např. není možné použít část funkcionality managementu díla, agentní software není plně funkční na 50–100 koncových zařízeních, případně jiná forma poruchy, která má závažný dopad na bezpečnost prostředí nebo kontinuitu činností zadavatele.
5. Vady kategorizované jako Priorita 3 se týkají méně závažného selhání díla, kdy např. agentní software není funkční na 1–49 koncových zařízeních, nebo jiná forma poruchy, která má mírný dopad na bezpečnost prostředí nebo kontinuitu činností zadavatele.
6. Vady kategorizované jako Priorita 4 se týkají drobného selhání díla, primárně se jedná o události, které nemají žádný dopad na bezpečnost prostředí zadavatele a jejich řešení nevyžaduje okamžitou akci dodavatele. Přípustné je řešení formou softwarové záplaty vydané výrobcem v rámci standardního procesu vývoje nové verze.
7. Potřebu podpory na místě ohlašuje pověřená osoba zadavatele dodavateli v pracovní době zadavatele (7:45 – 16:00 hod.) telefonicky na telefonní číslo dodavatele 236 099 009 s následným písemným potvrzením na e-mailovou adresu dodavatele soc@t-mobile.cz nebo pouze e-mailem na výše uvedenou e-mailovou adresu dodavatele. Ohlášení učiněná po pracovní době zadavatele se považují za ohlášení učiněná následující pracovní den, v čase odpovídajícím začátku uvedené pracovní doby zadavatele.
8. Dodavatel je povinen potvrdit přijetí ohlášení vady dle příslušné priority uvedené v odst. 2 tohoto článku smlouvy nejpozději do 2 pracovních hodin od ohlášení, a to na e-mailovou adresu pověřené osoby zadavatele dle čl. III odst. 4 této smlouvy, není-li v této smlouvě stanoveno dále jinak.
9. Dodavatel poskytne zadavateli aktualizace SW dle odst. 1 písm. b) tohoto článku bez zbytečného odkladu, nejpozději však do 14 dnů od uvedení výrobcem na trh, nedohodnou-li se smluvní strany jinak.
10. Dodavatel je povinen nahlásit případnou změnu kontaktních údajů uvedených v odstavci 7 tohoto článku nejpozději následující pracovní den po provedení změny na e-mailové adresy pověřených osob zadavatele. Změna je účinná dnem jejího oznámení druhé smluvní straně, a to bez povinnosti uzavírat dodatek k této smlouvě.
11. Podpora poskytovaná dodavatelem musí vyhovovat technickým specifikacím a požadavkům výrobce dodaných HW a SW prostředků.
12. Konkrétní termín provedení podpory dle čl. VI odst. 1 písm. c) stanoví zadavatel, nedohodnou-li se smluvní strany na konkrétním termínu. Dodavatel vyhotoví o poskytnuté podpoře dle čl. VI odst. 1 písm. c) této smlouvy v daném měsíci výkaz práce, který bude obsahovat tyto údaje:
    a) evidenční číslo požadavku,
    b) stručná specifikace požadavku,
    c) způsob vyřízení požadavku,

d) datum vyřízení požadavku,
e) celkový počet hodin/člověkodní provedené práce.

Správnost údajů uvedených ve výkazu práce bude potvrzena podpisem kterékoliv z pověřených osob za zadavatele.

Článek VII
Licenční ujednání

1. Dodavatel poskytuje po dobu trvání této smlouvy zadavateli nevýhradní, nepřevoditelné, nedělitelné a teritoriálně neomezené oprávnění k výkonu práva užívat programové prostředky dodané dle této smlouvy a dle účelu této smlouvy. Právo užívání programových prostředků přechází na zadavatele dnem jejich instalace/implementace v místě plnění a předáním účtu správce vzdáleného management tenantu zadavatele.
2. Dále dodavatel poskytuje zadavateli nevýhradní, časově a místně neomezené oprávnění užívat realizační studii a dokumentaci skutečného stavu dodané dle této smlouvy, a to i v podobě jakýchkoliv jejich návrhů, ke všem způsobům užití, zejména, avšak nikoliv výlučně, ke způsobům užití podle § 12 odst. 4 autorského zákona, kdy tato práva nabude zadavatel okamžikem jejich poskytnutí dodavatelem. Součástí této licence je i souhlas se zveřejněním (sdělováním veřejnosti) studie či dokumentace, a to i dálkově a hromadně účinným způsobem s tím, že poskytnutím studie či dokumentace zadavateli se zadavatel současně stává vlastníkem médií, na kterých jsou zachyceny. Zadavatel může jakékoli oprávnění tvořící součást zde uvedeného oprávnění zcela nebo zčásti poskytnout třetí osobě, a to i bezúplatně. Zadavatel je oprávněn sám nebo prostřednictvím třetí osoby studii nebo dokumentaci nebo jejich části měnit, upravovat, zpracovávat, spojovat s jiným (autorským) dílem/prvky či zařazovat do (autorského) díla souborného.
3. Zadavatel není povinen využít dle tohoto článku smlouvy poskytnuté licenční oprávnění ani zčásti.
4. Dodavatel prohlašuje, že je právo dle odstavce 1 či 2 tohoto článku smlouvy oprávněn poskytnout a že na něm neváznou žádná práva třetích osob, která by poskytnutí bránila, jinak odpovídá za škodu tím způsobenou.
5. Licence poskytnuté dle této smlouvy se vztahují i na veškeré poskytnuté aktualizace (tj. update/upgrade/patch/hotfix atd.).
6. Odměna za poskytnutí licencí podle této smlouvy je součástí cen podle čl. V této smlouvy.

Článek VIII
Kybernetická bezpečnost a další bezpečnostní požadavky zadavatele

1. Dodavatel se zavazuje zajistit, aby jeho pracovníci či poddodavatelé dodavatele a jejich pracovníci v plném rozsahu dodržovali bezpečnostní požadavky zadavatele, které jsou uvedeny v příloze č. 3 této smlouvy.
2. Dodavatel je v souvislosti s plněním této smlouvy dále povinen postupovat v souladu s obecnými pravidly v oblasti bezpečnosti IT, která tvoří přílohu č. 4 této smlouvy.
3. Dodavatel bere na vědomí, že zadavatel je správcem informačních systémů kritické informační infrastruktury dle ustanovení § 3 písm. c) ZKB a správcem významného/ých informačního/ch systému/ů dle ustanovení § 3 písm. e) ZKB uvedených v preambuli této smlouvy.
4. Dodavatel je při plnění této smlouvy v postavení významného dodavatele ve smyslu § 2 písm. n) a § 8 odst. 1 písm. f) a odst. 2 VKB a bere na vědomí, že po dobu účinnosti této

smlouvy bude veden v evidenci významných dodavatelů zadavatele ve smyslu § 8 odst. 1 písm. b) a c) VKB.

5. Rozsah zapojení dodavatele na zajištění bezpečnosti aktiv informačních systémů kritické informační infrastruktury a aktiv významných informačních systémů používaných v prostředí zadavatele je určen předmětem této smlouvy.
6. Dodavatel je při poskytování plnění oprávněn užívat data předaná mu zadavatelem za účelem plnění předmětu smlouvy či data za tímto účelem získaná pouze v rozsahu nezbytném ke splnění smlouvy a pouze v souladu s touto smlouvou a příslušnými právními předpisy, tj. zejména ZKB a VKB.
7. Dodavatel se zavazuje při výkonu své činnosti včas a prokazatelně upozornit zadavatele na zřejmou nevhodnost jeho příkazů či doporučení vztahujících se k pravidlům bezpečnosti, jejichž následkem může vzniknout újma nebo nesoulad s právními předpisy, a zajistit ve spolupráci se zadavatelem náhradní způsob naplnění pravidel bezpečnosti, pokud stávající řešení přestalo být funkční a efektivní.
8. Dodavatel je srozuměn s tím, že zadavatel provádí v pravidelných intervalech hodnocení rizik v souvislosti s informačním systémem/informačními systémy dle odst. 3 tohoto článku, kterého/ých se týká poskytování plnění dle této smlouvy.
9. Dodavatel se zavazuje informovat zadavatele o tom, jakým způsobem řídí bezpečnostní rizika spojená s plněním předmětu této smlouvy a dále jaká jsou zbytková rizika související s plněním této smlouvy.
10. Dojde-li u dodavatele k výskytu bezpečnostních incidentů, které mohou ovlivnit bezpečnost informací nebo informačních systémů zadavatele, zavazuje se dodavatel o těchto bezpečnostních incidentech bezodkladně informovat zadavatele. Dodavatel se dále zavazuje oznamovat zadavateli bezodkladně neobvyklé chování těchto informačních systémů a podezření na jakékoliv zranitelnosti bezpečnosti informací.
11. Dodavatel se zavazuje informovat zadavatele o významné změně ovládání dodavatele. Ovládáním se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů či ekvivalentní postavení, a to do 5 pracovních dnů od uskutečnění této změny.
12. Dodavatel se zavazuje informovat zadavatele o změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými dodavatelem k plnění této smlouvy, a to do 5 pracovních dnů od uskutečnění této změny.
13. Dodavatel je povinen zajistit, aby byly v případě ukončení smlouvy veškerá data a informace získané či vzniklé v souvislosti s plněním této smlouvy likvidovány bezpečným způsobem, který zaručí, že nebude možné zrekonstruovat jednotlivé datové struktury, části dat a informací do podoby, jež by umožnila identifikovat obsah a zpracování nebo použití dat a/nebo informací na konkrétním nosiči dat. Dodavatel je přitom povinen zajistit soulad postupu při likvidaci dat s přílohou č. 4 VKB.
14. Dojde-li za dobu účinnosti této smlouvy ke změnám ZKB a/nebo VKB takového charakteru a rozsahu, že s nimi nebude smlouva v souladu, zavazují se smluvní strany uzavřít písemný dodatek k této smlouvě, jehož předmětem bude úprava či doplnění práv a povinností smluvních stran nezbytných k nápravě tohoto stavu, a to bez zbytečného odkladu poté, co legislativní změny ZKB a/nebo VKB nabydou platnosti.
15. Dodavatel je povinen na základě informace obsažené v e-mailové zprávě pověřené osoby zadavatele odeslané pověřené osobě dodavatele umožnit zadavateli provést

prostřednictvím zadavatelem určené osoby auditní šetření ve vztahu k dodavatelem dodanému plnění dle čl. I odst. 1, a to v souladu s požadavky dle VKB. Dodavatel je v této souvislosti povinen osobě či osobám provádějícím auditní šetření poskytnout veškerou nezbytnou součinnost k jeho provedení.

16. Dodavatel se zavazuje doložit zadavateli každoročně vždy nejpozději do 30. 9. zprávu nezávislého auditora (např. SOC 2 Type 2 report), která bude obsahovat popis bezpečnostních opatření přijatých výrobcem a jejich stav v předchozím kalendářním roce. Zprávu za rok 2023 dodavatel doloží nejpozději ve lhůtě pro ukončení Etapy 2.
17. Dodavatel se zavazuje bez zbytečného odkladu prostřednictvím pověřených osob hlásit veškeré incidenty vzniklé u výrobce software, který je součástí díla.

Článek IX
Osoby dodavatele poskytující plnění

1. Dodavatel se zavazuje, že plnění dle čl. I bude poskytováno pouze osobami splňujícími kvalifikaci požadovanou v bodu 7.3 písm. b) zadávací dokumentace k veřejné zakázce s názvem „Ochrana klientských stanic“ (dále jen „veřejná zakázka“), na jejímž základě byla uzavřena tato smlouva, tj. že každá z těchto osob je certifikována k instalaci, implementaci a k provádění provozní podpory systému dle této smlouvy, případně splňuje další jiné požadavky stanovené v zadávací dokumentaci. Požadované certifikáty musejí být platné po celou dobu účinnosti této smlouvy. Dodavatel je povinen kdykoliv po dobu účinnosti této smlouvy na výzvu zadavatele tuto skutečnost doložit, a to do 5 pracovních dnů od doručení výzvy.
2. Změna v osobách dle předchozího odstavce, poskytujících plnění, může být provedena pouze se souhlasem zadavatele, a to po splnění kvalifikačních požadavků zadavatele ve stejném rozsahu, jaký byl stanoven v zadávacím řízení veřejné zakázky, nebude-li dohodnuto jinak. Odsouhlasení změny bude provedeno e-mailem alespoň jednou pověřenou osobou zadavatele, bez povinnosti uzavřít dodatek k této smlouvě.
3. Zadavatel si za splnění podmínek dle odstavce 1 tohoto článku vyhrazuje právo požádat o výměnu některé z uvedených osob z důvodu opakované nespokojenosti s kvalitou jí odváděné práce nebo nedostatečnou komunikací se zadavatelem.
4. Za plnění poskytovaná poddodavatelem je dodavatel odpovědný jako by toto plnění poskytoval sám. Dodavatel se zavazuje, že poskytne zadavateli, pokud bude i část plnění poskytována poddodavatelem, seznam kontaktních údajů na osoby provádějící plnění za poddodavatele. Zadavatel je oprávněn průběh plnění realizovaný poddodavatelem řešit napřímo s jeho pracovníky a dodavatel není oprávněn tuto komunikaci s poddodavatelem či jeho pracovníky jakkoliv omezovat nebo mařit.

Článek X
Smluvní pokuty, úrok z prodlení

1. V případě, že dodavatel nedodrží kteroukoli lhůtu pro plnění dle čl. III odst. 1 této smlouvy, uhradí zadavateli smluvní pokutu ve výši 1 000 Kč za každý započatý pracovní den prodlení.
2. V případě prodlení dodavatele ve lhůtě pro potvrzení ohlášení vady podle čl. VI odst. 8 této smlouvy je zadavatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každou započatou pracovní hodinu prodlení.
3. V případě prodlení dodavatele ve lhůtě pro odstranění vady Priority 1 podle čl. VI odst. 2 této smlouvy je zadavatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každou

započatou pracovní hodinu prodlení.

4. V případě prodlení dodavatele ve lhůtě pro odstranění vady Priority 2 podle čl. VI odst. 2 této smlouvy je zadavatel oprávněn požadovat smluvní pokutu ve výši 500 Kč za každou započatou pracovní hodinu prodlení.
5. V případě prodlení dodavatele ve lhůtě pro odstranění vady Priority 3 podle čl. VI odst. 2 této smlouvy je zadavatel oprávněn požadovat smluvní pokutu ve výši 300 Kč za každou započatou pracovní hodinu prodlení.
6. V případě prodlení dodavatele s poskytnutím aktualizace SW ve lhůtě dle čl. VI odst. 9 této smlouvy, a to i dohodnuté mezi smluvními staranami, je zadavatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každý pracovní den prodlení.
7. V případě zjištění, že dodané dílo nesplňuje jakýkoliv technický požadavek zadavatele dle přílohy č. 2 této smlouvy, je zadavatel oprávněn požadovat smluvní pokutu ve výši 150 000 Kč za každý zjištěný případ.
8. V případě prodlení dodavatele při nápravě nedostatků zjištěných při tvorbě realizační studie dle čl. II odst. 2 je zadavatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každý pracovní den prodlení.
9. V případě prodlení dodavatele při předání zprovozněného a nakonfigurovaného managementu dle čl. II odst. 3 Kroku 1 je zadavatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každý pracovní den prodlení.
10. V případě prodlení dodavatele při úpravě konfigurace v případě zjištění jiných než drobných nedostatků dle čl. II odst. 3 nebo 4 (Etapa 3 a 4) je zadavatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každý pracovní den prodlení.
11. V případě prodlení dodavatele při úpravě konfigurace v případě zjištění drobných nedostatků dle čl. II odst. 3 nebo 4 (Etapa 3 a 4) je zadavatel oprávněn požadovat smluvní pokutu ve výši 500 Kč za každý pracovní den prodlení.
12. V případě prodlení dodavatele při úpravě konfigurace dle čl. II odst. 1 (Etapa 1) je zadavatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každý pracovní den prodlení.
13. V případě prodlení dodavatele se zaškolením uživatelů díla dle čl. II odst. 4 je zadavatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každý pracovní den prodlení.
14. V případě prodlení dodavatele s předáním dokumentace díla dle čl. II odst. 4 je zadavatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každý pracovní den prodlení.
15. V případě porušení jakékoliv povinnosti dodavatele dle čl. VIII odst. 1, 2, 6, 7, 10, 11, 12, 13 a 16 je zadavatel oprávněn požadovat smluvní pokutu ve výši 20 000 Kč za každé jednotlivé porušení.
16. V případě porušení kterékoliv povinnosti dodavatele dle čl. IX je zadavatel oprávněn požadovat smluvní pokutu ve výši 40 000 Kč za každý jednotlivý případ porušení.
17. V případě prodlení dodavatele v kterékoliv lhůtě dle čl. XI odst. 5 nebo 6 této smlouvy je zadavatel oprávněn účtovat dodavateli smluvní pokutu ve výši 1 000 Kč za každý pracovní den prodlení.
18. V případě, že se ukáže tvrzení dodavatele uvedené v čl. XI odst. 1, 2 a 4 této smlouvy jako nepravdivé nebo poruší-li dodavatel závazek stanovený v čl. XI odst. 3 této smlouvy, vzniká zadavateli nárok na smluvní pokutu ve výši 100 000 Kč za každé jednotlivé nepravdivé tvrzení dodavatele či za každé jednotlivé porušení závazku dodavatele.

19. V případě porušení kterékoliv povinnosti dodavatele podle čl. XI odst. 8 této smlouvy je zadavatel oprávněn požadovat po dodavateli smluvní pokutu ve výši 500 Kč, a to za každý zjištěný případ takového porušení.
20. V případě porušení povinnosti dodavatele podle čl. VIII odst. 17 této smlouvy je zadavatel oprávněn požadovat po dodavateli smluvní pokutu ve výši 100 000 Kč, a to za každý zjištěný případ takového porušení.
21. V případě prodlení zadavatele s úhradou daňového dokladu má dodavatel právo požadovat úrok z prodlení podle nařízení vlády č. 351/2013 Sb.
22. Smluvní pokuta a úrok z prodlení jsou splatné do 14 dnů ode dne doručení platebního dokladu povinné smluvní straně. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu povinného ve prospěch účtu oprávněného.
23. Smluvní pokutou není dotčeno právo na náhradu škody v plné výši.

Článek XI
Další závazky dodavatele

1. Dodavatel potvrzuje, že ke dni účinnosti této smlouvy on ani jeho poddodavatelé nenaplňují definiční znaky subjektů uvedených v čl. 5k nařízení (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění jeho změn (dále také jako „nařízení č. 833/2014“), nebo subjektů uvedených v čl. 1h rozhodnutí Rady 2014/512/SZBP ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění jeho změn (dále jen „rozhodnutí 2014/512/SZBP“), kterým je zakázáno zadat či plnit jakoukoli veřejnou zakázku nebo koncesní smlouvu ve smyslu v tomto ustanovení uvedeného nařízení či rozhodnutí. Subjekty naplňující definiční znaky subjektů uvedených v čl. 5k nařízení č. 833/2014 nebo subjektů uvedených v čl. 1h rozhodnutí 2014/512/SZBP budou dále označovány jako „určené subjekty“.
2. Dodavatel dále potvrzuje, že ke dni účinnosti této smlouvy není osobou uvedenou v příloze I nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění jeho změn (dále také jako „nařízení č. 269/2014“), nebo v příloze I nařízení Rady (EU) č. 208/2014 ze dne 5. března 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině, ve znění jeho změn (dále také jako „nařízení č. 208/2014“), nebo v příloze I nařízení Rady (ES) č. 765/2006 ze dne 18. května 2006 o omezujících opatřeních vůči prezidentu Lukašenkovi a některým představitelům Běloruska, ve znění jeho změn (dále také jako „nařízení č. 765/2006“), nebo v příloze rozhodnutí Rady 2014/145/SZBP ze dne 17. března 2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění jeho změn (dále také jako „rozhodnutí 2014/145/SZBP“). Osoba uvedená v příloze I nařízení č. 269/2014 nebo v příloze I nařízení č. 208/2014 nebo v příloze I nařízení č. 765/2006 nebo v příloze rozhodnutí Rady 2014/145/SZBP bude dále označována jako „určená osoba“.
3. Dodavatel se současně zavazuje, že určeným osobám dle předchozího odstavce (není-li jí sám) nebo v jejich prospěch nezpřístupní žádné finanční prostředky ani hospodářské zdroje získané v souvislosti s plněním dle této smlouvy, a to přímo ani nepřímo.
4. Dodavatel dále potvrzuje, že plnění jím poskytované dle této smlouvy neporušuje žádným způsobem jakékoliv platné právní předpisy vydané zejména orgány Evropské unie [tj. zejména zákazy dovozu výrobků ze železa a oceli ve smyslu nařízení Rady (EU)

č. 2022/428 ze dne 15. března 2022, kterým se mění „základní“ nařízení (EU) č. 833/2014, nebo nařízení Rady (EU) č. 2022/355 ze dne 2. března 2022, kterým se mění „základní“ nařízení (ES) č. 765/2006 o omezujících opatřeních vzhledem k situaci v Bělorusku apod.]. Zadavatel je oprávněn při porušení této povinnosti dodavatele plnění nepřevzít v jakékoliv jeho části.

5. V případě, že by v průběhu účinnosti této smlouvy dodavatel nebo jeho jakýkoliv poddodavatel naplnili definiční znaky určeného subjektu nebo se dodavatel stal určenou osobou, je dodavatele povinen o takové skutečnosti zadavatele bez zbytečného odkladu, nejpozději do 2 pracovních dnů od nastání takové skutečnosti, písemně informovat.

6. Dojde-li za dobu účinnosti této smlouvy ke změnám v kterémkoliv z výše uvedených nařízení Rady (EU) či rozhodnutí Rady nebo k přijetí jakékoliv jiné nové legislativy tak, že bude nezbytné dát tuto smlouvu s nařízením Rady (EU), rozhodnutím Rady nebo jinou novou legislativou do souladu, zavazují se smluvní strany uzavřít písemný dodatek k této smlouvě, jehož předmětem bude úprava či doplnění práv a povinností smluvních stran v rámci této smlouvy (sankční mechanismy či nové možnosti ukončení smlouvy z toho nevyjímaje), a to bez zbytečného odkladu, nejpozději do 15 pracovních dnů poté, co změny nařízení Rady (EU), rozhodnutí Rady či jiná nová legislativa nabydou platnosti, nedohodnou-li se smluvní strany jinak.

7. Vznikne-li zadavateli v souvislosti s nepravdivým prohlášením nebo porušením povinností dodavatele dle odstavce 1–6 tohoto článku jakákoliv škoda, je dodavatel tuto škodu zadavateli povinen v plné výši nahradit.

8. Dodavatel se dále zavazuje, že v souvislosti s plněním této smlouvy:

   a) zajistí legální zaměstnávání osob a férové a důstojné pracovní podmínky pro všechny pracovníky podílející se na plnění této smlouvy. Férovými a důstojnými pracovními podmínkami se přitom rozumí takové pracovní podmínky, které splňují alespoň minimální standardy stanovené pracovněprávními a mzdovými předpisy. Dodavatel je povinen zajistit splnění požadavků dle tohoto ustanovení i u svých poddodavatelů;

   b) zajistí řádné a včasné plnění finančních závazků vůči svým poddodavatelům, kdy za řádné a včasné plnění se považuje plné uhrazení poddodavatelem vystavených faktur za plnění poskytnutá dodavateli v souvislosti s touto smlouvou, a to nejpozději do 14 dnů od obdržení platby ze strany zadavatele (pokud již splatnost poddodavatelem vystavené faktury nenastala dříve). Zadavatel je oprávněn požadovat předložení dokladů o provedených platbách poddodavatelům.

Článek XII
Doba trvání smlouvy, výpověď, odstoupení od smlouvy

1. Smlouva se v části poskytování podpory a zajišťování licencí pro provoz díla uzavírá na dobu neurčitou.

2. Smlouvu lze v části poskytování podpory a zajišťování licencí pro provoz díla ukončit písemnou výpovědí bez uvedení důvodu, která musí být doručena druhé smluvní straně nejpozději 6 měsíců přede dnem uplynutí předplacené doby podpory či licencí. Závazek zaniká uplynutím posledního dne předplacené doby.

3. V případě, že účinnost smlouvy skončí před koncem účtovacího období, vrátí dodavatel zadavateli alikvotní část předplacené ceny podpory a licencí.

4. Poruší-li kterákoliv strana podstatným způsobem závazky vyplývající z této smlouvy, má druhá strana právo odstoupit od smlouvy, a to i v části, prostřednictvím písemného

odstoupení. Takové odstoupení bude platné a nabude účinnosti dnem jeho doručení druhé smluvní straně.

5. Za podstatné porušení smlouvy strany považují zejména tyto případy:
   - ze strany dodavatele:
     a) dodaný HW nebo SW nebude splňovat veškeré požadavky zadavatele uvedené v příloze č. 2 této smlouvy,
     b) dodavatel bude v prodlení s předáním díla nebo jakékoliv etapy díla dle čl. III odst. 1 delším než 15 pracovních dnů,
     c) dodavatel bude v prodlení s odstraněním vady HW dle čl. VI odst. 1 písm. a) nebo c) nebo uvedením SW a konfigurace do funkčního stavu dle čl. VI odst. 1 písm. c) delším než 30 pracovních dnů,
     d) opakované nesplnění kterékoliv povinnosti dodavatele dle čl. VIII odst. 1 a 15, a to i přes předchozí upozornění zadavatele,
     e) nesplnění povinností dodavatele uvedených v čl. VIII odst. 2, 6, 7, 10, 11, 12, 14 a 16,
     f) další případy výslovně stanovené v této smlouvě,
   - ze strany zadavatele:
     a) prodlení s úhradou ceny plnění dle této smlouvy delší než 30 dnů.
6. Smluvní strany se dohodly, že je zadavatel oprávněn odstoupit od smlouvy kdykoliv v průběhu insolvenčního řízení zahájeného na majetek dodavatele, nebo pokud dodavatel vstupí do likvidace.
7. Zadavatel je oprávněn odstoupit od této smlouvy, a to i v její jakékoliv části, v případě, kdy na základě písemné informace od dodavatele či z vlastní iniciativy shledá, že dodavatel nebo jeho kterýkoliv poddodavatel naplnili definiční znaky určeného subjektu nebo dodavatel se stane určenou osobou nebo dodavatel neuzavře dodatek ke smlouvě ve smyslu čl. XI odst. 6 této smlouvy nebo dodavatel poruší povinnost nezpřístupnit jakékoliv určené osobě (není-li jí sám) nebo v její prospěch žádné finanční prostředky ani hospodářské zdroje získané v souvislosti s plněním dle této smlouvy, a to přímo ani nepřímo, nebo povinnost dodat či poskytnout plnění, které neporušuje žádným způsobem jakékoliv platné právní předpisy vydané zejména orgány Evropské unie.
8. Zadavatel je dále oprávněn odstoupit od smlouvy, pokud dojde k významné změně kontroly nad dodavatelem, přičemž kontrolou se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů či ekvivalentní postavení nebo dojde ke změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými dodavatelem k plnění této smlouvy a tato změna bude zadavatelem vyhodnocena jako bezpečnostní riziko ve smyslu ZKB a/nebo VKB.
9. Zadavatel je oprávněn vypovědět tuto smlouvu, a to i v její jakékoliv části, bez výpovědní doby v případě, kdy na základě písemné informace od dodavatele či z vlastní iniciativy shledá, že dodavatel nebo jeho kterýkoliv poddodavatel naplnili definiční znaky určeného subjektu nebo dodavatel se stane určenou osobou nebo dodavatel neuzavře dodatek ke smlouvě ve smyslu čl. XI odst. 6 této smlouvy nebo dodavatel poruší povinnost nezpřístupnit jakékoliv určené osobě (není-li jí sám) nebo v její prospěch žádné finanční prostředky ani hospodářské zdroje získané v souvislosti s plněním dle této smlouvy, a to přímo ani nepřímo, nebo povinnost dodat či poskytnout plnění, které neporušuje

žádným způsobem jakékoliv platné právní předpisy vydané zejména orgány Evropské unie. Tato výpověď je účinná dnem jejího doručení dodavateli.

10. Odstoupení od smlouvy se nedotýká nároku na zaplacení smluvní pokuty nebo nároku na náhradu škody vzniklé porušením smlouvy.

11. Smluvní strany si v souladu s ustanovením § 1992 občanského zákoníku sjednávají, že zadavatel je oprávněn zrušit tuto smlouvu zaplacením odstupného ve výši 30 000 Kč na účet dodavatele, a to kdykoli do akceptace Etapy 2. Zrušení smlouvy je účinné zaplacením sjednaného odstupného na bankovní účet dodavatele. Zaplacením odstupného zanikají všechna práva a povinnosti obou smluvních stran vyplývající ze zrušené smlouvy s výjimkou závazku mlčenlivosti dodavatele a případně vzniklé smluvní pokuty a náhrady škody.

Článek XIII
Uveřejnění smlouvy a skutečně uhrazené ceny

1. Dodavatel si je vědom zákonné povinnosti zadavatele uveřejnit na svém profilu tuto smlouvu včetně všech jejích případných změn a dodatků a výši skutečně uhrazené ceny za plnění této smlouvy.

2. Profilem zadavatele je elektronický nástroj, prostřednictvím kterého zadavatel, jako veřejný zadavatel dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“), uveřejňuje informace a dokumenty ke svým veřejným zakázkám způsobem, který umožňuje neomezený a přímý dálkový přístup, přičemž profilem zadavatele v době uzavření této smlouvy je https://ezak.cnb.cz/.

3. Povinnost uveřejňování dle tohoto článku je zadavateli uložena § 219 ZZVZ.

4. Uveřejňování bude prováděno dle ZZVZ a příslušného prováděcího předpisu k ZZVZ.

Článek XIV
Závěrečná ustanovení

1. Smlouva nabývá platnosti a účinnosti dnem podpisu oprávněnými zástupci obou smluvních stran.

2. Smlouvu je možno měnit nebo doplňovat pouze formou písemných, vzestupně číslovaných dodatků podepsaných zástupci obou smluvních stran, není-li ve smlouvě uvedeno jinak. Dodatek v elektronické podobě se považuje za řádně podepsaný zadavatelem, je-li podepsán kvalifikovanými elektronickými podpisy.

3. Závazkový vztah založený touto smlouvou se řídí českým právním řádem, zejména občanským zákoníkem a autorským zákonem.

4. Spory vyplývající z této smlouvy budou řešeny především dohodou smluvních stran. Nebude-li možné dosáhnout dohody, bude spor řešen před místně a věcně příslušným soudem České republiky, a to výlučně podle českého práva.

5. Veškerá komunikace mezi smluvními stranami vztahující se k této smlouvě bude probíhat v českém nebo slovenském jazyce, nebude-li smluvními stranami v konkrétním případě dohodnuto jinak.

6. Odpověď stran této smlouvy podle § 1740 odst. 3 občanského zákoníku s dodatkem nebo odchylkou není přijetím nabídky, ani když podstatně nemění podmínky nabídky.

7. Smluvní strany vylučují uplatnění ustanovení § 1765 a § 1766 a § 2620 občanského zákoníku na svůj smluvní vztah založený touto smlouvou, čímž se ruší nárok dodavatele

na jednání podle § 1765 odst. 1 občanského zákoníku. Dodavatel tímto přebírá nebezpečí změny okolností dle § 1765 odst. 2 občanského zákoníku.

8. Práva a povinnosti vzniklé z této smlouvy mohou být postoupeny pouze po předchozím písemném souhlasu druhé smluvní strany.
9. Smlouva je vyhotovena v elektronické podobě, přičemž každá ze smluvních stran obdrží vyhotovení smlouvy opatřené elektronickými podpisy.
10. Nedílnou součástí této smlouvy jsou následující přílohy:

Příloha č. 1 – Specifikace a výčet dodávaných HW komponent a potřebných SW licencí
Příloha č. 2 – Technické požadavky zadavatele
Příloha č. 3 – Bezpečnostní požadavky zadavatele
Příloha č. 4 – Obecná pravidla pro dodavatele v oblasti bezpečnosti IT

V Praze

Za zadavatele:

……..
Ing. Milan Zirnsák
ředitel sekce informatiky
podepsáno elektronicky

……..
Ing. Zdeněk Virius
ředitel sekce správní
podepsáno elektronicky

V Praze

Za dodavatele:

…….
Daniel Štefan
na základě pověření
podepsáno elektronicky

Příloha č. 1

Specifikace a výčet dodávaných HW komponent a potřebných SW licencí a bližší popis integrací s externími zdroji

Seznam dodávaných SW licencí:

- Nabízené licence jsou v režimu MSSP – CrowdStrike Powered Service Provider partner (also known as a packaged MSP). https://www.crowdstrike.com/partners/managed-service-security-providersmssps/
- V rámci ceny nabízíme balíček MSSP Defend jehož jsou součástí tyto moduly:

  o Falcon Prevent
  o Falcon Insight
  o Threat Graph Standard on EU Cloud (7/15/30)
  o Device Control
  o University LMS Subscription New Customer Access Pass
  o Falcon Search Retention (180 days)

Doplnění k licencím

EDR platforma Falcon společnosti Crowdstrike se licencuje na zařízení (device) nikoliv na uživatele. Zařízením je myšleno jakékoliv zařízení, které je potřeba chránit, včetně instance virtuálního desktopu. Počet uživatelů je pro potřeby výpočtu celkového počtu licencí irelevantní. Stejně tak se licence neliší, jestli chrání server s mnoha uživateli nebo jednouživatelskou stanici.

Z těchto prerekvizit jsme vypočítali potřebný počet licencí takto:
Koncová zařízení = 1800
Serverová zařízení = 160
Počet uživatelů, kteří mohou přistoupit k virtualizovanému desktopu = 1500

Celkový kalkulovaný počet licencí činí tedy **3460 ks**.

Integrace

V nabídce kalkulujeme integraci s vaším sandboxem Checkpoint. Integrace proběhne formou komunkace API – API, kde počítáme s funkční implementací Checkpoint Threat Prevention API na vaší straně.

Integrace s ThreatIntel – opět bude přes API, kde předpokládáme že máte konkrétní účet do některé ThreatIntel platformy, ze které budeme vyčítat požadovaná data, která následně přes API pošleme do EDR platformy.

Příloha č. 3

Bezpečnostní požadavky zadavatele

1. Dodavatel odpovídá za to, že do objektů zadavatele (dále jen „ČNB“) budou vstupovat nebo vjíždět pouze ti jeho pracovníci, kteří jsou jmenovitě uvedeni v seznamu pracovníků schváleném ČNB (dále jen „seznam“). Tato povinnost se vztahuje i na posádky vozidel dodavatele vjíždějících do garáží ČNB za účelem složení a naložení nákladu. Dodavatel předloží seznam ČNB nejpozději pět pracovních dní před zahájením prací.
2. Seznam bude obsahovat tyto položky: jméno, příjmení a číslo průkazu totožnosti každého z pracovníků dodavatele. Dodavatel se zavazuje zajistit, aby všichni jeho pracovníci uvedení v seznamu byli ještě před předložením seznamu ČNB proškoleni o podmínkách zpracování osobních údajů a o právech subjektů údajů ve smyslu obecného nařízení o ochraně osobních údajů - Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“). Dodavatel se zejména zavazuje, že všichni jeho pracovníci uvedení v seznamu budou nejpozději do okamžiku předložení seznamu ČNB poučeni:
   a) o tom, že dodavatel předá jejich osobní údaje v rozsahu: jméno, příjmení a číslo průkazu totožnosti České národní bance, sídlem Na Příkopě 28, Praha 1 v rámci plnění této smlouvy, a to za účelem ochrany práv a oprávněných zájmů ČNB (zajištění evidence osob vstupujících do budovy ČNB z důvodu ochrany majetku a osob a správy systému kontrol vstupů ČNB);
   b) o veškerých právech subjektu údajů, která mohou uplatnit vůči dodavateli a ČNB, zejména o právu na přístup k osobním údajům, které jsou o nich zpracovávány, právu na námitku proti zpracování osobních údajů, právu požadovat nápravu situace, která je v rozporu s právními předpisy, a to zejména formou zastavení nakládání s osobními údaji, jejich opravou, doplněním či odstraněním, jakož i o právu podat stížnost k Úřadu pro ochranu osobních údajů.
3. Za poučení svých pracovníků ponese dodavatel vůči ČNB následně odpovědnost. V případě nesplnění povinnosti podle odst. 2 této přílohy nahradí dodavatel újmu, která v souvislosti s uvedeným ČNB vznikne, a to včetně případné nemajetkové újmy vzniklé poškozením dobrého jména a dobré pověsti, újmy vzniklé v důsledku postihu pravomocně uloženého ČNB správním nebo jiným k tomu oprávněným orgánem veřejné moci a újmy vzniklé ČNB v důsledku úspěšného uplatnění práv pracovníků dodavatele vůči ČNB.
4. Požadavky na případné doplňky a změny schváleného seznamu je nutno neprodleně oznámit ČNB. Případné doplňky a změny seznamu podléhají schválení ČNB. Osoby neschválené ze strany ČNB nemohou vstupovat do objektů ČNB, přičemž ČNB si vyhrazuje právo neuvádět důvody jejich neschválení.
5. Dodavatel uvede předem ty své pracovníky, pro které požaduje vystavení vstupních karet ke vstupu do objektů ČNB. Vystavení vstupních karet podléhá schválení ze strany ČNB. První vstupní karty budou vystaveny na náklady ČNB. Každé další vystavení vstupní karty bude zpoplatněno částkou 200,- Kč (vč. DPH) s tím, že tato částka bude dodavateli vyfakturována. Za vystavení nové vstupní karty nebude nutné platit v případech, kdy:
   - dosavadní karta přestane fungovat bez viditelného mechanického poškození,
   - dojde ke změně příjmení pracovníka,
   - byla karta odcizena a událost je doložitelná protokolem od Policie ČR.

6. Dodavatel bude při zahájení činnosti pro ČNB vybaven základním počtem vstupních karet pro jednotlivé pracovníky podle schváleného seznamu. Vstupní karta umožní oprávněnému pracovníkovi dodavatele samostatný vstup do vyhrazených prostor objektu ČNB a samostatný pohyb v nich. Každá vstupní karta bude nepřenosná a bude vydávána odborem bankovní bezpečnosti a krizového řízení ČNB.
7. Vstupní karty budou vydávány ze strany ČNB pro každého pracovníka dodavatele jednotlivě proti podpisu, a to po předložení výpisu z rejstříku trestů, který nebude starší než tři měsíce. Výpis z rejstříku trestů bude pracovníkovi vrácen. Při převzetí vstupní karty bude dotčený pracovník dodavatele poučen o způsobu používání vstupní karty a o režimu vstupu osob a vjezdu vozidel do objektů ČNB a o pohybu v nich.
8. Pracovník dodavatele, kterému byla vydána vstupní karta, je povinen okamžitě po zjištění ztráty, odcizení, zneužití, zničení nebo poškození vstupní karty, které brání jejímu řádnému užívání, toto oznámit odboru bankovní bezpečnosti a krizového řízení ČNB.
9. Při ukončení pracovního poměru pracovníka dodavatele uvedeného v seznamu nebo při ukončení plnění podle smlouvy je dodavatel povinen neprodleně vrátit vstupní kartu dotčeného pracovníka odboru bankovní bezpečnosti a krizového řízení ČNB.
10. ČNB si vyhrazuje právo nevydat vstupní karty pracovníkům dodavatele bez udání důvodu.
11. ČNB si vyhrazuje právo vstupní kartu pracovníkovi dodavatele odebrat z důvodu porušení režimu vstupu osob a vjezdu vozidel do objektu ČNB nebo porušení režimu pohybu v něm.
12. ČNB si vyhrazuje právo vyřadit i schválené pracovníky dodavatele ze seznamu bez udání důvodů. Schválení pracovníci musí dodržovat směrnice ČNB a pokyny ostrahy pro vstup do vyhrazených prostor a pro pobyt v nich.
13. Pracovníci dodavatele jsou povinni podrobit se při každém vstupu do objektu ČNB bezpečnostní kontrole prováděné bankovními policisty.
14. ČNB si vyhrazuje právo nevpustit do objektů ČNB pracovníka dodavatele, který je zjevně pod vlivem alkoholu, drog nebo jiné omamné látky.
15. Vstup do objektů ČNB se zvířaty je zakázán.
16. Vstup soukromých návštěv do vnitřních prostor objektů ČNB je zakázán. Pro tyto účely je možné využít určené návštěvní místnosti.
17. Dodavatel je povinen zajistit, že jeho pracovníci budou vstupovat do prostorů ČNB a zdržovat se v nich pouze ve firemním pracovním oděvu s viditelným nesnímatelným označením logem dodavatele. Pracovní oděv musí být doplněn viditelně nošenou vstupní kartou vydanou ČNB každému pracovníkovi dodavatele podle schváleného seznamu.
18. Dodavatel a jeho pracovníci budou věnovat při plnění díla v oblasti požární ochrany zvýšenou pozornost:
    - dodržování právních předpisů o požární ochraně,
    - předpisům ČNB při provádění požárně nebezpečných prací se zvýšeným požárním nebezpečím (svařování, řezání plamenem, pájení, broušení, rozbrušování apod.),
    - průrazům a průchodům u rozvodů instalací a technologií hranicemi požárních úseků, včetně zachování, obnovení nebo nového vyhotovení jejich protipožárních ucpávek.
19. Dodavatel se zavazuje zajistit, že jeho pracovníci, jakož i pracovníci případných jeho poddodavatelů, kteří se budou na plnění podle této smlouvy podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se v průběhu plnění seznámí a které nejsou veřejně

známy. Pracovníci či poddodavatelé dodavatele a jejich pracovníci smí používat informace získané v souvislosti s plněním dle této smlouvy výhradně pro účely plnění této smlouvy. Dostane-li se kterákoliv z osob uvedených v tomto odstavci v průběhu plnění do kontaktu s údaji zadavatele vyplývajícími z jeho provozní činnosti, zavazuje se tyto údaje nezneužít, nezměnit ani nijak nepoškodit, neztratit či neznehodnotit.

20. Povinnost mlčenlivosti podle odst. 19 této přílohy není časově omezena.
21. V případě mimořádné události se pracovníci dodavatele musí řídit pokyny bankovních policistů nebo dozorujícího zaměstnance ČNB a dále instrukcemi vyhlašovanými vnitřním rozhlasem ČNB.
22. Pracovníci dodavatele nesmí vnášet do prostor ČNB nebezpečné předměty, jako jsou střelné zbraně, výbušniny, hořlavé kapaliny, tlakové lahve apod. O tom, co je či není nebezpečný předmět, rozhodují bankovní policisté v souladu s vnitřními předpisy ČNB.
23. Fotografování a pořizování videozáznamů je ve všech prostorách objektů ČNB zakázáno. Výjimku tvoří pořizování dokumentace technických havárií a poruch. Konkrétní případ musí předem písemně povolit ředitel odboru bankovní bezpečnosti a krizového řízení nebo ředitel příslušné pobočky ČNB.
24. Ve všech prostorách objektů ČNB je přísný zákaz kouření a používání otevřeného ohně. O povolení k provedení požárně nebezpečné práce se zvýšeným požárním nebezpečím požádá dodavatel písemnou formou dozorujícího zaměstnance ČNB, a to vždy nejpozději jeden pracovní den před zahájením prací.
25. Pracovníci dodavatele se musí zdržet poškozování či odcizení majetku ČNB, a dále i jakéhokoli nevhodného chování vůči zaměstnancům a návštěvníkům ČNB.
26. Pracovníci dodavatele uvedení na seznamu se musí před započetím výkonu práce v objektech ČNB prokazatelně seznámit s „Pravidly pro smluvní partnery ČNB k zajištění bezpečnosti a ochrany zdraví při práci, požární ochrany a ochrany životního prostředí v ČNB“ (dále jen „pravidla“). Pravidla předá v listinné formě pověřeným osobám dodavatele požární a bezpečnostní technik ČNB. Pověřená osoba dodavatele s pravidly seznámí všechny dotčené pracovníky dodavatele.
27. ČNB je oprávněna v objektu ČNB kdykoliv podrobit kontrole kteréhokoliv pracovníka dodavatele uvedeného na seznamu ohledně dodržování požární ochrany, bezpečnosti práce a všech výše uvedených ustanovení.

Příloha č. 4

Obecná pravidla pro dodavatele v oblasti bezpečnosti IT

1) Pokud jsou tato obecná pravidla v rozporu s ustanovením textu této smlouvy nebo zadávací dokumentace nebo její jinou přílohou, má přednost ustanovení textu této smlouvy nebo zadávací dokumentace nebo její jiná příloha.
2) Dodavatel je povinen zajistit, že jeho pracovníci či poddodavatelé a jejich pracovníci, kteří se budou na plnění podle této smlouvy podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se u zadavatele seznámí a které nejsou veřejně dostupné. Povinnost mlčenlivosti není časově omezena.
3) Dodavatel je rovněž povinen chránit informace, které nejsou veřejně dostupné, zejména předanou dokumentaci, před jejich prozrazením a/nebo zpřístupněním neoprávněným osobám a dále použít získané informace výhradně pro účely plnění smlouvy s ČNB.
4) Dodavatel nemá vzdálený přístup k systémům a do počítačové sítě ČNB.
5) Pracovníci dodavatele, kteří budou samostatně přistupovat k informačním systémům a systémovému prostředí ČNB, se před nebo při prvním přístupu musí seznámit s bezpečnostními požadavky a svými povinnostmi vyplývajícími z vnitřních předpisů ČNB.
6) Dodavatel a jeho pracovníci nejsou oprávněni:
   a) obcházet bezpečnostní mechanizmy prostředků výpočetní techniky;
   b) sdělovat své přístupové údaje k systémům ČNB;
   c) sdílet přístup k systémům ČNB (umožnit jinému pracovat pod uživatelovým oprávněním);
   d) provádět akce požadované třetí osobou (instalace softwaru, návštěva webových stránek apod.) bez ověření oprávněnosti požadavku.
7) Dodavatel a jeho pracovníci jsou povinni:
   a) okamžitě nahlásit sekci informatiky, pokud identifikují možnost obejití bezpečnostních mechanizmů prostředků výpočetní techniky. To neplatí pro dodavatele a uživatele, jejichž předmět smlouvy nebo pracovní náplň obsahuje tuto činnost;
   b) při opuštění pracovní stanice stanici uzamknout (např. vytažením multifukčního průkazu ze stanice) nebo se odhlásit a ověřit, že k odhlášení/uzamčení opravdu došlo;
   c) bezpečně zlikvidovat nepotřebná výměnná média (např. CD/DVD, flash disk, paměťová karta) prostřednictvím služby HelpDesku;
   d) bez prodlení odebrat z tiskárny vytištěné dokumenty, popřípadě pro zajištění důvěrnosti použít zabezpečený tisk, pokud to nastavení tiskárny umožňuje;
   e) v případě detekce viru nebo podezření na přítomnost škodlivého kódu neprodleně kontaktovat HelpDesk a stanici kompletně prověřit antivirovým programem za případné spolupráce HelpDesku.
8) Pracovníci dodavatele nesmí:
   a) zaznamenávat heslo tak, aby mohlo být snadno identifikováno (týká se i zapisování do elektronických dokumentů, např. Notepad). Pro uchování je možné použít například bezpečné úložiště na čipové kartě uživatele (SmartNotes);

b) používat stejná hesla v systémech ČNB a pro přístup do dalších systémů a aplikací mimo ČNB (např. soukromá e-mailová schránka, Facebook, LinkedIn).

9) Dodavatel a jeho pracovníci nejsou oprávněni:

a) používat soukromou e-mailovou schránku pro činnosti související s plněním dle této smlouvy, kromě výjimečné situace, která nesnese odkladu a při níž hrozí nebezpečí z prodlení v případě nedostupnosti nebo poruchy pracovního e-mailu;

b) nastavovat automatické přeposílání e-mailů z pracovní e-mailové adresy mimo systémové prostředí ČNB;

c) ukládat jiné než veřejné informace mimo úložiště pod správou ČNB (případně pod správou smluvně zajištěného partnera), zejména do cloudových služeb (např. uloz.to, leteckaposta.cz, Google Disk, Microsoft OneDrive a další).

10) Dodavatel a jeho pracovníci nejsou oprávněni:

a) nepovoleně používat, kopírovat a šířit software, jako např.:

i) instalovat nebo spouštět na počítačích ČNB soukromě pořízený software (včetně softwaru licencovaného na uživatele jako soukromou osobu);

ii) instalovat nebo spouštět na počítačích ČNB z internetu stažený software (včetně komerčního software, software typu shareware, freeware, public domain a software licencovaného modelem GPL – General Public Licence). To neplatí v případech, kdy předmět této smlouvy obsahuje tuto činnost;

iii) instalovat či přenášet software ve vlastnictví ČNB na jiné počítače ČNB, na své soukromé počítače nebo na počítače třetích stran nebo pořizovat kopie softwaru instalovaného v počítači ČNB. To neplatí

(1) pro situace výslovně schválené a popsané v jiném vnitřním předpisu (např. vzdálený přístup ze zařízení, které není ve vlastnictví ČNB) a

(2) v případech, kdy předmět této smlouvy obsahuje tuto činnost;

b) používat nebo poskytnout neoprávněně jiným uživatelům sériová čísla, licenční klíče, hardwarové klíče nebo jiné technické prostředky sloužící k zajištění ochrany nebo jednoznačné identifikaci vlastníka licence softwaru získané v ČNB;

c) bránit spouštění nástrojů sloužících pro automatizované kontroly nainstalovaného a spouštěného softwaru a provádět činnosti, které by vedly ke zkreslení získaných dat z těchto nástrojů.

Archivace elektronické pošty

1) Zpráva zaslaná tak, že alespoň jedním z adresátů zprávy je emailová adresa ...@cnb.cz, se ukládá současně s přijetím i do dlouhodobého archivního úložiště.

2) Veškeré zprávy odesílané z emailové adresy ...@cnb.cz se ukládají do dlouhodobého archivního úložiště současně s odesláním.

Kontrola přístupu na Internet

Z důvodu zvláštní povahy činnosti ČNB a z toho plynoucí povinnosti zajištění bezpečnosti informačních systémů ČNB, z nichž některé jsou součástí kritické informační infrastruktury státu, jsou přístupy uživatelů na Internet automaticky zaznamenávány na úrovni domén 2. řádu (tj. např. idnes.cz).

Příloha č. 2

Funkcionalita managementu	Popis funkce	Požadované funkční vlastnosti	Mandatorní požadavek
Centrální management	Všechny funkce požadované v tomto dokumentu jsou dostupné a konfigurovatelné prostřednictvím jedné centrální konzole managementu.	Centrální konzole poskytuje možnost konfigurace prostředí a politik s možností granulárního nastavení všech požadovaných funkcionalit uvedených v tomto dokumentu, zobrazuje aktuální stav chráněného prostředí, umožňuje prohledávání metadat atd.	Ano
Retence dat	Dostupnost informací vzniklých provozem systému.	Dostupnost detekovaných událostí v prostředí management konzole minimálně 12 měsíců od jejich vzniku.	Ano
		Dostupnost plné telemetrie/metadat v rozsahu minimálně 90 dnů od jejich vzniku.	Ano
Autentizace uživatelů	Systém umožnuje vynucení užití dvou-faktorové autentizace pro přihlášení všech uživatelů centrální konzole managementu		Ano
Reakce na incidenty	Zajišťuje okamžitou reakci na hrozby včetně snížení dopadu v případě detekce bezpečnosntího incidentu. Poskytuje konzoli pro sledování situace v reálném čase pro podrobné vyšetřování.	Umožňuje automatickou reakci na incident bez nutnosti zásahu operátora systému.	Ano
		Umožnuje síťově izolovat vybranou koncovou stanici.	Ano
		Snapshot systému/souborů a jejich automatickou obnovu v případě odhalení aktivního incidentu.	Ano
		Vizualizace šíření nákazy mezi jednotlivými zařízeními formou časové osy.	Ano
Vzdálený příkazový řádek	Umožňuje z webového managementu přístup k příkazovému řádku koncového zařízení. U platformy Microsoft Windows je požadovaná podpora minimálně skriptovacího jazyku PowerShellu. U Linux/UNIX distribucí je požadovaná podpora minimálně skriptovacího jazyka bash.	Umožňuje vzdálený přístup k plnému příkazovému řádku zařízení.	Ano
		Umožňuje definovat skupinu uživatelů s možností využívání funkcionality vzdáleného příkazového řádku.	Ano
		Umožňuje definovat politiku omezující použití vzdáleného příkazového řádku na vybrané skupině zařízení.	Ano
		Umožňuje vynucení aktivního schválení využití vzdáleného příkazového řádku jiným uživatelem systému formou potvrzení v prostředí centrálního managementu.	Ano
		Vynucení užití dvou-faktorové autentizace uživatele, který chce vzdálenou příkazovou řádku použít.	Ano
		Auditování veškeré aktivity spojené s využitím nebo rekonfiguraci nastavení možnosti užití vzdálené příkazové řádky.	Ano
Forenzní analýza	Získání aktuálních informací z koncového zařízení pro forenzní analýzu. Pokytuje platformu pro vyšetřování incidentu za účelem identifikace root cause, pochopení způsobu nakažení a průniku a sběr důkazů pro technologické i právní potřeby.	Metadata aktivit/telemetrie dostupná minimálně po dobu 90 dnů ze všech chráněných zařízení.	Ano
Threat Hunting	Zajišťuje platformu pro proaktivní vyhledávání hrozeb a zranitelností. Poskytuje možnost cíleného vyhledávání všech monitorovaných parametrů napříč všemi zařízeními ve všech dostupných metadatech. Tvorba dotazů pomocí pokročilých filtrů nebo vlastní zdokumentované syntaxe.	Manuální zpětné prohledávání všech metadat na základě libovolných parametrů zadaných operátorem systému.	Ano
		Automatické zpětné prohledávání metadat/telemetrie na základě uživatelsky zadaných pravidel s možností definované reakce v případě pozitivního nálezu.	Ano
Threat Intelligence	Umožňuje integraci s externími zdroji bezpečnostních informací za účelem zvýšení kvality detekce a snížení rizika průniku zero-day hrozeb.	Externí zdroje předávají IoC (minimálně v rozsahu IP adresa, doména, hash souboru).	Ano
Reportování	Generuje souhrnné reporty a nabízí analytické a managerské přehledy za účelem poskytnutí celkového přehledu stavu chráněného prostředí s detailním pohledem na bezpečnostní incidenty, trendy hrozeb, soulad s předpisy a standardy, aktuálním stavem koncových stanic apod. ve formátu PDF.	Reporty musí být upravitelné dle potřeby objednatele.	Ano
Notifikace	Systém musí být schopný zasílat notifikace určeným osobám v případě zjištění bezpečnostních nebo provozních událostí.	E-mail	Ano
Znalostní báze útočných technik a taktik	Systém automaticky mapuje identifikované události na techniky a taktiky aktuální verze MITRE frameworku. U identifikovaných událostí může obohacovat informace o odkazy na znalostní bázi aktuálního MITRE frameworku a/nebo vlastní znalostní báze útočných technik a taktik.	U identifikovaných hrozeb dochází k automatickému mapování událostí na MITRE techniky a taktiky.	Ano
Podpora formátu pro SIEM	Export zaznamenaných událostí ve formátu.	Formát CEF	Ano
		Formát Syslog	Ano
Lokalizace systému	Lokalizace produktu do českého pracovního prostředí.	Prostředí managementu zobrazuje informace v lokální časové zóně.	Ano
		Export dat ze systému s uvedením časové zóny.	Ano
Granulární správa přístupů	Konzole na centrální správu umožňuje granulární řízení přístupů a oprávnění. Minimálně na úrovni rozlišení úrovně oprávnění: Správce - Analytik - Auditor.	Řízení přístupu k bezpečnostním politikám	Ano
		Řízení přístupu k objektům chráněných zařízení	Ano
REST API	Existující rozhraní pro automatizaci nebo strojové vyčítání libovolných dat systému.		Ano
Správa verzí agentního software	Verze agentní software je spravována výhradně z centrální konzole, agentní sofware není možné modifikovat ani s oprávněním lokálního administrátora.	Upgrade agentního software na chráněném zařízení.	Ano
		Možnost tvorby skupin zařízení s konkrétní verzí agentního software. Primárně pro řízení a testování nových verzí agentního software před nasazením do produkčního prostředí.	Ano
Certifikační a legislativní požadavky	Doložení certifikace SOC2 Type 2 v případě cloudové varianty produktu.		Ano
	Uložení všech získaných metadat/telemetrie ze zařízení zadavatele na území Evropské unie.		Ano
Bezpečnost dat	Jakákoliv data, se kterými nástroj pracuje, neopouští lokální prostředí/infrastrukturu. Netýká se sbíraných metadat/telemetrie chráněných zařízení.		Ano
	Šifrování informací.	Šifrování ukládaných informací algoritmy splňující vyhlášky NÚKIB.	Ano
		Šifrování přenášených informací minimálně protokolem TLS 1.2 a algoritmy splňující vyhlášky NÚKIB.	Ano
	Výmaz dat po ukončení poskytování služby.	Pernamentní výmaz všech nasbíraných metadat a událostí.	Ano
		Pernamentní výmaz všech záloh informací zadavatele pořízených po dobu trvání smlouvního vztahu.	Ano
Zálohy	Provádění periodických záloh konfigurace managemnetu.		Ano

Funkcionalita endpointu	Popis funkce	Požadované funkční vlastnosti	Splňuje řešení ?
Anti-malware	Detekuje a blokuje známý malware nebo podezřelé soubory.		Ano
	Umožňuje definovat periodické scany vybraných lokálních a vzdálených diskových zařízení.		Ano
	Na platformě Windows nahrazuje integrací s Windows Security Center defaultní anti-malware Microsoft Defender Antivirus.		Ano
	Poskytuje lokální karanténu pro přístup k zajištěným vzorkům škodlivého software.		Ano
Anti-exploit	Ochrana před známými typy průniků využívajících zranitelností operačního systému nebo provozovaných aplikací.		Ano

Behaviorální analýza	Pomocí algoritmů strojového učení detekuje a blokuje nebezpečné a podezřelé chování součástí operačního systému, zejména spouštěných souborů, služeb nebo procesů, přístupu k operační paměti, zápisy do souborů a registrů systému, pokusy o exploitaci nebo zlovolné využití legitimních součástí operačního systému.		Ano
Ochrana proti ransomware	Disponuje detekčními mechanismy na identifikaci a zastavení známého i neznámého ransomware. V případě nákazy a destrukce souborů umožnuje automatický rollback infikovaných nebo zničených souborů do původního stavu.	Windows 10 a vyšší verze	Ano
		Windows Server 2016 a vyšší verze	Ano
Kontrola periferií	Umožnuje centrální správu periferií, zejména zařízení připojitelné prostřednictvím USB a bluetooth.		Ano
	Správce systému musí být schopný povolovat nebo zakazovat užité zařízení na základě jednoznačných identifikátorů třídy, výrobců, produktu, seriového čísla nebo verze protokolu.		Ano
	U pamětových USB zařízení musí být systém schopný omezení akcí nově připojeného zařízení, a to na úrovni alespoň: čtení a zápis, čtení, blokace celého zařízení.		Ano
	Notifikace pro příslušného uživatele operačního systému o akcích spojených s připojeným zařízením (nejméně povolení a blokace zařízení).		Ano
	Systém musí zaznamenávat události o použití autorizovaných i neautorizovaných zařízení, s minimálně všemi podrobnostmi uvedenými výše.		Ano
	Centrální logování informací ukládaných na přenosná media v minimálním rozsahu: čas, uživatel, název souboru, velikost.		Ano
Endpoint Visibility	Poskytuje hloubkovou viditelnost do aktivit na koncovém zařízení. Získává data a metadata o procesech, síťových spojeních, změnách nad soubory, systémových událostech a uživatelském chování. Zajišťuje infromace pro bezpečnostní tým pro plné pochopení nežádoucího chování na koncovém zařízení ve všech svých fázích.		Ano
Sandboxing	Podpora on-premise sandboxu CheckPoint SandBlast. Alternativou pro splnění tohoto bodu je dodání on-premise sandboxu jako součást tohoto VŘ (HW, licence, podpora výrobce i dodavatele budou součástí nabídkové ceny). Takto dodaný sandbox musí být ve všech výkonnostních parametrech (všechny položky části „Performance" v datasheetu výrobce) stejný nebo lepší než zadavatelem aktuálně provozovaná dvojice appliance CheckPoint SandBlast TE250x.		Ano
Ochrana agentního SW	Ochrana funkčnosti lokálního agenta, kdy není možné agenta odinstalovat nebo zastavit ani pomocí oprávnění lokálního administrátora systému.		Ano
	Pro manipulaci se software agenta je zapotřebí využít centrální konzole. Manipulace musí být zabezpečena heslem, tokenem, nebo jiným bezpečnostním mechanismem.		Ano
Detekční mód	Umožňuje definici bezpečnostní politiky, tak aby všechny ochrané mechanismy byly provozovány pouze v detekčním módu, bez aktivních zásahů provozu. Zjištěné události musí být zalogovány v centrálním managementu.		Ano
GUI	Uživatel má dostupné GUI agentního SW na všech požadovaných platformách, včetně nasazení na RDS serverech Citrix Virtual Apps and Desktops (Citrix XenApp).		Ano
	Umožňuje uživateli zobrazit aktuální bezpečnostní stav zařízení, na kterém pracuje.		Ano
	Notifikace uživatele o výskytu bezpečnostní události a způsobu jejího řešení.		Ano
	Umožňuje uživateli zobrazit seznam souborů zadržených v lokální karanténě.		Ano
Podpora RDS Citrix Virtual Apps and Desktops (Citrix XenApp)	Oficiální podpora výrobce k provozu agenta v prostředí terminálových služeb (technologie RDS, nejedná se o VDI).		Ano
	Jednoznačná identifikace uživatele ve víceuživatelském prostředí (více uživatelů pracuje na jedné instanci OS, pod jednou IP adresou). Zasílání notifikací pouze uživateli, který je původce události. Nepřípustné je zejména notifikování nesprávných uživatelů terminálového serveru, zápis do logu pod jiným uživatelem, než který událost vyvolal apod.		Ano
	Dostupnost standardního GUI agentního software pro každého přihlášeného uživatele terminálového serveru.		Ano
Podpora OS platforem	Windows 10 a novější		Ano
	Windows server 2016 a novější		Ano
	RHEL 7 a novější		Ano
	OL7 a novější		Ano
	MacOS 12 a novější		Ano
Offline detekce a reakce	Schopnost plnohodnotné ochrany koncového zařízení v případě, kdy agentní software není ve spojení s centrálním managementem.		Ano

Funkcionalita management	Popis funkce	Požadované funkční vlastnosti	Splnění daného požadavku
Typ nasazení managementu	Definuje, jestli bude managemnet nabízeného řešení nasazen v prostředí zákazníka nebo ve veřejně dostupném cloudovém prostředí. Dodavatel zvolí, jaký typ nasazení zadavateli nabídne.	On-premise	NE
		Cloud	ANO
XDR platforma	Systém nabízí možnosti shromažďovat, analyzovat a korelovat data z různých bezpečnostních nástrojů, minimálně z firewallu, EDR a NDR.		NE
Forenzní analýza	Získání aktuálních informací z koncového zařízení pro forenzní analýzu. Pokytuje platformu pro vyšetřování incidentu za účelem identifikace root cause, pochopení způsobu nakažení, metody průniku a sběr důkazů pro technologické i právní potřeby.	Administrativně jednoduché generování forenzního balíčku z vybraného zařízení. Výstupem bude lidsky čitelný soubor nebo jejich kolekce obsahující nejméně: seznam procesů, registrů, seznam otevřených síťových spojení, seznam uživatelů, jejich oprávnění, členství ve skupiných a stáří účtů, seznam služeb, auditní logy, seznam naplánovaných úloh, dns cache, na platformě Windows kompletní kopii registrů.	NE
Reportování	Generuje souhrnné reporty. Nabízí analytické a managerské přehledy za účelem poskytnutí celkového přehledu stavu chráněného prostředí s detailním pohledem na bezpečnostní incidenty, trendy hrozeb, soulad s předpisy a standardy, aktuálním stavem koncových stanic apod. ve formátu PDF.	Poskytuje předdefinovanou sadu základních reportů výrobce o stavu chráněného prostředí.	ANO
Notifikace	Systém musí být schopný zasílat notifikace určeným osobám v případě zjištění bezpečnostních nebo provozních událostí.	SMS	NE
Znalostní báze útočných technik a taktik	Systém automaticky mapuje identifikované události na techniky a taktiky aktuální verze MITRE frameworku. U identifikovaných událostí může obohacovat informace o odkazy na znalostní bázi aktuálního MITRE frameworku a/nebo vlastní znalostní báze útočných technik a taktik.	U identifikovaných hrozeb poskytuje přímý odkaz na příslušnou techniku nebo taktiku MITRE frameworku.	ANO
		U identifikovaných hrozeb poskytuje přímý vstup do vlastní znalostní báze výrobce s podrobnými doplňujícími informacemi o identifikované hrozbě.	ANO
Import definice hrozeb a pravidel	Umožňuje manuální import typů indikátorů hrozeb.	IoA	ANO
		IoC (nejméně URL, IP, doménové jméno, e-mailová adresa)	ANO
	Umožňuje manuální import detekčních pravidel ve formátech.	YARA	NE
		XML	NE
Integrace	Management umožňuje formou přímé podpory nebo instalací oficiálních pluginů integraci s dalšími bezpečnostními a provozními produkty provozovanými v prostředí zadavatele. Funkcionalita musí být k dispozici formou jednoduché integrace bez nutnosti objednávky dodatečných servisních MD na zprovoznění.	FW CheckPoint	ANO
		NDR GrayCortex	ANO
Lokalizace systému	Lokalizace produktu do českého pracovního prostředí.	Prostředí managementu je v českém jazyce.	NE
Granulární správa přístupů	Centrální konzole umožňuje granulární řízení přístupů a oprávnění uživatelů.	Řízení přístupu na základě AD skupin.	NE
Podpora MS AD	Podporuje vyčítání objektů (uživatelů, skupin, koncových bodů) z lokálního Active Directory za účelem tvorby inventáře a ověřování administrátorů do konzole pro centrální správu.		NE
Správa verzí agentního software	Agentní software je spravovaný výhradně z centrální konzole, agentní sofware není možné modifikovat ani s oprávněním lokálního administrátora.	Downgrade agentního software.	ANO
Zálohy	Možnost zálohování získaných metadat/telemetrie do prostředí zadavatele.		ANO
AI analytika	Systém má dostupné rozhraní založené na LLM pro zadávaní dotazů v přirozeném jazyce. Na základě vstupů provede překlad do syntaxe/query jazyka systému a uživateli vrátí analýzu obsahující požadované informace. Uživatel musí být schopný upřesnit původní dotaz, kdy systém toto upřesnění zpracuje a doplní původní analýzu o nové informace.	Systém má dostupné rozhraní pro zadávaní libovolných dotazů v přirozeném jazyce.	NE
		Dotazy mohou být pokládany v českém jazyce.	NE
		Systém disponuje inventářem pro ukládaní dříve položených dotazů.	NE
		Položky výše zmíněného inventáře mohou být sdíleny s dalšími uživateli systému.	NE

Funkcionalita koncové zařízení	Popis funkce	Požadované funkční vlastnosti	
Antimalware	Scany nově připojených externích a síťových diskových zařízení.		NE
Ochrana proti ransomware	Disponuje detekčními mechanismy na identifikaci a zastavení neznámého ransomware. V případě nákazy zařízení prostřednictvím ransomware nebo wiperu umožnuje automatický rollback infikovaných/zničených souborů do původního stavu.	Linux RHEL7+	ANO
		MacOS 12+	ANO
Firewall	Možnost řízení síťového provozu pomocí definování vlastních pravidel.		NE
	Možnost aplikace pravidel na skupiny zařízení.		NE
	Detekce připojení uvnitř nebo mimo organizaci s definicí pravidel na základě této informace.		NE
Web Protection	URL filtering		NE
	Kategorizace vlastních URL		NE
	Výjimky z filtračních politik pro skupiny zařízení minimálně pro metody allow a block		NE
	Blokace drive-by download		NE
	Anti-phising kontrola formulářů		NE
Kontrola periferií	Šifrování paměťových medií koncového zařízení.		NE
	Kontrola oprávnění pro instalaci software na koncovém zařízení.		NE

Řízení aplikací	Kontrola spouštění aplikací s možností definovat vlastní allow list. Allow list musí být možné definovat minimálně na základě těchto parametrů: cesty k souboru, názvu souboru, výstupu hashovací funkce SHA256, digitálního podpisu a identifikace výrobce software.		NE
HIPS	Detekuje a blokuje pokusy o známé i neznámé útoky na úrovni síťové komunikace.		ANO
	Využívá technologie virtuálního záplatování zranitelností.		NE
	Detekuje a blokuje pokusy o průzkumné scany (reconnaissance).		ANO
	Umožňuje importovat a definovat vlastní IPS pravidla.		NE
DNS protection	Identifikuje dotazy na škodlivé domény a dokáže v reálném čase zajistit zablokování překladu.		NE
Sandboxing	Automatické zasílání podezřelých souborů do on-premise sandboxu.		ANO
	Manuální zasílání souborů do sandboxu běžným uživatelem koncového zařízení.		NE