Kupní smlouva

(dále jen „smlouva“)

dle § 2079 a násl. zákona č. 89/2012 Sb., občanského zákoníku,
ve znění pozdějších předpisů (dále jen „**občanský zákoník**“)

1. Smluvní strany

1.1.	**Kupující:**	**Město Krnov**
	se sídlem:	Hlavní náměstí 96/1 Pod Bezručovým vrchem, 794 01 Krnov 1
	zastoupen:	Mgr. Tomášem Hradilem, starostou
	Identifikační číslo:	00296139
	DIČ:	CZ00296139
	(dále jen jako „**kupující**“)	
1.2.	**Prodávající:**	**awin IT, s. r. o.**
	se sídlem:	Nad Šutkou 540/14, Kobylisy, 182 00 Praha 8
	zastoupen:	Jindřich Rosička
	zástupce ve věcech technických:	René Kmoch
	IČ:	03173631
	Bankovní spojení:	225668183/0600
	Telefon:	+420 778 058 033
	E-mail:	info@awinit.cz
	(dále jen jako „**prodávající**“)	

Obě smluvní strany po vzájemném projednání a shodě uzavírají tuto smlouvu:

2. Předmět smlouvy

2.1. Účelem této smlouvy je dodávka zařízení včetně jeho implementace a napojení na ostatní infrastrukturu kupujícího (včetně současně budované infrastruktury) a následné předání funkčního kompletu kupujícímu, zaškolení administrátorů, uživatelů, rozvoje a podpory. Zařízení je určené pro kupujícího (Město Krnov) a pro jeho organizace.

2.2. Podkladem pro uzavření této smlouvy je nabídka prodávajícího, podaná v zadávacím řízení nazvaném **„V 00855 – Krnov – ochrana sítě před kybernetickými hrozbami“, část 3** (dále jen „Veřejná zakázka“), zadávaném přiměřeně dle Metodického pokynu pro oblast zadávání zakázek pro programové období 2021 – 2027 vydaného Ministerstvem pro místní rozvoj (dále jen „Pravidla“) a dle § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění.

2.3. Touto smlouvou se prodávající zavazuje dodat za podmínek v ní sjednaných kupujícímu zboží, uvedené v článku 3. této smlouvy a převést na něj vlastnické právo k tomuto zboží.

2.4. Kupující se zavazuje zboží převzít a zaplatit za něj sjednanou kupní cenu způsobem a v termínu stanoveném touto smlouvou.

2.5. Předmět plnění bude spolufinancován z dotačního projektu **„Krnov – ochrana sítě před kybernetickými hrozbami“, reg. č. CZ.31.2.0/0.0/0.0/23_093/0009763**, financovaného z Národního plánu obnovy (dále jen „Projekty“).

3. Předmět koupě

3.1. Předmětem smlouvy je **pořízení a implementace Endpoint protection řešení**, jehož specifikace včetně technických parametrů je uvedena v příloze č. 1 této smlouvy (dále jen „zboží“).

3.2. Součástí předmětu koupě jsou i veškeré doklady požadované právními předpisy k používání předmětu koupě - zboží. Prodávající prohlašuje, že předmět koupě splňuje veškeré podmínky stanovené právními předpisy k jeho používání, a že kupujícímu předá veškeré doklady potřebné k provozování předmětu koupě, za což kupujícímu ručí.

3.3. Předmětem koupě dle této smlouvy je dále:

- doprava do místa plnění,
- implementace, tj. veškeré nezbytné práce jejichž smyslem je zprovoznění včetně zapojení do stávajícího prostředí kupujícího tak, aby je kupující mohl užívat obvyklým způsobem (dále jen „implementace“),
- předání průvodní dokumentace,
- zaškolení kupujícího,
- testovací provoz,
- nezbytná technická podpora po dobu udržitelnosti Projektu, která činí 5 let od data předání do provozu. Technická podpora zahrnuje zejména aktualizace SW, maintenance, legislativní upgrade a update (dále jen „technická podpora“). Podrobné podmínky poskytování technické podpory jsou uvedeny v příloze č. 2 této smlouvy.

4. Kupní cena a platební podmínky

4.1. Celková kupní cena činí:

2 999 848 Kč bez DPH

629 968,08 Kč DPH

3 629 816,08 Kč vč. DPH

4.2. Cena bez DPH podle čl. 4.1. této smlouvy je stanovena dle technické specifikace (Příloha č. 1 této smlouvy) jako cena nejvýše přípustná a konečná a zahrnuje celý předmět plnění dle této smlouvy (s výjimkou ceny za poskytování technické podpory, která je upravena v čl. 4.5. níže).

4.3. Sjednaná cena celkem může být změněna pouze v případě změny zákona č. 235/2004 Sb., o DPH, týkající se sazby DPH a v souvislosti s ustanoveními § 222 zákona č. 134/2016 Sb., o zadávání veřejných zakázek.

4.4. Kupující se zavazuje zaplatit kupní cenu na základě faktur, vystavených prodávajícím a doručených kupujícímu dle níže uvedeného mechanismu:

- Prodávající vystaví zálohovou fakturu na 70 % z kupní ceny dodaného zboží po oboustranném podpisu zápisu o dodání zboží.
- Prodávající vystaví fakturu na 30 % z celkové kupní ceny po oboustranném podpisu předávacího protokolu (tj. po předání a převzetí zboží do plného provozu).

4.5. Cena za technickou podporu po předání zboží do provozu je stanovena dohodnou smluvních strany na:

19 354 Kč bez DPH za 1 měsíc

4 064,34 Kč DPH

23 418,34 vč. DPH za 1 měsíc

4.6. Úhrada ceny za technickou podporu bude probíhat na základě měsíčně vystavované faktury. Datum uskutečnitelného zdanitelného plnění je sjednáno na poslední kalendářní den v měsíci.

4.7. Faktury musí splňovat náležitosti daňového dokladu podle § 28 zákona č. 235/2004 Sb., o DPH, bude obsahovat cenový rozpad dle jednotlivých položek dle přílohy č. 1 této smlouvy a bude obsahovat číslo a název dotačního projektu (konkrétně bude uveden text ve znění: *Projekt **„Krnov – ochrana sítě před***

kybernetickými hrozbami", reg. č. CZ.31.2.0/0.0/0.0/23_093/0009763*, je spolufinancován z Národního plánu obnovy*) a bude zaslána prodávajícím na adresu kupujícího. **Splatnost faktury činí 30 kalendářních dní.**

4.8. Kupující bude oprávněn před uplynutím lhůty splatnosti vrátit prodávajícímu bez zaplacení fakturu, která nebude obsahovat některou náležitost uvedenou v této smlouvě, případně bude mít jiné závady v obsahu nebo bude uvedeno bankovní spojení a číslo účtu prodávajícího v rozporu s touto smlouvou anebo tyto náležitosti budou uvedeny chybně. U vrácené faktury musí kupující vyznačit důvod vrácení. Prodávající je povinen podle povahy nesprávnosti fakturu opravit nebo nově vyhotovit. Kupujícímu vrácením faktury přestává běžet původní lhůta splatnosti. Celá lhůta splatnosti běží znovu ode dne doručení opravené nebo nově vyhotovené faktury kupujícímu.

4.9. Platby budou zásadně probíhat bezhotovostní formou na bankovní účet prodávajícího uvedený ve smlouvě. Změnu bankovního spojení a čísla účtu prodávajícího bude možno provést pouze písemným dodatkem k této smlouvě nebo písemným sdělením prokazatelně doručeným kupujícímu, nejpozději spolu s příslušnou fakturou.

4.10. Faktura se považuje za včas uhrazenou, pokud je fakturovaná částka odepsána z účtu kupujícího.

5. Místo a doba plnění a dodací podmínky

5.1. Místem plnění je sídlo zadavatele.

5.2. Prodávající je povinen dodat veškeré zboží **nejpozději do 75 dní od účinnosti této smlouvy**. Kupující umožňuje postupné dodání zboží po částech.

5.3. Dodávka se považuje podle této smlouvy za dodanou, pokud bylo:

- zboží řádně dodáno včetně příslušné dokumentace (k instalaci, nastavení, zabezpečení jednotlivých komponent a včetně návrhu plánu obnovy).
- provedena instalace, implementace (případné podrobné specifické podmínky implementace jsou uvedeny v příloze č. 1 smlouvy) a úspěšně vyzkoušena funkčnost,
  - činnost u níž se nepředpokládá žádný výpadek služeb lze provádět v pracovní době MÚ
  - činnost u které se obě strany shodnou že předpokládaný výpadek bude kratší než 10 min lze provádět mimo úřední hodiny.
  - činnosti s výpadkem delší se mohou provádět pouze mimo pracovní dobu MÚ. Termín odstávky musí být znám alespoň týden předem
  - termín školení uživatelů určený předem.
  - školení OIT může probíhat v průběhu instalace.
- součástí instalace bude následný testovací provoz provedený bez zbytečného odkladu v délce nutné pro ověření funkčnosti dodaného HW a SW. Náplň testovacího provozu bude následující:
  - zahoření a ověření funkčnosti HW zařízení
  - ověření vzájemné spolupráce jednotlivých HW zařízení
  - ověření napojení na LAN síť zadavatele
  - provedení zátěžových testů
  - ověření chování systému při výpadku některého ze zařízení (ověření vysoké dostupnosti)
  - ověření chování systému při výpadku el. energie

5.4. Po dodání zboží v částech **2 a 3 zakázky** proběhne **audit kybernetické bezpečnosti**.

5.5. V rámci auditu kybernetické bezpečnosti dojde k prověření funkčnost technických opatření a celkové bezpečnosti dodávky pomocí jejího otestování. Otestování provede 3. osoba zvolená kupujícím, a to nejpozději do 14 dní od dodání zboží v částech 2 a 3 této veřejné zakázky, přičemž toto otestování bude trvat maximálně 60 dní. V návaznosti na dokončení auditu kybernetické bezpečnosti prodávající napraví nalezené chyby bránící užívání dle účelu smlouvy, a to nejpozději do 14 dní od okamžiku, kdy obdrží výsledek auditu kybernetické bezpečnosti.

5.6. Po splnění dodávky zboží bude vyhotoven **zápis o předání a převzetí zboží**, který bude obsahovat níže uvedené náležitosti:
- název a sídlo prodávajícího a kupujícího,
- označení dodaného zboží včetně výrobního čísla,
- datum dodání,
- číslo a název dotačního projektu (konkrétně bude uveden text ve znění: *Projekt **„Krnov – ochrana sítě před kybernetickými hrozbami“, reg. č. CZ.31.2.0/0.0/0.0/23_093/0009763** je spolufinancován z Národního plánu obnovy*).

5.7. Zápis o předání a převzetí zboží podepíší oprávnění zástupci obou smluvních stran, přičemž podpisem zápisu o předání a převzetí dochází k převzetí a předání zboží a ke splnění předmětu koupě.

6. Odpovědnost za vady, záruka za jakost, servis

6.1. Prodávající nese odpovědnost za to, že zboží dodané a předané podle této smlouvy je ke dni dodání plně funkční a splňuje technické parametry uvedené této smlouvě. Prodávající přejímá níže uvedenou záruku za jakost zboží dodaného podle této smlouvy. Záruční doba počíná běžet dnem oboustranného podpisu zápisu o předání a převzetí zboží. **Záruční doba pro jednotlivé položky v souladu s přílohou č. 1 této smlouvy činí 60 měsíců** ode dne předání a převzetí zboží.

6.2. Záruka se nevztahuje na spotřební materiál a na vady způsobené zaviněným jednáním kupujícího anebo způsobené vyšší mocí.

6.3. Kupující se zavazuje respektovat pokyny prodávajícího v oblasti údržby a používání správných pracovních postupů.

6.4. Technická podpora a servis budou poskytovány minimálně po celou dobu udržitelnosti projektu (tj. min. 60 měsíců ode dne předání do provozu).

6.5. Technická podpora a servis budou realizovány v sídle kupujícího. Výjimku tvoří činnosti realizovatelné vzdáleným připojením.

6.6. V případě nahlášení závady prodávajícímu bude oprava provedena vzdáleně či na místě nejpozději následující pracovní den od jejího nahlášení. V případě nemožnosti opravy následující pracovní den nabídne prodávající kupujícímu alternativu (tj. náhradní řešení) na dobu trvání opravy. V případě záruční opravy (tj. pokud se nejedná o vadu způsobenou zaviněným jednáním kupujícího anebo způsobenou vyšší mocí), není kupující povinen hradit náklady na cestovné servisních techniků ke kupujícímu a zpět, tyto náklady nese prodávající.

6.7. Nahlášení závady bude provedeno prostřednictvím e-mailu zaslaného na e-mailovou adresu it@awinit.cz, telefonicky na tel. číslo +420 778 058 033 prostřednictvím elektronické oznamovací služby (tzv. HelpDesku) nebo prostřednictvím vzdáleného připojení na PC uživatele / server.

6.8. Telefonická, e-mailová podpora a podpora prostřednictvím vzdáleného připojení bude k dispozici minimálně v pracovních dnech od 8 do 16 hod.

6.9. Služba HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 7x24 hod (s výjimkou předem nahlášených servisních zásahů při správě systému HelpDesk).

6.10. Prodávající se v záruční době zavazuje zajistit dostupnost náhradních dílů a spotřebního materiálu.

6.11. Veškeré záruční a servisní podmínky, uvedené v tomto článku 6. smlouvy, platí pouze tehdy, **pokud není v rámci technické specifikace v příloze č. 1 této smlouvy pro konkrétní produkty uvedeno jinak**. (Resp. odlišná úprava záručních a servisních podmínek v příloze č. 1 této smlouvy má před tímto čl. 6 smlouvy přednost.)

6.12. Podrobné podmínky poskytování technické podpory jsou upraveny v příloze č. 2 této smlouvy.

7. Smluvní pokuta a úrok z prodlení

7.1. Smluvními stranami bylo ujednáno, že pokud bude kupující v prodlení s úhradou ceny plnění ujednané podle této smlouvy, je kupující povinen zaplatit úrok z prodlení ve výši 0,05 % z dlužné částky za každý, byť i započatý kalendářní den prodlení.

7.2. Ocitne-li se prodávající v prodlení s plněním podle této smlouvy dle čl. 5.2, či 5.5., je povinen zaplatit kupujícímu smluvní pokutu ve výši 0,05 % z kupní ceny, a to za každý, byť i započatý kalendářní den prodlení se splněním dodávky.

7.3. Ocitne-li se prodávající v prodlení s plněním dle čl. 6.6. této smlouvy, je povinen zaplatit kupujícímu smluvní pokutu ve výši 500,- Kč za každý započatý den prodlení s dokončením servisní opravy dle čl. 6.6.

7.4. Uplatněním nároku na smluvní pokutu dle této smlouvy není dotčen nárok na náhradu škody.

7.5. Smluvní pokuta je splatná ve lhůtě 30 dnů od doručení jejího vyúčtování povinné smluvní straně z této smluvní pokuty.

8. Doba trvání smlouvy, ukončení smlouvy

8.1. Tato smlouva se uzavírá na dobu určitou, nejdéle do doby splnění závazku dle této smlouvy (tj. do okamžiku ukončení poskytování nezbytné technické podpory, resp. do doby uplynutí 5 let od data předání zboží do provozu).

8.2. Od této smlouvy může smluvní strana dotčená porušením povinnosti jednostranně odstoupit pro podstatné porušení této smlouvy, přičemž za podstatné porušení této smlouvy se zejména považuje:

a) na straně kupujícího – nezaplacení kupní ceny podle této smlouvy ve lhůtě delší 14 dní po dni splatnosti příslušné faktury,

b) na straně prodávajícího – prodlení s dodáním zboží o více než 14 dní po termínu dodání dle čl. 5.2. či dodání nefunkčního zboží, nesplňujícího požadavky čl. 3 této smlouvy, marné uplynutí sjednané lhůty pro vyřízení záruční opravy dle čl. 6.6. či prodlení s opravou chyb bránících užívání zboží dle účelu smlouvy, nalezených v rámci auditu kybernetické bezpečnosti, a to o více než 14 dní po termínu dle čl. 5.5. této smlouvy.

8.3. Smluvní strana porušením povinnosti dotčená je povinna odstoupení od smlouvy písemně oznámit druhé smluvní straně.

9. Ostatní ujednání

9.1. Smluvní strany se dohodly, že vlastnické právo k dodanému předmětu smlouvy nabývá kupující okamžikem převzetí zboží od prodávajícího.

9.2. Nebezpečí škody na zboží přechází z prodávajícího na kupujícího okamžikem převzetí zboží od prodávajícího či okamžikem, kdy kupujícímu bylo umožněno zboží převzít a ten jej nepřevzal.

9.3. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých vzájemných závazků. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této smlouvy.

9.4. Smluvními stranami bylo ujednáno, že veškeré informace, jež si navzájem poskytnou, jsou označeny jako důvěrné a žádná ze smluvních stran není oprávněna je poskytnout třetí osobě ani použít v rozporu s jejich účelem pro své potřeby.

9.5. Prodávající nesmí bez předchozího souhlasu kupujícího postoupit svá práva a povinnosti plynoucí ze smlouvy třetí osobě.

9.6. Kupující se zavazuje umožnit přístup určeným pracovníkům prodávajícího do prostoru svého objektu za účelem splnění této smlouvy (předání a převzetí zboží, servis a technická podpora).

9.7. Právní vztahy touto smlouvou neupravené, jakož i právní poměry z ní vznikající a vyplývající, se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanského zákoníku a dalšími právními předpisy České republiky.

9.8. Ujednává se, že případné spory vzniklé z této smlouvy budou účastníci řešit především vzájemnou dohodou. Pro řízení o případných sporných nárocích se ujednává příslušnost soudů. Rozhodným právem je právo České republiky.

9.9. Za písemnou formu výzvy nebo oznámení se pro účely této smlouvy pokládají oznámení učiněná elektronickou poštou na dohodnuté elektronické adresy.

9.10. Prodávající je povinen zajistit, že veškeré vlastnosti předmětu smlouvy, včetně jeho update, legislativních update, upgrade a legislativních upgrade budou po celou dobu účinnosti této smlouvy odpovídat obecně platným právním předpisům ČR.

9.11. Prodávající prohlašuje, že bude mít po celou dobu plnění předmětu smlouvy uzavřenu pojistnou smlouvu krytí odpovědnost za škodu způsobenou provozní činností s limitem pojistného plnění minimální výši kupní ceny zboží dle čl. 4.1., kterou se zavazuje kdykoliv na vyžádání předložit k nahlédnutí kupujícímu.

10. Závěrečná ustanovení

10.1. Prodávající je povinen umožnit všem subjektům oprávněným k výkonu kontroly projektu, z jehož prostředků je dodávka hrazena, provést kontrolu dokladů souvisejících s plněním zakázky, a to po dobu danou právními předpisy ČR k jejich archivaci (zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů).

10.2. Prodávající je povinen uchovávat veškerou dokumentaci související s realizací plnění dle Smlouvy včetně účetních dokladů po dobu deseti let od finančního ukončení projektu s názvem **„Krnov – ochrana sítě před kybernetickými hrozbami“, reg. č. CZ.31.2.0/0.0/0.0/23_093/0009763**, minimálně však do konce roku 2037. Pokud je v českých právních předpisech stanovena lhůta delší, musí ji poskytovatel použít.

10.3. Prodávající je povinen uvádět povinné prvky publicity podle podmínek strukturálních fondů EU na všech tištěných dokumentech vytvořených v souvislosti s předmětem koupě (nevztahuje se na interní účetní dokumentaci apod.). Tyto povinné prvky publicity sdělí a poskytne prodávajícímu na vyžádání kupující.

10.4. Prodávající je povinen při kontrole poskytnout na vyžádání kontrolnímu orgánu daňovou evidenci v plném rozsahu. **Prodávající je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinou spolupůsobit při výkonu finanční kontroly.**

10.5. Prodávající se zavazuje umožnit osobám oprávněným k výkonu kontroly projektu, z něhož je veřejná zakázka hrazena, provést kontrolu dokladů souvisejících s plněním zakázky, a to po dobu nejméně 10 let od ukončení financování díla způsobem, který je v souladu s platnými právními předpisy České republiky a Evropských společenství.

10.6. Prodávající je povinen minimálně do konce roku 2037 poskytovat požadované informace a dokumentaci související s realizací projektu, z něhož je Veřejná zakázka hrazena, zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.

10.7. Prodávající bere na vědomí, že úhrada ceny za předmět plnění bude provedena s využitím dotačních prostředků, získaných kupujícím a podléhajících kontrole z hlediska vykazování účelnosti jejich čerpání. Prodávající se zavazuje, že kupujícímu nahradí veškeré škody a náklady, které mu vzniknou nebo budou muset být vynaloženy, pokud z důvodu porušení této smlouvy prodávajícím vznikne kupujícímu závazek vrátit dotaci nebo její část, poskytnutou na úhradu ceny za předmět plnění, jejímu poskytovateli, a to i včetně penále případně vyměřeného jako důsledek porušení pravidel nakládání s veřejnými prostředky. To platí obdobně, pokud prodávající znemožní řádný výkon kontroly orgánům, oprávněným ke kontrole účelnosti vynaložení dotačních prostředků, resp. nepředloží jimi požadované doklady.

10.8. Prodávající se zavazuje během plnění smlouvy i po jejím ukončení smlouvy zachovávat mlčenlivost o všech skutečnostech, o kterých se dozví od kupujícího v souvislosti s plněním smlouvy

10.9. Tuto smlouvu lze měnit nebo doplnit pouze dohodou smluvních stran, a to formou písemného číslovaného dodatku.

10.10. Smluvní strany prohlašují, že si tuto smlouvu přečetly, a že byla ujednána po vzájemném projednání podle jejich svobodné vůle, určitě, vážně a srozumitelně.

10.11. Prodávající se zavazuje k dodržování mezinárodních sankcí Evropské unie, přijatých v souvislosti s ruskou agresí na území Ukrajiny vůči Rusku a Bělorusku, zejména nařízení Rady EU č. 2022/576, nařízení Rady (EU) č. 269/2014 ve spojení s prováděcím nařízením Rady (EU) č. 2022/581, nařízení Rady (EU) č. 208/2014 a nařízení Rady (ES) č. 765/2006 nebo v jejich prospěch (dále jen „mezinárodní sankce EU“).

10.12. Smlouva je, v souladu s podmínkami zákona č. 134/2016 Sb., podepsána elektronicky.

10.13. Rada města Krnov souhlasila s uzavřením této smlouvy na svém jednání dne 10. 11. 2025 usnesením č. 3398/86/RM/2025.

10.14. Smlouva nabývá platnosti dnem podpisu a účinnosti dnem jejího uveřejnění v registru smluv. Uveřejnění smlouvy v registru smluv provede kupující.

10.15. Nedílnou součástí této smlouvy jsou následující přílohy:

Příloha č. 1 – Technická specifikace

Příloha č. 2 – Podmínky poskytování technické podpory

Prodávající:	Kupující:
V Praze dne dle data el. podpisu	V Krnově dne dle data el. podpisu
Jindřich Rosička Digitálně podepsal Jindřich Rosička Datum: 2025.12.02 09:31:34 +01'00'	
.....	.....
Jindřich Rosička	Mgr. Tomáš Hradil, starosta
Jednatel	Město Krnov

Příloha č. 1 – Technická specifikace

Dodané prvky musí fungovat jako platforma, tedy funkční celek, na které jsou kladeny následující požadavky. Funkční požadavky u jednotlivých částí dodávky jsou zpřesněním a mohou být duplicitní.

Pořízení a implementace ochrany

Parametr	Minimální požadavek	Splňuje ANO/NE[1]
Výrobce, název, verze a licenční program XDR	Sophos Central Device Encryption - 60 MOS 250 Sophos Central Zero Trust Network- 60 MOS 50 Sophos Central Mobile Advanced - 60 MOS 100 Sophos Central Intercept X Advanced withXDR - 60 MOS 250 Sophos Central Intercept X Advanced for Server with XDR - 60 MOS 20 Implementace 3 MD	
Licence	• Ochrana stanice 250 ks • Ochrana server 30 ks	ANO
Vlastnosti	• Správa všech poptávaných produktů (ochrana endpointů a serverů) z jednoho administračního rozhraní • Přístup do administračního rozhraní pomocí protokolu HTTPS • Centrální administrační rozhraní musí mít dokumentované API • Vícefaktorová autentifikace pro administrátory • Centrální administrace podporuje automatické odhlášení uživatele při nečinnosti • Centrální správa je poskytována online výrobcem v zabezpečeném datacentru (cloud) • Umístění zabezpečeného datacentra je možné zvolit v rámci lokality EU (je zahrnuto v ceně nabízené licence) • Centrální administrační rozhraní musí umožnit vytvoření dvoustupňové hieararchické struktury (celá organizace - podřízené organizace) • Administrátor celé organizace musí mít právo vytvářet podřízené organizace a přidělovat jim potřebné licence z rozsahu přiděleného celé organizaci • Administrátoři podřízených organizací mohou administrovat pouze svoji organizaci a její uživatele • Centrální administrace podporuje řízení uživatelů dle rolí a to minimálně v rozsahu: • Administrátor celé organizace - Může vytvářet nové podřízené organizace a přidělovat jim administrátory • Hlavní administrátor podřízené organizace - Má plná práva pro správu a může přidělovat role dalším uživatelům • Bežný administrátor podřízené organizace - Má plná práva pro správu • Pracovník technické podpory - Má práva pro čtení pro správu, může číst logy, může vyvolat sken a update uživatelského zařízení, spravuje výstrahy • Uživatel s přístupem pro čtení - Má práva pro čtení pro správu, logy a výstrahy	ANO

[1] Pozn. Účastník ve sloupci vyplní splnění závazných požadavků zadavatele (ANO/NE), případně doplní číselnou hodnotu požadovaného parametru. Účastník doloží závazných požadavků zadavatele rovněž odkazy na stránky výrobce, kde je možné požadovaný parametr ověřit (viz tabulka *„URL k dokumentaci technických parametrů“* níže). Účastník musí splňovat veškeré min. technické požadavky zadavatele.

	• Centrální administrace podporuje napojení na systémy SIEM a zasílání událostí typu Události a Výstrahy • Centrální administrace poskytuje vestavěné logování a reportování • Centrální adminsitrace podporuje zasílání alertů emailem na definované adresy • Centrální administrace disponuje souhrnným dashboardem, tedy místem, na kterém se zobrazují klíčové informace o celém prostředí	
Endpoint Protection	• Licence na uživatele bez ohledu na počet použitých zařízení – 250 uživatelů • Podpora OS Windows 11 a vyšší, MAC OS X 10.10 a vyšší • Kontrola a blokování HW zařízení - USB disky, externí HDD/SSD, CD/DVD, Wi-Fi, Bluetooth, Infrared, Modemy • Kontrola a blokování aplikací, nejméně 30 předdefinovaných kategorií • Detekce malware pomocí strojového učení Deep Learning • Skenování souborů proti malware (lokální i vzdálené soubory) • Skenování archivů • Signatury AV dostupné v reálném čase v Cloudu, nezávislost na četnosti aktualizace databáze • Analýza chování před spuštěním souboru (HIPS) • Blokování potenciálně nechtěných aplikací (PUA) • DLP - blokování přenosu dat na základě pravidel, možnost úplné blokace nebo upozornění uživatele a vyžádání potvrzení • Analýza chování při běhu procesů • Aktivní zamezení negativních dopadů zneužití zranitelností • Blokování neautorizovaného šifrování (kryprovirus) dat • Automatická obnova souborů do původního stavu před zašifrováním • Ochrana prohlížeče před injektáží kódu • Automatické odstranění malware • Automatické odstranění zbytkových souborů (čištění registrů) po zablokování malware • Určení zdroje a příčiny útoku, grafická reprezentace děje útoku • Ochrana proti zásahu uživatele s lokálními admin. právy do nastavení klienta • Detekce pomocí strojového učení bez nutnosti připojení k internetu • Zjednodušený náhled na nákazu minimálně v rozsahu, vstupní bod malware do systému (aplikace), malware, přijaté opatření • Grafické znázornění průběhu nákazy minimálně v rozsahu, vstupní bod malware do systému (aplikace), zápisy do systému a do registrů OS, komunikace na internet včetně zobrazí IP a URL adres • Možnost globálního vyčištění a blokování nalezeného malware na všech systémech najednou (pomocí jedné akce). • Automatické vyhodnocení incidentů • Zobrazení obecných informací o proběhnutých útocích (alespoň z poslední doby)minimálně v rozsahu jméno malware, počet postižených systémů a hodnocení nebezpečnosti malware výrobcem. • Možnost dešifrace a kontroly HTTPS provozu	ANO

	• Application lockdown (Web Browser, Java, Media, Office) • Součástí řešení je lehký klient na koncové stanice • Řešení poskytuje zázemí pro threat hunting • Možnost terminálového připojení na endpoint z centrální správy na úrovni systému • Možnost spouštění SQL dotazů vůči endpointům pro aktivní vyhledávaní hrozeb (minimálně 290 před definovaných dotazů) • Automatická nebo manuální izolace koncového zařízení (např. při napadení malwarem) • Správa Windows Firewall	
Server Protection	• Podpora OS Windows Server 2019 a vyšší, Amazon Linux 2, CentOS 7/Minimal/Stream, Red Hat Enterprise Linux 7/8, Ubuntu 18.04/20.04/Minimal • Podpora Windows Remote Desktop Services • Podpora MS Azure a Amazon Web Services • Blokování škodlivých webových stránek • Kontrola souborů dle reputace • Webová kontrola / Blokování URL na základě kategorie (nejméně 10 předdefinovaných kategorií) • Kontrola a blokování HW zařízení - USB disky, externí HDD/SSD, CD/DVD, Wi-Fi, Bluetooth, Infrared, Modemy • Kontrola a blokování aplikací, nejméně 40 předdefinovaných kategorií • Whitelistening aplikací • Správa Windows Firewall • Možnost bezagentového skenování virtuálních prostředí VMware a Hyper-V • Detekce malware pomocí strojového učení Deep Learning • Automatické výjimky ze skenování • Skenování souborů proti malware • Skenování archivů • Signatury AV dostupné v reálném čase v Cloudu, nezávislost na četnosti aktualizace databáze • Analýza chování před spuštěním souboru (HIPS) • Blokování potenciálně nechtěných aplikací (PUA) • DLP - blokování přenosu dat na základě pravidel, možnost úplné blokace nebo upozornění uživatele a vyžádání potvrzení • Analýza chování při běhu procesů • Aktivní zamezení negativních dopadů zneužití zranitelností • Blokování neautorizovaného šifrování (kryptovirus) dat • Automatická obnova souborů do původního stavu před zašifrováním • Ochrana prohlížeče před injektáží kódu • Automatické odstranění malware • Automatické odstranění zbytkových souborů (čištění registrů) po zablokování malware • Určení zdroje a příčiny útoku, grafická reprezentace děje útoku • Ochrana proti zásahu uživatele s lokálními admin. právy do nastavení klienta • Uzamčení stavu serveru z pohledu aplikací a služeb • Zjednodušený náhled na nákazu minimálně v rozsahu, vstupní bod malware do systému (aplikace), malware, přijaté opatření	ANO

	• Grafické znázornění průběhu nákazy minimálně v rozsahu, vstupní bod malware do systému (aplikace), zápisy do systému a do registrů OS, komunikace na internet včetně zobrazí IP a URL adres • Možnost globálního vyčištění a blokování nalezeného malware na všech systémech najednou (pomocí jedné akce). • Automatické vyhodnocení incidentů • Zobrazení obecných informací o proběhnutých útocích (alespoň z poslední doby)minimálně v rozsahu jméno malware, počet postižených systémů a hodnocení nebezpečnosti malware výrobcem. • Možnost tzv. lockdownu zařízení, následně není možná instalace aplikací • Aktivní rozeznávání běžících aplikací • Možnost spouštění SQL dotazů vůči endpointům pro aktivní vyhledávaní hrozeb (minimálně 300 předdefinovaných dotazů) • Řešení poskytuje zázemí pro threat hunting • Řešení disponuje před-definovanými politikami dle best practices • Anti-Virus pro Linux servery (Amazon Linux/Amazon Linux 2, CentOS 7/8, Debian 9/10, Oracle Linux 7/8, RHEL 7/8, SUSE Linux Enterprise Server 12/15, Ubuntu 18LTS/20.04 LTS)	

Obecné požadavky na nabízené řešení

Předmětem je komplexní zabezpečení bezpečnosti dle níže uvedených specifikací.

A.) Zabezpečení koncových bodů

1.) Specifikace řešení

Předmětem je zabezpečení operačních systémů na koncových (uživatelských) počítačích a serverech.

Centrální správa řešení musí být v cloudu přes webové rozhraní a umístění se připouští pouze v EU. Součástí dodávky musí být veškeré potřebné programové vybavení, tj. všechny licence potřebné pro instalaci a provoz.

Podpora a záruka na dodaný software musí být 5 let pro následující prostředí:

Počet serverů (operačních systémů): 30

Počet stanic: 250

Počet stanic pro ochranu šifrováním: 250

Počet uživatelů: 250

Počet uživatelů ZTNA: 50

a.) Požadované funkce

(1) Základní požadavky

Požadované vlastnosti a funkce	POPIS	Splňuje ANO/NE
Podporované OS	Windows 11 a vyšší, Windows 2019 a vyšší, macOS, Linux Na OS macOS a Linux se připouští omezenější funkcionality než na OS Windows.	ANO
Podpora klientů pro operační systémy ve virtuálním prostředí v rozsahu popisu.	VMware vSphere a Microsoft Hyper-V	ANO
Integrace s Active Directory	- Synchronizace uživatelů a skupin je zajištěna pomocí služby, jež vyčítá informace z Active Directory a šifrovaným tunelem je synchronizuje do centrální správy. - Synchronizace uživatelů a skupin z Azure Active Directory. - S Active Directory komunikuje synchronizační služba pomocí služeb LDAPS (port 636) případně LDAP (port 389). - Synchronizační služba synchronizuje minimálně tyto parametry: Username, Login, Email address, skupiny a členy každé skupiny - Synchronizační služba musí podporovat LDAP filtry pro užší výběr synchronizovaných položek - Synchronizační služba musí podporovat manuální a intervalovou synchronizaci v definovaných časových intervalech	ANO

	- Mimo synchronizaci uživatelů a skupin z Active Directory musí řešení nabízet vytváření lokálních uživatelů a skupin	
Aktualizační cache a optimalizace komunikace	Komponenta zajišťující centrální stahování aktualizací a jejich redistribuci v rámci lokální sítě + komunikační proxy pro komunikaci s centrální správou	ANO
Instalace nových verzí klientů koncových klientů v rámci aktualizačního procesu (navíc k běžné aktualizaci bezpečnostních signatur).	Nesmí vyžadovat manuální aktualizaci programových komponent.	ANO
Klientskou část musí být možné skriptovat (například instalovat v režimu tiché instalace a instalovat novou verzi přímo z lokální cache)	-	ANO
Instalace (aktualizace) nových verzí centrální správy v ceně licencí po celou dobu platnosti licence	-	ANO
Logování bezpečnostních incidentů	Globální logování ze všech komponent software dostupné z centrální správy. Filtrace dle uživatele, počítače nebo skupin (uživatelů a počítačů)	ANO
Nastavení politik na úrovni skupina/uživatel/server	-	ANO
API rozhraní pro propojení s nástroji třetích stran	-	ANO
Dvoufázové ověřování při přihlášení do administrátorské konzole		ANO
Podpora českého jazyka	Minimálně pro klienta software na koncovém systému uživatele.	ANO

(2) Běžná antimalware kontrola

Požadované vlastnosti a funkce	**POPIS**	**Splňuje ANO/NE**
Rezidentní antimalware ochrana	Aktualizace min. 4 x denně	ANO
Heuristická analýza	-	ANO
Použití online signatur při výskytu podezřelých souborů	-	ANO
Skenování souborů před stažením z internetu	Před uložením na disk	ANO
Plánované skenování	-	ANO

Definice výjimek	Na plánovaný sken i anti-malware ochranu, a to minimálně na soubor, složku, proces, exploit, webovou stránku a C&C komunikaci.	ANO

(3) Proaktivní ochrana

Požadované vlastnosti a funkce	POPIS	Splňuje ANO/NE
Blokování C&C komunikace a komunikace typu Botnet	-	ANO
HIPS (Host-Based IPS)	-	ANO
Kontrola zařízení (minimálně USB vyjímatelná zařízení, USB šifrovatelná vyjímatelná zařízení, optická média, bluetooth, multimediální zařízení, Wi-Fi)	Pro každé ID zařízení nebo modelovou řadu zařízení musí být možnost zvlášť zvolit akce (povolit, pouze monitorovat, blokovat).	ANO
Data Loss Prevention	Blokace přenosů dat na základě datového typu a obsahu souboru.	ANO
Aplikační kontrola	Včetně možnosti samostatného monitorování výskytu nepovolených aplikací a blokace aplikací z pravidelně aktualizovaného seznamu výrobce.	ANO
Ochrana přístupu na internet minimálně v rozsahu,	• **Blokování škodlivých webových stránek** • **Kontrola souborů dle reputace** • **URL filtrování (30+ kategorií, Data Loss, blokování přístupů na veřejné emailové portály).**	ANO
Zabezpečení při spouštění OS	• **Detekce a odstranění rootkitů** • **Ochrana Master Boot Record před zašifrováním**	ANO

(4) Ochrana nové generace

Požadované vlastnosti a funkce	POPIS	Splňuje ANO/NE
Anti – Exploit	Požadována ochrana blokování útoků využívajících zranitelností v operačním systému nebo aplikacích.	ANO
Ochrana před známými typy průniků	Detekce a prevence známých i neznámých exploitů, nezávislá na signaturách Ochrana minimálně před následujícími exploit technikami: ○ Enforce Data Execution Prevention (DEP) ○ Mandatory Address Space Layout Randomization (ASLR) ○ Bottom Up ASLR ○ Null Page (Null Dereference Protection) ○ Heap Spray Allocation ○ Dynamic Heap Spray	ANO

	○ Stack Pivot ○ Stack Exec (MemProt) ○ Stack-based ROP Mitigations (Caller) ○ Branch-based ROP Mitigations ○ Structured Exception Handler Overwrite Protection (SEHOP) ○ Import Address Table Filtering (IAF) ○ Load Library ○ Reflective DLL Injection ○ VBScript God Mode ○ WoW64 ○ Syscall ○ Hollow Process ○ DLL Hijacking ○ Shellcode a Dynamic Shellcode ○ APC Protection (Double Pulsar / AtomBombing) ○ Squiblydoo AppLocker Bypass ○ Process Privilege Escalation	
Anti – Exploit alespoň pro základní aplikace (MS Office, Java, Internetové prohlížeče apod.)	-	ANO
Anti – ransomware	Požadováno blokování i neznámých malware kategorie ransomware a crypto-Ransomware na základě funkce vyhledávání škodlivého šifrování vč. funkcionality roll-back (vrácení původních, již zašifrovaných souborů po zastavení Crypto-Ransomware) Funkcionalita zastavení síťového šifrování (přes počítačovou síť).	ANO
Přímá ochrana MBR	Například proti ransomware	ANO
Ochrana proti zvýšení oprávnění útočníka	-	ANO
Aplikační whitelisting pro servery	-	ANO
Ochrana proti přepisování kódu v paměti	-	ANO
Ochrana proti odcizení přihlašovacích údajů	-	ANO
Machine Learning technologie	Včetně analýzy důvodu označení za škodlivý kód a potlačení False Positive detekce antimalware	ANO
Automatické vyčištění systému na aplikační úrovni	-	ANO
Automatická izolace postižených stanic od sítě na úrovni klienta endpoint protection na koncovém systému uživatele.	-	ANO

(5) Ochrana dat šifrováním

Požadované vlastnosti a funkce	POPIS	Splňuje ANO/NE
Možnost šifrování pevných disků koncových stanic (min. Windows a Mac)	Včetně možnosti šifrovat pouze disk s OS	ANO
Podpora TPM	Bez nutnosti zadávat heslo před startem operačního systému	ANO
Podpora šifrování souborů	Možnost zašifrovat jednotlivé soubory na disku s ochranou heslem (pro zabezpečené sdílení dat)	ANO
Centrální přehled stavu šifrování na koncových bodech		ANO
Centrální záloha „dešifrovacích“ klíčů	Pro poskytnutí možnosti obnovy diskového oddílu	ANO

(6) XDR (Extended Endpoit Detection & Response)

Požadované vlastnosti a funkce	POPIS	Splňuje ANO/NE
Alertování	Při zachyceném incidentu vygenerování alertu	ANO
Průzkum incidentu na základě záznamu v systému XDR	Zobrazení a označení zdroje malware (kudy se malware dostal do sítě).	ANO
Zjednodušený náhled na nákazu	Minimálně v rozsahu, vstupní bod malware do systému (aplikace), malware, přijaté opatření	ANO
Grafické znázornění průběhu nákazy	Minimálně v rozsahu, vstupní bod malware do systému (aplikace), zápisy do systému a souborové úrovni a do registrů OS, komunikace na internet včetně zobrazí IP a URL adres, analýza souborů přes Machine Learning	ANO
Možnost globálního vyčištění a blokování nalezeného malware.	-	ANO
Automatické vyhodnocení incidentů	-	ANO
Zobrazení obecných informací o proběhnutých útocích (alespoň z poslední doby)	Minimálně v rozsahu jméno malware, počet postižených systémů a hodnocení nebezpečnosti malware výrobcem.	ANO
Podpora Threat Huntingu	Práce s koncovými systémy v reálném čase zasílání dotazů, příkazů apod. na koncové systémy přes XDR rozhraní pomocí vlastních a předdefinovaných dotazů (jejich rozsah záleží na výrobci).	ANO
Zpomalení koncových zařízení (čtení a zápis do souborového systému stanice)	Max. o 5 %	ANO
Možnost získávání dat do XDR z dalších zdrojů třetích stran.		ANO

B.) Zabezpečení mobilních zařízení

1.) Specifikace zabezpečení

Předmětem je řešení správy a zabezpečení mobilních systémů na koncových (uživatelských) počítačích a chytrých zařízeních tzv. Unified Endpoint Management včetně Mobile Security.

Software a jeho moduly musí být integrovány do jednoho celku s jednou a ochranou koncových bodů, tzn. centrální, společnou správou přes webové rozhraní. Součástí dodávky musí být veškeré potřebné programové vybavení, tj. všechny licence potřebné pro instalaci a provoz.

Podpora a záruka na dodaný software musí být 5 let pro následující prostředí:

Počet uživatelů mobilních zařízení: 100

a.) Požadované funkce pro chytrá zařízení

(1) Základní požadavky

Požadované vlastnosti a funkce	POPIS	Splňuje ANO/NE
Podporované klientské systémy	Android a iOS, IoT zařízení	ANO
Integrace s Active Directory		ANO
Stejný nástroj se musí využívat pro správu ochrany počítačů i chytrých zařízení.		ANO
Instalace nových klientů přes průvodce	Uživatelé musí mít možnost přidávat svá zařízení přes „uživatelských portál“	ANO
Instalace nových politik součástí instalace	Musí mít možnost proběhnout v jedné instalační úloze.	ANO
Instalace nových programů součástí instalace klienta	Musí mít možnost proběhnout v jedné instalační úloze.	ANO
Instalace (aktualizace) nových verzí centrální správy v ceně licencí po celou dobu platnosti licence		ANO
Podpora BYOD	Včetně možnosti oddělení politik pro zařízení organizace a vlastněných uživatelem	ANO
Skupinování a aplikace bezpečnostních politik minimálně na skupiny zařízení a jednotlivá zařízení		ANO
Výpis zařízení uživatele a jejich stavu pro každé zařízení.		ANO
Zobrazení výrobního (sériového) čísla a IMEI čísla chytrého zařízení v centrální správě	Především možnost pozdějšího dohledání v případě ztráty/odcizení zařízení.	ANO
Podpora Android Enterprise a Samsung Knox		ANO

Logování bezpečnostních incidentů	Globální logování ze všech komponent software dostupné z centrální správy. Filtrace dle uživatele, počítače nebo skupin (uživatelů a počítačů)	ANO

(2) Bezpečnost

Požadované vlastnosti a funkce	**POPIS**	**Splňuje ANO/NE**
Antimalware ochrana	Minimálně pro platformu Android	ANO
Machine learning (engine používající strojové učení)	Minimálně pro platformu Android	ANO
Webová filtrace (včetně URL filtrování)	-	ANO
Ochrana WIFI připojení	Minimálně kontrola bezpečnostni zvolené Wifi sítě	ANO
Možnost definice Wifi sítí	Zařízení bude poté mít předdefinovanou wifi síť včetně přístupového hesla	ANO
Možnost schvalování aplikací pro instalaci na koncovém zařízení	Možnost povolení stahování nových aplikací pouze přes Wifi	ANO
Skenování souborů stažených z internetu	Minimálně pro platformu Android	ANO
Plánované skenování	Minimálně pro platformu Android	ANO
Minimální délka a složitost hesla	Možnost nastavení politiky délky hesla a složitosti (použití speciální znaků, velká a malá písmena, číslice), podpora přihlášení pomocí gest a biometrického přihlášení (Face ID a otisk prstu)	ANO
Ochrana proti použití stejného hesla znovu		ANO
Automatický zámek po uplynuté době		ANO
Maximální stáří hesla		ANO
Vynucení šifrování zařízení		ANO
Možnost provádět geolokaci zařízení	Včetně auditní stopy (kdo a kdy zařízení vyhledával)	ANO
Funkce vzdáleného smazání dat v zařízení		ANO
Vynucení minimální verze OS		ANO
Možnost provedení resetování zařízení do továrního nastavení		ANO
Možnost zakázání kamery		ANO

(3) Správa zařízení

Požadované vlastnosti a funkce	**POPIS**	**Splňuje ANO/NE**
Podpora vzdálené instalace politik		ANO
Podpora vzdálené instalace aplikací	Z vlastního úložiště i za využití obchodů výrobce (Google Play a App Store)	ANO
Specifikace vyžadovaných software (například, antimalware, VPN klient apod.)		ANO
Možnost specifikace zakázaných software	Například přeinstalované aplikace od výrobce zařízení nebo nežádoucí aplikace.	ANO
Možnost exportu zařízení do xls	Export kvůli inventarizaci – minimálně v rozsahu: jméno zařízení, popis, druh hardware, verze OS, skupina, stav správy, nainstalované aplikace, sériové číslo.	ANO
Možnost rozšíření správy o Windows 11 a macOS.	Podpora těchto mobilních zařízení (notebooky).	ANO
Kontrola stavu zařízení a reportování	Reportování minimálně v rozsahu – odpovídá nebo neodpovídá požadavkům na zařízení	ANO

(4) Ostatní mobilní zařízení

Požadované vlastnosti a funkce	POPIS	**Splňuje ANO/NE**
Podporované klientské systémy	Windows 11 a novější, MacOS (na MacOS nemusí být dostupné všechny funkce níže)	ANO
Možnost nastavení politiky hesel		ANO
Zakázání změny základních systémových nastavení	Minimálně v rozsahu datum, čas, časová zóna, VPN nastavení	ANO
Zakázání sdílení internetu		ANO
Zakázání kamery, Bluetooth, SD karet		ANO
Zákaz manuální ostranění z managementu		ANO
Možnost správy (instalace certifikátů)		ANO
Možnost nastavení Wi-Fi		ANO

URL k dokumentaci technických parametrů[2]

URL odkazy na dokumentaci výrobce, dokládající technické parametry
https://www.sophos.com/en-us/legal/sophos-central-endpoint-and-server
https://assets.sophos.com/X24WTUEQ/at/q52k9f3bqkkt4gh5nkmt2crh/sophos-workload-protection-licensing-guide.pdf
https://www.sophos.com/en-us/legal/sophos-central-device-encryption
https://docs.sophos.com/central/ZTNA/startup/en-us/setup/index.html#sophos-cloud-gateway
https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/ManagingDevices/index.html

[2] Účastník zde v jednotlivých řádcích uvede URL odkazy, kterými bude dokumentovat výše uvedené technické parametry jím nabízeného předmětu plnění.

Příloha č. 2 – Podmínky poskytování technické podpory[3]

Monitoring spravovaných zařízení a služeb musí zajistit:

Nepřetržitý dohled

- Systém musí umožnit 24/7 monitoring spravované infrastruktury a okamžité hlášení incidentů.

Proaktivní přístup k řešení problémů

- Systém by měl identifikovat a hlásit anomálie, které mohou vést k výpadkům, ještě před jejich vznikem, a umožnit tak preventivní zásahy.

Přehledné rozhraní a reporting

- Dodavatel je povinen zajistit kupujícímu přístup k přehledným reportům o stavu spravovaných zařízení a služeb.
- Součástí reportů musí být informace o klíčových událostech, výpadcích a jejich řešení, jakož i statistiky využití a výkonu.

Kompatibilita se spravovanými zařízeními a službami

- Systém musí být plně kompatibilní s hardwarem a softwarem, které budou předmětem správy.

Bezpečnost a ochrana dat

- Dodavatel musí garantovat, že monitorovací systém bude splňovat bezpečnostní standardy a že veškerá data budou chráněna v souladu s platnou legislativou.

Kupující bude hlásit požadavky na služby následujícími způsoby:

- Do helpdesk systému dodavatele
- Kupující bude využívat Helpdesk systém poskytnutý dodavatelem pro evidenci a správu požadavků.
- Dodavatel musí zajistit přístup k Helpdesk systému pro autorizované osoby kupujícího.
- Systém musí umožňovat přehlednou evidenci požadavků, jejich aktuální stav a historii řešení.

Hlášení prostřednictvím e-mailu

- Kupující bude mít možnost hlásit požadavky na určenou e-mailovou adresu dodavatele.
- Dodavatel zajistí, aby e-mailové hlášení bylo automaticky zaevidováno v Helpdesk systému a označeno odpovídající prioritou.

Hlášení prostřednictvím telefonu

- V naléhavých případech, zejména u požadavků s vysokou prioritou, může kupující hlásit požadavky telefonicky na kontaktní číslo dodavatele.
- Telefonicky hlášené požadavky musí být následně zaevidovány v Helpdesk systému dodavatele.

Požadavky na Helpdesk systém dodavatele:

- Musí být k dispozici během pracovní doby (8 – 16 hodin)
- Dodavatel zajistí uživatelskou podporu při využívání Helpdesk systému.
- Systém musí umožnit automatické potvrzení přijetí požadavku.
- Evidence požadavků musí být přístupná kupujícímu pro kontrolu a zpětnou vazbu.

KVALITATIVNÍ PARAMETRY TECHNICKÉ PODPORY:

- **Minimalizace výpadků:** Služba bude poskytována tak, aby byly minimalizovány výpadky obchodní a provozní činnosti kupujícího způsobené spravovanou technikou.
- **Prioritní řešení:** Požadavky s přímým dopadem na produkt kupujícího budou řešeny nejpozději do 4 hodin v běžné pracovní době kupujícího.

REAKČNÍ DOBA TECHNIKŮ DODAVATELE V PRACOVNÍ DOBĚ (8:00 – 16:00):

- Priorita vysoká:

[3] V rámci této přílohy je prodávající označen rovněž jako „dodavatel“.

    - Situace: Vady zabraňující provozu, produkt není použitelný ve svých základních funkcích nebo se vyskytuje funkční závada znemožňující činnost systému. Tento stav může ohrozit běžný provoz Objednatele a nelze jej dočasně řešit organizačním opatřením.
    - Reakce: Okamžitá odezva technika, výjezd technika (nebo online zásah) do 8 hodin, řešení problému.
- Priorita střední:
    - Situace: Vady omezující provoz, funkčnost systému je ve svých funkcích degradována tak, že tento stav omezuje běžný provoz Objednatele. Jedná se také o vady způsobující problémy při užívání a provozování produktu nebo jeho části, ale umožňující provoz, jimiž způsobené problémy lze dočasně řešit organizačními opatřeními.
    - Reakce: Odezva technika do 8 hodin, řešení následující pracovní den.
- Priorita nízká:
    - Situace: Vady neomezující provoz, jedná se o drobné vady, které nespadají do kategorií „vysoká“ nebo „střední“.
    - Reakce: Řešení dle dohody při další návštěvě technika nebo do tří pracovních dnů vzdálenou správou.

Sankce za nedodržení kvalitativních požadavků:

- V případě prodlení Prodávajícího s odstraněním vad ve lhůtách stanovených v této příloze výše se Prodávající zavazuje Kupujícímu uhradit smluvní pokutu ve výši 200 Kč za každou hodinu prodlení v případě vad kategorie „priorita vysoká“ a smluvní pokutu ve výši 500 Kč za každý i započatý den prodlení v případě vady kategorie „priorita střední“, a to pro každý případ prodlení, není-li jinými ustanoveními této smlouvy výslovně uvedeno jinak.
- V případě, že Prodávající neumožní Kupujícímu zadat požadavek na servisní zásah z důvodu nedostupnosti služeb Hot-line ani HelpDesk, způsobené výpadkem uvedených služeb na straně Prodávajícího, je Kupující oprávněn po Prodávajícím požadovat smluvní pokutu ve výši 500 Kč za každý jednotlivý případ. To se netýká případu, kdy Prodávající provádí preventivní údržbu a na tuto skutečnost předem upozornil Kupujícího.
- Smluvní pokuty a úrok z prodlení jsou splatné do 30 dnů od doručení jejich vyžádání oprávněnou smluvní stranou straně povinné. Platby budou provedeny bezhotovostním bankovním převodem na účet oprávněné smluvní strany. Ujednání o smluvních pokutách se nedotýkají náhrady škody.
- Za podstatné porušení této smlouvy, pro něž může smluvní strana dotčená porušením povinnosti jednostranně odstoupit, se mimo jiné považuje:

    - neposkytnutí servisní podpory Prodávajícím, po řádném nahlášení požadavku Kupujícím, delší než 30 dní,
    - nedodržení doby odezvy nebo jiných dohodnutých termínů Prodávajícím o více jak 5 dnů,
    - bezdůvodné přerušení prací na servisním případu Kupujícího,
    - opakované nesplnění závazku Kupujícího poskytnout Prodávajícímu součinnost při plnění ustanovení této smlouvy i přes písemné upozornění doručené Kupujícímu.