LICENČNÍ SMLOUVA

Název:	**Česká republika – Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, organizační složka státu**
IČO:	48135267
DIČ:	Není plátcem DPH
Sídlo:	Biskupský dvůr 1148/5, 110 00 Praha 1
Zástupce:	Ing. Jiří Kratochvíl, předseda úřadu

(dále jen „**Objednatel**“)

a

Název:	ESET software spol. s r.o.
IČO:	26467593
DIČ:	CZ26467593
Sídlo:	Jankovcova 1037/49, 170 00 Praha 7
Zástupce:	Jan Urbík
Zápis v rejstříku:	25. červenec 2001
Bankovní spojení:	Citibank Europe plc, 2552930205/2600

(dále jen „**Dodavatel**“)

uzavírají, ve smyslu ustanovení § 2358 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**“), níže uvedeného dne, měsíce a roku tuto

licenční smlouvu
(dále jen „**smlouva**“)

1. Úvodní ustanovení

1.1. Dodavatel prohlašuje, že má dostatečné zkušenosti a schopnosti, aby řádně a včas poskytl Objednateli plnění dle této smlouvy, a že má dostatečné znalosti a zkušenosti k zajištění řádného plnění, s jehož obsahem se před podpisem této smlouvy seznámil.

1.2. Tato smlouva se uzavírá za účelem zajistit dlouhodobou a nepřetržitou ochranu informačních aktiv a klíčových IT služeb Objednatele před současnými kybernetickými hrozbami, jejichž úroveň a sofistikovanost dlouhodobě roste. Cílem je zajistit včasnou identifikaci bezpečnostních incidentů, rychlou reakci na známé i dosud neznámé hrozby a minimalizaci dopadů případných útoků na provoz organizace.

1.3. Dodavatel se zavazuje dodat takové řešení antivirové ochrany, které bude umožňovat jednotné řízení bezpečnostních politik, průběžný dohled nad stavem ochrany a efektivní reakci na bezpečnostní události napříč celým IT prostředím, aniž by neúměrně zvyšovalo nároky na interní personální kapacity Objednatele.

2. Předmět smlouvy

2.1. Dodavatel se zavazuje Objednateli poskytnout nevýhradní licence k užívání komplexního antivirového a bezpečnostního řešení nové generace, které kromě standardní ochrany koncových zařízení a serverů zahrnuje také centrální správu, pokročilé detekční a reakční mechanismy (EDR/XDR) a spravovanou detekci a reakci v režimu 24×7×365, jejichž popis je uveden v příloze č. 1 této smlouvy, a které splňují podmínky dle technické specifikace, která tvoří přílohu č. 2 této smlouvy (všechny tyto licence nebo předplatná dále jen „**předmět smlouvy**“).

2.2. Součástí předmětu smlouvy je:

2.2.1. poskytnutí nevýhradní licence k užití softwarové ochrany pro 160 ks koncových zařízení (80 ks stolních PC a 80 ks notebooků) a 75 serverů (všechny virtuální) (dále jen „**Antivirové řešení**“);

2.2.2. průběžné poskytování služeb podpory a aktualizací a Antivirového řešení a služby spravované detekce a reakce v režimu 24x7x365 nad EDR/XDR po dobu 60 měsíců od podpisu předávacího protokolu nebo zajištění licence (předplatného) pro tyto služby od výrobce řešení;

2.2.3. provedení implementace Antivirového řešení spočívající v instalaci, konfiguraci a uvedení Antivirového řešení do provozu v prostředí Objednatele; a

2.2.4. zajištění školení administrátorů za účelem používání Antivirového řešení.

2.3. Antivirové řešení je poskytováno jako časově omezené, nevýhradní, nepřevoditelné a s právem užití Antivirového řešení pro interní potřeby Objednatele.

2.4. Objednatel se zavazuje řádně a včas dodané Antivirové řešení převzít a zaplatit Dodavateli cenu sjednanou touto smlouvou.

2.5. Dodavatel se zavazuje, že Antivirové řešení splňuje technické podmínky uvedené v Příloze č. 2 (Technická specifikace). Na základě výzvy Objednatele se Dodavatel zavazuje předložit bez zbytečného odkladu doklady potvrzující splnění výše uvedených technických podmínek.

3. Práva a povinnosti smluvních stran

3.1. Dodavatel je povinen postupovat s náležitou odbornou péčí v souladu s právními předpisy, chránit práva a oprávněné zájmy Objednatele. Dodavatel se zavazuje k řádnému a včasnému plnění předmětu této smlouvy dle čl. 2 této smlouvy za podmínek stanovených touto smlouvou a pokyny Objednatele.

3.2. Smluvní strany prohlašují, že předmět smlouvy dle čl. 2 této smlouvy není plněním nemožným, a že smlouvu uzavírají po pečlivém zvážení všech možných důsledků.

3.3. Dodavatel je povinen jako součást předmětu smlouvy předat Objednateli kompletní technickou dokumentaci nezbytnou pro používání Antivirového řešení.

3.4. Dodavatel je povinen zachovat mlčenlivost o všech skutečnostech obchodní, výrobní či technické povahy souvisejících s Objednatelem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu a nejsou v příslušných obchodních kruzích běžně dostupné. Dodavatel se zavazuje zajistit, aby osoby, které musí tyto skutečnosti k plnění předmětu smlouvy znát, je uchovaly v tajnosti vůči třetím právnickým nebo fyzickým osobám.

3.5. Dodavatel se zavazuje mít po celou dobu platnosti této smlouvy sjednáno pojištění odpovědnosti za škodu způsobenou v souvislosti s výkonem podnikatelské činnosti, a to s limitem pojistného plnění nejméně 2 mil. Kč.

3.6. Objednatel poskytne Dodavateli k zajištění plnění předmětu smlouvy podle čl. 2 této smlouvy nezbytnou součinnost, tj. zejména zajistí vstup do příslušných prostor Dodavateli tak, aby Dodavatel mohl dostát svým závazkům a povinnostem stanovených touto smlouvou a příslušnými právními předpisy, nemůže-li Dodavatel zajistit požadované plnění jinak.

3.7. Dodavatel je povinen provést předmět smlouvy vlastním jménem, na vlastní odpovědnost a nebezpečí.

3.8. Dodavatel 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 povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů.

3.9. Dodavatel prohlašuje, že předmět smlouvy bude bez právních vad, a že splněním předmětu smlouvy nebudou porušena práva třetích osob, z nichž by pro Objednatele vyplynul jakýkoliv finanční nebo jiný závazek ve prospěch třetí strany. V případě, že toto prohlášení bude nepravdivé, je Dodavatel v plném rozsahu odpovědný za případné následky takovéhoto jednání, přičemž právo Objednatele na případnou náhradu škody a smluvní pokutu zůstává nedotčeno.

3.10. V případě, že Dodavatel k plnění vyžaduje součinnost Objednatele, je povinen požádat o poskytnutí součinnosti v dostatečném předstihu.

3.11. Dodavatel je povinen včas písemně upozornit Objednatele na zřejmou nevhodnost jeho pokynů, jejichž následkem může vzniknout škoda nebo nesoulad s obecně závaznými právními předpisy. Pokud Objednatel navzdory takovému upozornění trvá na svých pokynech, Dodavatel neodpovídá za jakoukoli škodu způsobenou jednáním na základě takových pokynů Objednatele.

3.12. Dodavatel se zavazuje při plnění této smlouvy postupovat tak, aby šetřil životní prostředí.

3.13. Dodavatel se zavazuje po dobu plnění této smlouvy platit svým poddodavatelům, kteří se na ní podílejí. Dodavatel se zavazuje, že si sjedná a bude dodržovat smluvní podmínky se svými poddodavateli srovnatelnými s podmínkami sjednanými v této Smlouvě. V případě, že se na plnění této smlouvy podílí poddodavatel Dodavatele, Dodavatel se zavazuje, že:

3.13.1. si sjedná a bude dodržovat smluvní podmínky se svými poddodavateli srovnatelnými s podmínkami sjednanými ve Smlouvě, a to v rozsahu výše smluvních pokut a délky záruční doby. Uvedené smluvní podmínky se považují za srovnatelné, bude-li výše smluvních pokut a délka záruční doby shodná se Smlouvou;

3.13.2. bude řádně a včas plnit finanční závazky svým poddodavatelům, kdy za řádné a včasné plnění se považuje plné uhrazení poddodavatelem vystavených faktur za plnění poskytnutá za plnění této smlouvy (nebo jeho části), a to vždy do 15 dnů od obdržení platby ze strany Dodavatele za konkrétní plnění.

3.14. Dodavatel prohlašuje, že tuto smlouvu bude plnit výhradně prostřednictvím poddodavatelů, jejichž seznam je uveden v příloze č. 3 této smlouvy. Dodavatel je oprávněn měnit osoby poddodavatelů po předchozím vyrozumění Objednatele s tím, že nový poddodavatel musí splňovat nejméně odbornost a podmínky, jako poddodavatel, kterého v rámci plnění této smlouvy nahradil. Za poddodavatele se nepovažuje výrobce řešení, jehož licence nebo předplatné služeb je dodáváno.

3.15. Dodavatel, je-li obchodní společností, prohlašuje, že osoba naplňující definici veřejného funkcionáře ve smyslu ust. § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů nebo touto osobou ovládaná osoba, nevlastní v Dodavateli podíl o velikosti nejméně 25 % účasti společníka v obchodní společnosti. Obdobně Dodavatel prohlašuje, že prohlášení dle předchozí věty se uplatní i na poddodavatele, prostřednictvím kterého Dodavatel prokazoval kvalifikaci v zadávacím řízení předcházející uzavření této smlouvy.

4. Poskytnutí licence

4.1. Dodavatel zprostředkovává Objednateli nevýhradní, časově omezenou licenci k užití Antivirového řešení. Licence je poskytována na dobu 60 měsíců, pro území

České republiky, pro instalaci na maximálně 160 ks koncových zařízení (80 ks stolních PC a 80 ks notebooků) a 75 serverů (všechny virtuální), výhradně pro interní potřeby Objednatele. Stejně je tomu v případě, že Dodavatel zprostředkovává také licenci výrobce pro zajištění technické podpory a služeb spravované detekce a reakce.

4.2. Objednatel není oprávněn Antivirové řešení dále šířit, poskytovat sublicence, upravovat zdrojový kód, zpřístupňovat Antivirové řešení třetím osobám.

4.3. Součástí licence je právo užívat veškeré aktualizace a nové verze Antivirového řešení poskytované Dodavatelem po dobu trvání smlouvy. Odměna za licence je zahrnuta v ceně dle čl. 6 této smlouvy. Žádné další licenční poplatky či jiné náklady související s Antivirovým řešením nebo jinými výhradními právy není Dodavatel oprávněn po Objednateli požadovat.

4.4. Dodavatel odpovídá za veškerou škodu způsobenou Objednateli porušením svých povinností, porušením ustanovení této smlouvy, nebo jiným protiprávním jednáním zaviněným pracovníky Dodavatele podílejícími se na plnění předmětu smlouvy. O náhradě škody platí obecná ustanovení občanského zákoníku. Řídí-li se používání Antivirového řešení a dodaných služeb smluvními ujednáními výrobce, nebo podmiňuje-li výrobce řešení a poskytovatel služeb, jehož licence jsou předmětem plnění této smlouvy, používání Antivirového řešení povinností uzavřít smlouvu upravující vztahy mezi Objednatelem (koncovým uživatelem) a výrobcem, uvede Dodavatel v rámci přílohy č. 1 také odkaz na smluvní ujednání výrobce a tuto skutečnost výslovně uvede v rámci příslušné přílohy.

5. Doba a místo plnění

5.1. Dodavatel se zavazuje k nasazení Antivirového řešení podle čl. 2 této smlouvy do ostrého provozu nejpozději ke dni 22. 3. 2026.

5.2. Místem plnění této smlouvy je sídlo Objednatele.

6. Cena a platební podmínky

6.1. Cena za plnění dle čl. 2 této smlouvy činí celkem:

6.1.1. cena bez DPH: 2 456 590,91 Kč

6.1.2. DPH 21 %: 515 884,09 Kč

6.1.3. cena s DPH: 2 972 475,00 Kč

6.2. Cena je stanovena jako konečná, nejvýše přípustná a jsou v ní zahrnuty veškeré náklady nutné pro řádné splnění sjednaného předmětu smlouvy včetně zejména nákladů na dopravu, cla, zisk Dodavatele, poplatky, pojištění a licence.

6.3. Dodavatel je oprávněn fakturovat Objednateli částku dle odst. 6.1 této smlouvy jednorázově, a to ke dni podepsání předávacího protokolu Antivirového řešení.

6.4. Daňový doklad bude vždy obsahovat pojmové náležitosti daňového dokladu stanovené zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, zákonem č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů. V případě, že daňový doklad nebude obsahovat správné údaje či bude neúplný, je Objednatel oprávněn daňový doklad vrátit ve lhůtě do data jeho splatnosti Dodavateli, aniž se tak dostane do prodlení. Dodavatel je povinen takový daňový doklad opravit, event. vystavit nový daňový doklad – lhůta splatnosti počíná v takovém případě běžet ode dne doručení opraveného či nově vystaveného dokladu Objednateli. Dodavatel souhlasí se zasílám daňového dokladu v elektronické podobě.

6.5. Není-li dohodnuto jinak, je splatnost daňového dokladu smluvními stranami dohodnuta na 60 kalendářních dnů ode dne řádného předání daňového dokladu Dodavatele Objednateli. Daňový doklad se považuje za řádně a včas zaplacený, bude-li poslední den této lhůty účtovaná částka odepsána z účtu ve prospěch účtu Dodavatele uvedeného na daňovém dokladu.

6.6. Daňové doklady mohou být doručovány v elektronické podobě a zasílány elektronicky, a to prostřednictvím datové schránky nebo e-mailu fakturace@unmz.gov.cz.

7. Záruční doba a reklamace

7.1. Dodavatel odpovídá za to, že licence na Antivirové řešení a licence na dodané služby, které jsou předmětem smlouvy (služba technické podpory a služba spravované detekce a reakce), bude po dobu trvání této smlouvy funkční a řešení bude odpovídat účelu, pro který bylo pořízeno.

7.2. Dodavatel poskytuje na předmět smlouvy záruku v délce trvání 60 měsíců ode dne protokolárního předání a převzetí implementovaného Antivirového řešení Objednatelem. Případné reklamace uplatňují a vyřizují kontaktní osoby smluvních stran uvedené v této smlouvě e-mailem. Dodavatel nenese odpovědnost za samotný provoz Antivirového řešení nebo poskytování služeb, jejichž dodavatelem je výrobce řešení. Záruky a odpovědnost vzhledem ke službám poskytovaným výrobcem řešení se řídí výhradně smluvními podmínkami výrobce řešení.

7.3. V případě, že je předmět smlouvy je dodán s vadami, či se vady v záruční době vyskytnou, je Dodavatel povinen oprávněně reklamované vady odstranit v souladu s právními předpisy. Je-li je součástí předmětu plnění také licence (předplatné) na technickou podporu výrobce, reklamace vad vzniklých v záruční době po převzetí plnění uplatní Objednatel u výrobce řešení, přičemž v reklamaci vadu popíše a uvede požadovaný způsob jejího odstranění.

7.4. Po dobu platnosti záruky je Dodavatel, resp. výrobce, povinen přijmout hlášení o výskytu vady způsobem definovaným Dodavatelem, resp. výrobcem v rámci služeb technické podpory. Pracovní doba technické podpory Dodavatele je v pracovních dnech od 9:00 do 17:00. Výskyt vady jsou oprávněny hlásit pouze kontaktní osoby ve věcech technických uvedených v této smlouvě. Reakční doba výrobce je popsána a řídí se Smluvními podmínkami profesionálních a bezpečnostních služeb výrobce. Technická podpora výrobce je dostupná v režimu 24/7.

7.5. Odstranění závady provede Dodavatel, resp. výrobce, v co nejkratším možném termínu.

7.6. Objednatel je oprávněn uplatnit vady předmětu plnění u Dodavatele kdykoliv během záruční doby bez ohledu na to, kdy Objednatel takové vady zjistil nebo mohl zjistit.

8. Sankce

8.1. Bude-li Dodavatel v prodlení s plněním dle této smlouvy, je Objednatel oprávněn požadovat po Dodavateli smluvní pokutu ve výši 1.000 Kč (slovy: jeden tisíc korun českých) za každý i započatý den prodlení.

8.2. V případě porušení povinnosti Dodavatele zachovávat mlčenlivost dle odst. 3.4 této smlouvy, má Objednatel právo požadovat smluvní pokutu ve výši 200.000 Kč (slovy: dvě stě tisíc korun českých) za každé porušení takové povinnosti.

8.3. V případě porušení povinnosti Dodavatele mít po celou dobu platnosti smlouvy sjednáno pojištění odpovědnosti za škodu způsobenou v souvislosti s výkonem podnikatelské činnosti v rozsahu stanoveném touto smlouvou uhradí Dodavatel smluvní pokutu ve výši 100.000 Kč (slovy: jedno sto tisíc korun českých).

8.4. Pro případ prodlení Objednatele s úhradou faktury je Dodavatel oprávněn účtovat Objednateli úrok z prodlení v zákonné výši.

8.5. Uhrazením smluvní pokuty není dotčeno právo poškozené smluvní strany domáhat se náhrady škody či újmy, která jí vznikla porušením smluvní povinnosti, které se smluvní pokuta týká, v plné výši, a to i ve výši přesahující smluvní pokutu. Výše smluvních pokut se do výše náhrady škody či újmy započítává.

8.6. Splatnost smluvní pokuty je 21 dnů od doručení písemné výzvy oprávněné smluvní strany k její úhradě straně povinné, a to bezhotovostním převodem na bankovní účet oprávněné smluvní strany.

9. Ukončení smlouvy

9.1. Tuto smlouvu lze ukončit písemnou dohodou nebo odstoupením od smlouvy.

9.1. Kterákoli smluvní strana má právo odstoupit od této smlouvy v případě podstatného porušení smlouvy druhou ze smluvních stran.

9.2. Smluvní strany této smlouvy se dohodly, že podstatným porušením této smlouvy se rozumí zejména následující případy:

9.2.1. Prodlení Dodavatele s plněním dle této smlouvy dle odst. 5.1. této smlouvy po dobu delší než 10 dnů;

9.2.2. Porušení povinnosti mlčenlivosti Dodavatele dle odst. 3.4 této smlouvy;

9.2.3. Porušení povinnosti Dodavatele mít sjednáno pojištění odpovědnosti za škodu dle odst. 3.5. této smlouvy;

9.2.4. Porušení povinnosti Dodavatele dle odst. 2.5 této smlouvy;

9.2.5. Dodavatel poskytuje Služby v rozporu se smlouvou a/nebo pokyny Objednatele, a ten nezjedná ani po písemné výzvě Objednatele nápravu;

9.2.6. Dodavatel závažným způsobem nebo opakovaně nedodržuje některou ze svých povinností podle této smlouvy;

9.2.7. Bude zahájeno insolvenční řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů, jehož předmětem bude úpadek nebo hrozící úpadek Dodavatele;

9.2.8. Dodavatel vstoupil do likvidace;

9.2.9. Bylo-li vůči Dodavateli, jeho skutečnému majiteli nebo osobě tvořící vrcholové vedení Dodavatele pravomocně vydáno usnesení o zahájení trestního stíhání;

9.2.10. Objednatel je v prodlení se splněním povinnosti uhradit cenu nebo její část o více než 60 dnů a nezjedná ani po písemné výzvě Dodavatele nápravu;

9.2.11. V případě, že dojde k podstatnému zvýšení rizika z hlediska bezpečnosti informací u Dodavatele změnou na straně Dodavatele, a ten nezjedná ani po písemné výzvě Objednatele nápravu; nebo

9.2.12. Dodavatel uzavřel smlouvu o prodeji či nájmu podniku či jeho části, na základě které převedl, resp. pronajal, svůj podnik či tu jeho část, jejíž součástí jsou i práva a závazky z právního vztahu dle této smlouvy na třetí osobu.

9.3. Odstoupení od smlouvy je účinné doručením písemného oznámení o odstoupení Dodavateli.

9.4. Ukončením účinnosti této smlouvy nejsou dotčena ustanovení smlouvy týkající se povinnosti z vadného plnění a nároků ze smluvních pokut, ustanovení o zachování mlčenlivosti, ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti této smlouvy.

9.5. V případě ukončení smlouvy z důvodů ležících na straně Objednatele před řádným splněním předmětu této smlouvy, je Objednatel povinen zaplatit Dodavateli do dne ukončení tohoto smluvního vztahu účelně vynaložené náklady na provedené plnění dle této smlouvy ve výši, kterou Dodavatel prokáže Objednateli, pokud jejich vyčíslení doručí Objednateli do patnácti (15) dnů od účinnosti ukončení smlouvy, to však pouze za předpokladu, že provedené činnosti jsou pro Objednatele využitelné.

9.6. Zaplacením smluvní pokuty není dotčen nárok Objednatele na náhradu škody v plném rozsahu.

10. Zpracování osobních údajů

10.1. Obě smluvní strany se zavazují zpracovávat osobní údaje za účelem plnění předmětného smluvního vztahu, v souladu se zákonem 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů (dále jen „**Zákon**“), a nařízením Evropského parlamentu a Rady (EU) č. 2016/679 (dále jen „**GDPR**“).

10.2. Osobní údaje budou smluvními stranami zpracovávány pouze v rozsahu nutném pro naplnění výše uvedeného účelu a pouze po dobu nutnou pro dosažení výše uvedených účelů, nejdéle však po dobu stanovenou příslušnými právními a interními předpisy a v souladu s nimi.

10.3. Každá ze smluvních stran je správcem ve smyslu ustanovení platných právních předpisů. K osobním údajům mají přístup pouze správce a osoby, které jsou ve vztahu k němu v pracovněprávním poměru nebo zpracovatel na základě smluvního vztahu se správcem a pouze za výše uvedenými účely zpracování. Přístup a nakládání s osobními údaji zpracovávanými každým ze správců podléhají interním předpisům daného správce.

10.4. Smluvní strany jsou povinny seznámit subjekty údajů (např. kontaktní osoby) s tím, že jejich osobní údaje mohou být zpracovány za účelem plnění předmětné smlouvy. Zároveň jsou povinny informovat subjekty údajů o možnosti uplatnění jejich práv u správce, a to na:

10.4.1. právo na přístup k osobním údajům, na jejich opravu nebo výmaz, právo na omezení zpracování a právo vznést námitku proti nezákonnému zpracování;

10.4.2. právo podat stížnost u dozorového úřadu.

11. Veřejnoprávní povinnosti Objednatele

11.1. Dodavatel bere výslovně na vědomí, že Objednatel má podle ustanovení § 2 odst. 1 písm. b) zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále jen „**zákon o registru smluv**“),

charakter subjektu, s nímž uzavřené soukromoprávní smlouvy, jakož i smlouvy o poskytnutí dotace nebo návratné finanční pomoci, podléhají povinnému uveřejnění postupem a za podmínek podle zákona o registru smluv.

11.2. Dodavatel je srozuměn a výslovně a bezvýhradně souhlasí s tím, že úplné znění této smlouvy včetně všech příloh bude uveřejněno v registru smluv, postupem a za podmínek podle zákona o registru smluv. Dodavatel bere rovněž na vědomí, že registr smluv je veřejně přístupný informační systém veřejné správy, jehož správcem je Ministerstvo vnitra, který slouží k uveřejňování smluv podle zákona o registru smluv a umožňuje bezplatný dálkový přístup.

11.3. Smluvní strany výslovně prohlašují, že veškeré informace, údaje a skutečnosti obsažené v této Smlouvě nepovažují samostatně ani v jejich souhrnu za informace, které nelze poskytnout nebo uveřejnit při postupu podle předpisů upravujících svobodný přístup k informacím, tedy zejména obchodní tajemství (ve smyslu ustanovení § 504 občanského zákoníku), bankovní tajemství (ve smyslu ustanovení § 38 odst. 1 zákona č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů) a utajované informace (ve smyslu příslušných ustanovení zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů) a udělují svůj výslovný souhlas k jejich uveřejnění bez stanovení jakýchkoliv dalších podmínek.

11.4. Objednatel se zavazuje uveřejnit tuto smlouvu prostřednictvím registru smluv ve smyslu zákona o registru smluv bez zbytečného odkladu po jejím podpisu oběma smluvními stranami, nejpozději však do 15 dnů od uzavření této smlouvy.

11.5. Dodavatel se zavazuje ověřit, zda byla povinnost Objednatele dle článku 11.4. této smlouvy řádně splněna. Není-li povinnost Objednatele dle článku 11.4. této smlouvy řádně a včas splněna, zavazuje se Dodavatel uveřejnit tuto smlouvu prostřednictvím registru smluv ve smyslu zákona o registru smluv sám, a to bez zbytečného odkladu poté, co se o nesplnění povinnosti Objednatele dle článku 11.4. Dodavatel dozvěděl, nejpozději však do 30 dnů ode dne, kdy byla tato smlouva uzavřena.

11.6. Smluvní strany berou na vědomí, že Objednatel je povinen poskytnout informace v souladu se zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a souhlasí s tím, aby veškeré informace obsažené v této Smlouvě byly bez výjimky poskytnuty třetím osobám, pokud o ně požádají.

12. Komunikace mezi smluvními stranami

12.1. Veškeré písemnosti, oznámení či další sdělení (dále jen „**sdělení**“), vyjma žádostí o technickou podporu, hlášením závad nebo v souvislosti se službami spravované detekce a reakce, jejichž hlášení se řídí mechanismem dle bodu 7.4, doručují smluvní strany prostřednictvím informačního systému datových schránek.

12.1.1. Identifikátor datové schránky Dodavatele: 4jk4j5x.

12.1.2. Identifikátor datové schránky Objednatele: 4htvpem.

12.2. Sdělení mohou být doručována též prostřednictvím e-mailu na následující e-mailové adresy stran:

12.2.1. e-mailová adresa Dodavatele: obchod@eset.com

12.2.2. e-mailová adresa Objednatele: patrik.vagel@unmz.gov.cz

12.3. Sdělení mohou být doručována též prostřednictvím poštovního doručovatele, a to na následující adresy stran:

12.3.1. adresa Dodavatele: Jankovcova 1037/49, 170 00 Praha 7

12.3.2. adresa Objednatele: Biskupský dvůr 1148/5, 110 00 Praha 1

12.4. Osoby oprávněné zastupovat smluvní stranu při plnění této smlouvy:

12.4.1. za Dodavatele: Jan Urbík, Country Manager

12.4.2. za Objednatele: Ing. Miroslav Chloupek, ředitel sekce vnějších vztahů a ekonomiky

12.5. Každá smluvní strana je oprávněna jednostranně změnit své kontaktní údaje, a to doručením sdělení obsahujícím novou adresu. Taková změna je účinná ode dne následujícího po dni doručení sdělení druhé smluvní straně.

12.6. Sdělení se považuje za doručené okamžikem potvrzení doručení ze strany adresáta. Bez takového potvrzení se považuje sdělení za doručené též:

12.6.1. v případě odeslání prostřednictvím datové schránky jedné smluvní strany do datové schránky druhé smluvní strany, okamžikem, kdy se do datové schránky přihlásí osoba, která má s ohledem na rozsah svého oprávnění přístup k dodanému sdělení. Nepřihlásí-li se do datové schránky osoba podle předchozí věty ve lhůtě do 10 dnů ode dne, kdy bylo sdělení dodáno do datové schránky, považuje se toto sdělení za doručené posledním dnem této lhůty;

12.6.2. v případě odeslání na e-mailovou adresu příjemce dnem následujícím po dni jeho prokazatelného odeslání;

12.6.3. v případě odesláním sdělení prostřednictvím poštovního doručovatele, se považuje sdělení doručené 3. dnem po odeslání prostřednictvím služeb poštovního doručovatele; přičemž doručení se považuje za účinné, i když se o něm adresát nedozvěděl.

12.7. Smluvní strany se dohodly, že sdělení zaslaná prostřednictvím e-mailu opatřená zaručeným elektronickým podpisem nebo ve formě PDF s vlastnoručním podpisem smluvní strany, považují za sdělení písemná, neodporuje-li to v konkrétním případě platné právní úpravě.

13. Závazek implementace společenské odpovědnosti

13.1. Dodavatel je povinen zajistit, aby byly do průběhu plnění této smlouvy zapojené pouze osoby splňující veškeré podmínky dle právních předpisů a disponující se všemi potřebnými povoleními.

13.2. Dodavatel se zavazuje dodržovat podmínky férových pracovních podmínek blíže vymezených v příloze č. 4 této smlouvy. Podpis předmětného čestného prohlášení o dodržení zásad odpovědného veřejného zadávání Dodavatelem byl předpokladem uzavření této smlouvy.

14. Závěrečná ustanovení

14.1. Tato smlouva nabývá platnosti okamžikem připojení podpisu poslední smluvní strany a účinnosti dnem uveřejnění v registru smluv vedeného Ministerstvem vnitra České republiky.

14.2. Nestanoví-li tato smlouva pro konkrétní případ výslovně jinak, lze ji měnit jen písemným dodatkem, uzavřeným mezi smluvními stranami.

14.3. Smlouva podléhá uveřejnění v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů. Návrh na uveřejnění smlouvy v registru smluv podá Objednatel.

14.4. Smluvní strany sjednávají, že právní vztah založený touto Smlouvou se řídí právem České republiky s vyloučením jeho kolizních norem.

14.5. Tato smlouva obsahuje následující přílohy:

14.5.1. Příloha č. 1: Popis plnění předmětu smlouvy

14.5.2. Příloha č. 2: Technická specifikace

14.5.3. Příloha č. 3: Seznam poddodavatelů

14.5.4. Příloha č. 4: Čestné prohlášení o dodržení zásad odpovědného veřejného zadávání

14.6. Tato smlouva je vyhotovena v listinné podobě ve dvou (2) stejnopisech, z nichž každá smluvní strana obdrží po jednom (1) stejnopisu, nebo v elektronické podobě, přičemž v takovém případě je podepsána uznávaným elektronickým podpisem nebo jiným platným způsobem elektronického podpisu dle příslušných právních předpisů. V případě elektronického vyhotovení obdrží každá smluvní strana jedno (1) vyhotovení v elektronické podobě.

14.7. Smluvní strany prohlašují, že jsou oprávněny k právnímu jednání, že si smlouvu před jejím podpisem přečetly a jsou seznámeny s jejím obsahem, že byla uzavřena po vzájemné dohodě, podle jejich vážné a svobodné vůle, dobrovolně, určitě a srozumitelně, což stvrzují svými podpisy.

V Praze

Objednatel:

_____

Česká republika – Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, organizační složka státu
Ing. Jiří Kratochvíl, předseda úřadu

V Praze

Dodavatel:

_____

ESET software spol. s r.o.
Jan Urbík, Country Manager

Příloha č. 1 – Popis plnění předmětu smlouvy

Na základě požadavků zakázky přikládáme charakteristiku řešení ESET PROTECT MDR, jehož licence (předplatné) je / jsou předmětem plnění smlouvy a které zahrnuje: licenci (předplatné) pro úroveň ochrany ESET PROTECT Elite včetně aktualizací řešení od výrobce, licenci (předplatné) služby spravované detekce a reakce 24/7 ESET MDR a služby prémiové technické podpory ESET Premium Support, všechny v délce 60 měsíců pro 235 zařízení.

Níže přikládáme základní specifikaci předmětu smlouvy a také odkazy na podrobnou specifikaci výrobce.

ESET PROTECT Elite obsahuje moduly

- Moderní vícevrstvou ochranu koncových zařízení různých platforem.
- Ochranu souborových serverů.
- Ochranu před hrozbami nultého dne ***ESET LiveGuard Advanced***.
- Nástroj ***Šifrování celého disku*** spravovaný z centrální správy ESET PROTECT, kterým je možné z centrální správou chránit data proti neoprávněnému přístupu v případě ztráty nebo krádeže zařízení (např. notebooků).
- Multifunkční ***konzole ESET PROTECT*** pro správu zabezpečení a spravovaných zařízení z jednoho místa, která umožňuje automatizovat i běžné kroky údržby (např. vynucení aktualizací Windows apod.).
- **Ochranu a správu mobilních zařízení *ESET Mobile Threat Defense*** pro zařízení s Android a MDM také pro iOS a iPadOS, které je v ceně pro stejný počet zařízení.
- Funkci ***Ransomware Remediation***, která obnoví původní soubory v případě detekování dosud neznámého ransomware (aktuálně dostupné pro stanice s Windows).
- Nástroj ***ESET Inspect*** pro **rozšířenou detenci a reakci (EDR/XDR)**, která slouží k odhalení hrozeb a nezvyklého chování v síti a umožňuje na hrozby rychle reagovat.
- **Správu zranitelností a záplat *ESET Vulnerability Assessment & Patch Management*** pro skenování zranitelností OS a aplikací třetích stran a možnost automatického nebo manuálního záplatování
- **Vícefaktorové ověřování *ESET Secure Authentication*** pro ochranu přístupů na stanice, servery RDP, VPN apod.
- **Pokročilou ochranu pro mail a cloudové aplikace** Microsoft 365 a Google Workspace a ochranu pro mail server MS Exchange.

Součástí řešení je vzdálená správa ESET PROTECT, díky které mají Vaši IT specialisté přehled o stavu zabezpečení a ochrany v reálném čase napříč zařízeními, včetně možnosti spravovat zařízení z jednoho místa, automatizovat některé postupy apod. Provoz *správy Eset Protect* zajišťuje výrobce – výhodou je rychlejší doručování vylepšení a aktualizací vzdálené správy a zároveň Vám odpadají náklady a starost o provoz. Pro nasazení v prostředích s omezenou viditelností do internetu je součástí řešení také možnost využívat proxy server ESET Bridge.

Úplná a přesná charakteristika řešení je uvedena na stránkách výrobce:

ESET PROTECT Elite | Kybernetická ochrana XDR | ESET – základní charakteristika

Firemní uživatelé | ESET Online nápověda – online nápověda a technická dokumentace pro všechny moduly řešení.

Používání řešení ESET je podmíněno akceptováním smluvních ujednání výrobce, jak je uvedeno níže.

Služba spravované detekce 24/7 ESET MDR a prémiové technická podpora ESET Premium Support

Součástí předmětu plnění smlouvy je také předplatné služby spravované detekce a reakce 24/7 **ESET MDR** a technické podpory ze strany výrobce **ESET Premium Support** pro počet zařízení dle smlouvy. Základní charakteristiky Bezpečnostních a Profesionálních služeb ESET jsou uvedeny v tabulkách níže.

Charakteristika Profesionálních služeb ESET

	STANDARD SUPPORT	ESET PREMIUM SUPPORT	ESET PREMIUM SUPPORT ULTIMATE	ESET DEPLOYMENT & UPGRADE	HEALTHCHECK
Doba reakce na kritickou událost (A)	Nejlepší možný	2 hodiny	30 minut	–	–
Doba reakce na závažnou událost (B)	Nejlepší možný	4 hodiny	2 hodiny	–	–
Doba reakce na běžnou událost (C)	Nejlepší možný	1 pracovní den	1 pracovní den	–	–
Dostupnost podpory	7:00-18:00, pracovní dny	365/24/7	365/24/7	–	–
Kontakty zákazníka	Omezený	Neomezený	Neomezený	–	–
Řazení přednostních hovorů do fronty	–	✓	✓	–	–
Tikety s nárokem na přednostní	–	Omezený	Neomezený	–	–
Manažer vyhrazený pro konkrétního klienta	–	–	✓	–	–
Přednostní přístup k vývojovým	–	–	✓	–	–
Proaktivní informační služby	–	–	✓	–	–
Nasazení a upgrade	–	–	1	✓	–
Kontrola stavu	–	–	1	–	✓

Poskytování Profesionálních služeb ESET ze strany výrobce a rozsah těchto jednotlivých služeb se řídí výhradně *Smluvními podmínkami* poskytování profesionální služeb, jak je uvedeno níže v části Smluvní ujednání výrobce.

Charakteristika Bezpečnostních služeb ESET – služeb spravované detekce a reakce

	ESET MDR	ESET MDR Ultimate
	Služba Managed Detection & Response (MDR) *	Prémiová varianta služby MDR + asistence DFIR
		Garantováno SLA
Globální tým pro sledování hrozeb	✓	✓
Monitorování aktivních kampaní malwarových skupin	✓	✓
Neustálé vylepšování a automatizace	✓	✓
Pokročilá knihovna pravidel a dotazů pro vyhledávání hrozeb (Advanced Signal Hunting Library)	✓	✓
Pravidla chování a optimalizace výjimek	✓ **	✓
Průběžné vyhledávání hrozeb pod vedením odborníků	✓	✓
Přizpůsobitelné reporty	✓	✓
Monitoring, vyhledávání, vyhodnocování a reakce 24/7	✓	✓
Viditelnost vektorů útoku	–	✓
Vyhrazený specialista pro reakci na incidenty	–	✓
Digitální forenzní analýza při reakci na incidenty (Asistence DFIR)	–	✓
Podpora při detekci malwaru	–	✓
Expertní analýza malwarových souborů	–	✓
Individuální vyhledávání všech aktuálních hrozeb	–	✓
Vyhledávání historických hrozeb	–	✓
Nasazení & aktualizace	–	✓
Odborná pomoc pro výstrahy MDR s rozšířeným kontextem	–	✓

* Službu ESET MDR je poskytována pouze pro řešení s cloudovou správou. ** Optimalizace na SIEM úrovni. Služby spravované detekce a reakce jsou dostupné k řešením ESET PROTECT Enterprise a ESET PROTECT Elite.

Poskytování Bezpečnostních služeb ESET ze strany výrobce a rozsah těchto jednotlivých služeb se řídí výhradně *Smluvními podmínkami* poskytování profesionální služeb, jak je uvedeno níže v části Smluvní ujednání výrobce.

Smluvní ujednání výrobce

Poskytovatelem předplatného (jinde také jako „licence“ nebo „předmět smlouvy“) je ESET spol. s r.o., se sídlem na adrese Einsteinova 24, 851 01 Bratislava, Slovensko, zapsané v obchodním rejstříku vedeném Městským soudem Bratislava III v oddílu Sro, vložka 3586/B, IČO: 31333532 (dále jako „**ESET SK**“), který je zároveň výrobcem řešení a poskytovatelem služeb. Podmínky poskytování a užívání předplatného a veškerá práva a povinnosti Nabyvatele (dále také jako „Uživatel“) a ESET SK ve vztahu k nim se řídí právními dokumenty ESET SK uveřejněnými na webové stránce ESET v části Centrum zásad společnosti ESET https://legal.eset.com/?lang=cs-CZ (dále jako „**Obchodní podmínky ESET SK**“). Obchodní podmínky ESET SK tvoří zejména: *Podmínky použití* (Terms of Use), *Zásady ochrany osobních údajů* (Privacy Policy for Business), *Zásady zabezpečení* (Security Policy), *Zásady životního cyklu* (End of Life Policy).

Uživatel podpisem této smlouvy potvrzuje, že se seznámil s Obchodními podmínkami ESET SK a souhlasí s nimi. Uživatel bere na vědomí, že Obchodní podmínky ESET SK se pro něj stávají závaznými získáním předplatného v momentu v nich uvedeném. Uživatel bere na vědomí, že používání předplatného je podmíněno vytvořením účtu ESET PROTECT Hub.

Uživatel bere na vědomí, že Zprostředkovatel není poskytovatelem předplatného a jeho povinnosti dle této smlouvy jsou omezeny na dodání předplatného dle sjednané specifikace a pomoc s nasazením řešení dle předmětu smlouvy. Zprostředkovatel zejména nenese odpovědnost za jakoukoliv újmu způsobenou využíváním předplatného.

Je-li předmětem plnění smlouvy zajištění licence nebo předplatného profesionálních nebo bezpečnostních služeb, řídí se rozsah a poskytování těchto služeb pouze zvláštními *Smluvními podmínkami*. Tyto Smluvní podmínky jsou součástí *Podmínek použití* a jsou dostupné jak pod odkazem výše, stejně tak je možné je najít samostatně na stránkách výrobce https://help.eset.com/enterprise_services/cs-CZ/terms_and_conditions.html.

Technická dokumentace řešení

Kompletní technická dokumentace k řešením (jednotlivým modulům a produktům, které je možné využívat s předplatným daného modulu) a službám je dostupná na stánkách výrobce: Firemní uživatelé | ESET Online nápověda, a to včetně technických předpokladů nasazení řešení a smluvních ujednání. Tato kompletní on-line dokumentace je považována za splnění podmínek ohledně předání dokumentace nebo návodů k řešení dle této smlouvy.

Příloha č. 2 – Technická specifikace

ANTIMALWARE ŘEŠENÍ PRO KONCOVÉ STANICE A SERVERY
Podporované klientské platformy Windows, Linux, MacOS, Android, vše v českém jazyce.
Antimalware, antiransomware, antispyware a anti-phishing pro aktivní ochranu před všemi typy hrozeb, která zahrnuje:
Personální firewall pro zabránění neautorizovanému přístupu k zařízení se schopností automatického přebrání pravidel z brány Windows Firewall.
Modul pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost zařízení s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory.
Ochrana před neautorizovanou změnou nastavení / vyřazení z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému
Aktivní i pasivní heuristickou analýzu pro detekci dosud neznámých hrozeb
Systém pro blokaci exploitů zneužívajících zranitelností nultého hne, který pokrývá nejpoužívanější vektory útoku: síťové protokoly Flash Player, Jabu, MS Office, webové prohlížeče, e-mailové klienty, PDF čtečny
Systém pro detekci malwaru již na síťové úrovni poskytující ochranu i před zneužitím zranitelností na síťové vrstvě.
Kontrolu šifrovaných spojení (SSL, TLS, HTTPS, IMAPS…).
Kontrolu RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování.
Cloudovou kontrola souborů pro urychlení skenování fungující na základě reputace souborů.
Kontrolu souborů v průběhu stahování pro snížení celkového času kontroly, kotrolu při zapisování na disku a extrahování archivačních souborů.
Detekci s využitím strojového učení.
Funkci ochrany proti zapojení do botnetu.
Ochranu před síťovými útoky skenující síťovou komunikaci a blokující pokusy o zneužití zranitelností na síťové úrovni.
Kontrola s podporou cloudu pro odesílání a online vyhodnocování neznámých a potenciálně škodlivých aplikací.
Lokální sandbox
Modul behaviorální analýzy pro detekce chování nových typů ransomwaru
Systém reputace pro získání informací o závadnosti souborů a URL adres.
Cloudový systém pro detekci nového malwaru ještě nezaneseného v aktualizacích signatur.
Technologie pro detekci rootktitů obvykle se maskujících za součásti operačního systému.
Skenr firmwaru BIOSu a UEFI, skenování souborů v cloudu OneDrive
Funkcionalita pro klienty MS Windows – Antimalware, Antispyware, Personal Firewall, Personal IPS, Application control, Device control, Security Memory (zabraňuje útokům na běžící aplikace), kontrola integrity systémových komponent.
Funkcionalita pro klienty MacOS – Antimalware, Personal Firewall, Device control, autoupgrade
Funkcionalita pro klienty Linux – Antimalware, Botnet Protection, ICAPs scan,
Možnost aplikování bezpečnostních politik i v offline režimu na základě definovaných podmínek.
Ochrana proti pokročilým APT hrozbám a zranitelnostem nultého dne.
Okamžité blokování/mazání napadených souborů na stanici (s možností stažení administrátorem k další analýze).

Duální aktualizační profil pro možnost stahování aktualizací z mirroru v lokální síti a zároveň vzdálených serverů při nedostupnosti lokálního mirroru.
Možnost definovat webové stránky, které se spustí v chráněném režimu prohlížeče, pro bezpečnou práci s kritickými systémy nebo internetovým bankovnictví.
Aktivní ochrany před útoky hrubou silou na protokol SMB a RDP.
Možnost zablokování konkrétní IP adresy po sérii neúspěšných pokusů o přihlášení pro protokoly SMB a RDP s možností výjimek ve vnitřních sítích.
CLOUDOVÁ ANALÝZA NEZNÁMÝCH VZORKŮ
Pro maximální ochranu před hrobami nultého dne a minimalizaci hw nároků řešení požadujeme funkci cloudového sandboxu plně integrovaného do produktu pro koncové a serverové zařízení, tj. cloudový sandbox nemá vlastního agenta, nevyžaduje instalaci další ko
Cloudový sandbox umožňuje spuštění vzorků malwaru pro:
Windows
Linux
MacOS
Možnost využití na koncových bodech a serverech pro aktivní detekci škodlivých souborů, přičemž umožňuje
Analýzu neznámých vzorků v řádu jednotek minut.
Optimalizaci pro znemožnění obejití anti-sandbox mechanismy.
Analýzu rootkitů a ransomwaru.
Detekovat a zastavit zneužití nebo pokus o zneužití zranitelnosti nultého dne.
Manuální odeslání vzorku do sandboxu.
Možnost proaktivní ochrany, kdy je potenciální hrozba blokována, dokud není znám výsledek analýzy ze sandboxu.
není omezeno množství odesílaných souborů.
Veškerá komunikace probíhá šifrovaným kanálem.
Okamžité odstranění souboru po dokončení analýzy v cloudovém sandboxu
Možnost volby, jaké kategorie souborů do cloudového sandboxu budou odcházet (spustitelné soubory, archivy, pravděpodobný spam, dokumenty atp.)
Řešení pracuje s behaviorální analýzou.
Detailní výsledek o analyzovaném souboru včetně informace o nalezeném škodlivém chování daného souboru formou webového repotu s možností exportu do PDF.
EDR/XDR ŘEŠENÍ
Možnost výběru mezi provozem EDR/XDR serveru (dále také jen jako "EDR server") v on-premise prostředí nebo cloud prostředí výrobce.
Podpora offline prostředí, technologie EDR/XDR vyhodnocuje a reaguje na události lokálně, nevyžaduje pro svou činnost připojení k internetu.
EDR/XDR řešení poskytuje stejnou úroveň ochrany v případě nedostupnosti internetového připojení. Pracuje autonomně a chybějící konektivita (do cloudu, nebo řídící server) nesmí ovlivnit kvality detekční technologie na koncovém bodu.
EDR/XDR agent pro prostředí Windows, Windows server, MacOS a linuxové distribuce
Možnost řízení managementu EDR/XDR prostřednictvím API, a to jak pro přijímání informací z EDR serveru, tak zasílání příkazů na EDR server;

EDR/XDR řešení podporuje vzdálené pouštění příkazů přímo z EDR konzole na platformě Windows s nejvyšším oprávněním System.
Zabezpečení konzole EDR/XDR
Autentizace do management konzole EDR/XDR pomocí dvoufaktorové autentizace
Nutnost aktivovat vícefaktorovou autentizaci pro používání pokročilých nástrojů typu terminálového připojení
Vzdálené spouštění příkazů z konzole je v EDR systému logováno.
Logování činností administrátora
Další požadované funkce EDR/XDR řešení:
Možnost izolace zařízení od sítě prostřednictvím EDR agenta přímo z konzole.
Tvorba vlastních Indikátorů ohrožení (IoC).
Možnost vyhledávání pomocí nově vytvořených IoC nad historickými daty.
Při provozu v on-premise prostředí je k dispozici škálování množství historických dat vyhodnocených v EDR, až 3 měsíce pro low-level-data, 3 roky pro detekované incidenty
Při provozu v cloudu možnost dodatečného dokoupení délky retence low-level-dat od výrobce řešení
Možnost aktivovat „učící režim“ pro automatizované vytváření výjimek k detekčním pravidlům
Řešení umožnuje analýzu vektorů útoku.
Schopnost ukončit infikovaný proces.
Možnost vytváření automatizovaného reakce (response úkonu) v podobě izolace stanice, blokace konkrétní hash, odhlášení uživatele, restartování počítače pro jednotlivé scénáře nebo detekce.
Možnost automatického vyřešení incidentu definovaných administrátorem
Schopnost prioritizace vzniklých incidentů.
Stažení podezřelého souboru ze stanice přes konzoli EDR/XDR.
Schopnost zobrazení detekcí provedených antimalware produktem.
Řešení je schopné generovat tzv. forest / full execution tree model.
Provázání s technikami popsanými ve znalostní bázi MITRE ATT&CK.
Řešení umožňuje fungovat v offline režimu, a to konkrétně jeho detekční pravidla + předem definované komplexnější incidenty/set detekčních pravidel po sobě jdoucích.
Průběžně aktualizovaná detekční pravidla EDR systému bez nutnosti aktualizace centrální správy/klienta.
Možnost definice vlastních komplexních „incidentů“ spojující v chronologickém pořadí detekci vybraných událostí.
Pokročilé detekční mechanismy pro detekci útoku i při nedostupnosti cloudového/centrálního serveru výrobce.
Exportu raw dat (veškerých dat) na externí úložiště, např. lokální disk apod.
Podpora formátu SHA256
Filtrování určitého typu dat zpracovávaného z klientem
Podpora response akce v podobě automatického odeslání souboru k analýze do cloudového sandboxu výrobce
Schopnost detekce:
škodlivých spustitelných souborů, skriptů, exploitů, rootkitů, síťových útoků, znežití WMI nástrojů, bezsouborového malware, pokusů o dumpování přihlašovacích údajů uživatele a další
Schopnost detekovat laterální pohyb útočníka.

Možnost ruční analýzy procesů veškerých spustitelných souborů a DLL knihoven.
Možnost náhledu na spuštěné skripty použitých v daném incidentu
Možnost zabezpečeného vzdáleného spojení přes servery výrobce do on-premise konzole EDR
DOHLED A PODPORA VÝROBCE
Technická podpora výrobce dostupná v režimu 24/7/365 s garantovanou dobou reakce.
Služba vyhodnocování dat z cloudové EDR/XDR komponenty (modulu) výrobcem v režimu 24/7/365 s možností zasáhnout v případě incidentu v prostředí zákazníka pomocí reakcí, které umožňuje EDR/XDR komponenta.
Pravidelný reporting o událostech vyhodnocených v rámci služby výrobce.
MANAGEMENT KONZOLE PRO SPRÁVU ŘEŠENÍ V RÁMCI NABÍZENÉHO BALÍKU
Webová konzole
Možnost instalace v on-premise prostředí na Windows nebo Linux nebo provozu formou virtual appliance.
Možnost provozu konzole v cloudu výrobce
Server/proxy architektura pro síťovou pružnost – snížení zátěže při stahování aktualizací detekčních modulů výrobce.
Nezávislý agent (pracuje i offline) vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta
Offline uplatňování politik a spouštění úloh při výskytu definované události (například: odpojení od sítě při nalezení škodlivého kódu).
Administrace antimalware řešení v nejpoužívanějších jazycích včetně češtiny.
Široké možnosti konfigurace oprávnění administrátorů (například možnost správy pouze části infrastruktury, které konkrétnímu administrátorovi podléhá).
Zabezpečení přístupu administrátorů do vzdálené správy pomocí dvufaktorové autentizace.
Informace o aktuálně přihlášených uživatelích na daném zařízení.
Podpora štítků/tagování pro snazší správu a vyhledávání.
Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce.
Vzdálené získání zachyceného škodlivého souboru z klienta.
Detekce nespravovaných (rizikových) počítačů komunikujících na síti.
Instalace a odinstalace aplikací 3. stran.
Vyčítání informací o verzích softwaru 3. stran.
Možnost vyčítat informace o hardwaru na spravovaných zařízeních (CPU, RAM, diskové jednotky, grafické karty…).
Vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku.
Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny a automatickému uplatnění navázané klientské úlohy nebo politiky.
Dynamické skupiny musí umět fungovat i v konkrétních časových slotech a uplatňovat podporované klientské úlohy

Automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů (například: 7 % všech počítačů / 40 klientů hlásí problém).
Podpora SNMP Trap, Syslogu, Rest API
Podpora instalace agenta skriptem - *.bat, *.sh, *.ini (GPO, SSCM…).
Reportování stavu klientů chráněných jinými bezpečnostními programy.
Schopnost zaslat reporty a upozornění na e-mail.
Řešení umožňuje odesílat notifikace o vybraných událostech prostřednictvím tzv. webhooků
Možnost integrace s řešením třetích stran podporující MDM (např. MS Intune, Workspace One)
Možnost řízení managementu konzole a jeho komponent prostřednictvím API, a to pro: centrální správu samotnou, komponenty antimalware řešení, EDR/XDR řešení
Možnost exportu informací o detekcích, incidentech
Možnost úpravy detekčních pravidel EDR
správy zařízení a jeho nastavení, instalačních balíčků, včetně možnosti automatizace jednotlivých úkonů
Přidání zařízení do vzdálené správy pomocí:
synchronizace s Active Directory (jedné nebo více Active Directory), včetně možnosti synchronizace počítačů a uživatelů
ruční přidání pomocí dle IP adresy nebo názvu zařízení,
pomocí síťového skenu nechráněných zařízení v síti.
DVOUFAKTOROVÁ AUTENTIZACE
Klientská část:
Doručení OTP:
- **aplikací v mobilním zařízení,**
- **e-mailem,**
- bezpečnostním tokenem,
- SMS zprávou,
- Možnost konfigurace vlastní SMS bránu pro doručení OTP kódu
- **vlastní aplikací.**
Další možnosti ověření:
- **FIDO**
- **Push Authnetication**
Aplikace výrobce s podporou Push-Notifications pro platformy:
- iOS
- Android
- watchOS, wear OS
Požadavky na aplikaci výrobce:
- Mobilní aplikace v hlavních jazykových lokalizacích včetně češtiny
- Přístup do mobilní aplikace ochráněn PINem / biometrikou
- Možnost generovat OTP v off-line prostředí (bez internetové připojení, bez GSM spojení)
Další požadavky
- Hardwarové tokeny HOTP splňující standard OATH
- Hardwarové tokeny certifikované výrobcem
- Kompletně softwarové řešení – bez nutnosti nákupu dalšího hardwaru
- Podpora **time based hardwarových tokenů (PSKC)**

- **Self-enrollment uživatelů**
Chráněné služby:
- **Příhlášení do webových aplikací společnosti Microsoft (OWA, SharePoint…),**
- Přihlášení přes RDP,
- **Exchange Control Panel & Exchange Administrator Center,**
- VMware Horizon View,
- Citrix XenApp,
- **VPN služby využívajících protokol RADIUS (Cisco, Citrix, Fortinet, Juniper, Microsoft, OpenVPN…),**
- **cloudové služby Office 365, G Suite, identity providerů (podpora SAML protokolu, podpora AD FS)**
- **Lokálního přihlášení do Windows, Linux, macOS účtů**
- **Vyžádání 2FA v nouzovém režimu Windows**
- **Vyžádání 2FA při vyvolání UAC dialogu ve Windows**
- **Vyžádání 2FA při uzamčeném účtu**
Požadavky na správu řešení:
- Webové konzole provozována v cloudu výrobce s možností nasazení v on-premise prostředí
- Přístup do konzole lze chránit 2FA ověřením
- **Podpora multitenantního provozu (možnost spravovat vícero uživatelských struktur v jedné konzoli)**
- Podpora synchronizace uživatelských účtů z Active Directory
- Možnost tvorby výjimek pro vnitřní sítě, kde není 2FA vyžadováno
- Umožnit uživatelům přihlášení bez použití 2FA pro vybrané služby
- Konzole umožňuje generovat Master recovery klíče pro konkrétní chráněné služby
- Možnost dočasně pozastavit požadavek na 2FA pro uživatele
- **Nastavení limitu pro počet neúspěšných zadání OTP**
- Centrální správa a přidělování hardwarových tokenů jednotlivým uživatelům
- Možnost reportování o úspěšných/ neúspěšných přihlášení uživatelů, způsobu použité autentizace (SMS, Push, OTP)
Možnost implementace 2FA do vlastních systémů pomocí:
- API
- SDK výrobce (Java, PHP, .NET, Windows Script Host)
Další požadavky na řešení:
Soulad s:
ISO27001 Standard,
PCI/DSS - The Payment Card Industry Data Security Standard,
ISAE 3402 – International Standards for Assurance Engagements no. 3402,
HIPAA - Health Insurance Portability and Accountability Act,
FFIEC - Federal Financial Institutions Examination Council compliances,
Možnost definovat maximální počet offline přihlášení.
Technická podpora v českém jazyce.
OCHRANA POŠTOVNÍCH SERVERŮ Microsoft Exchange

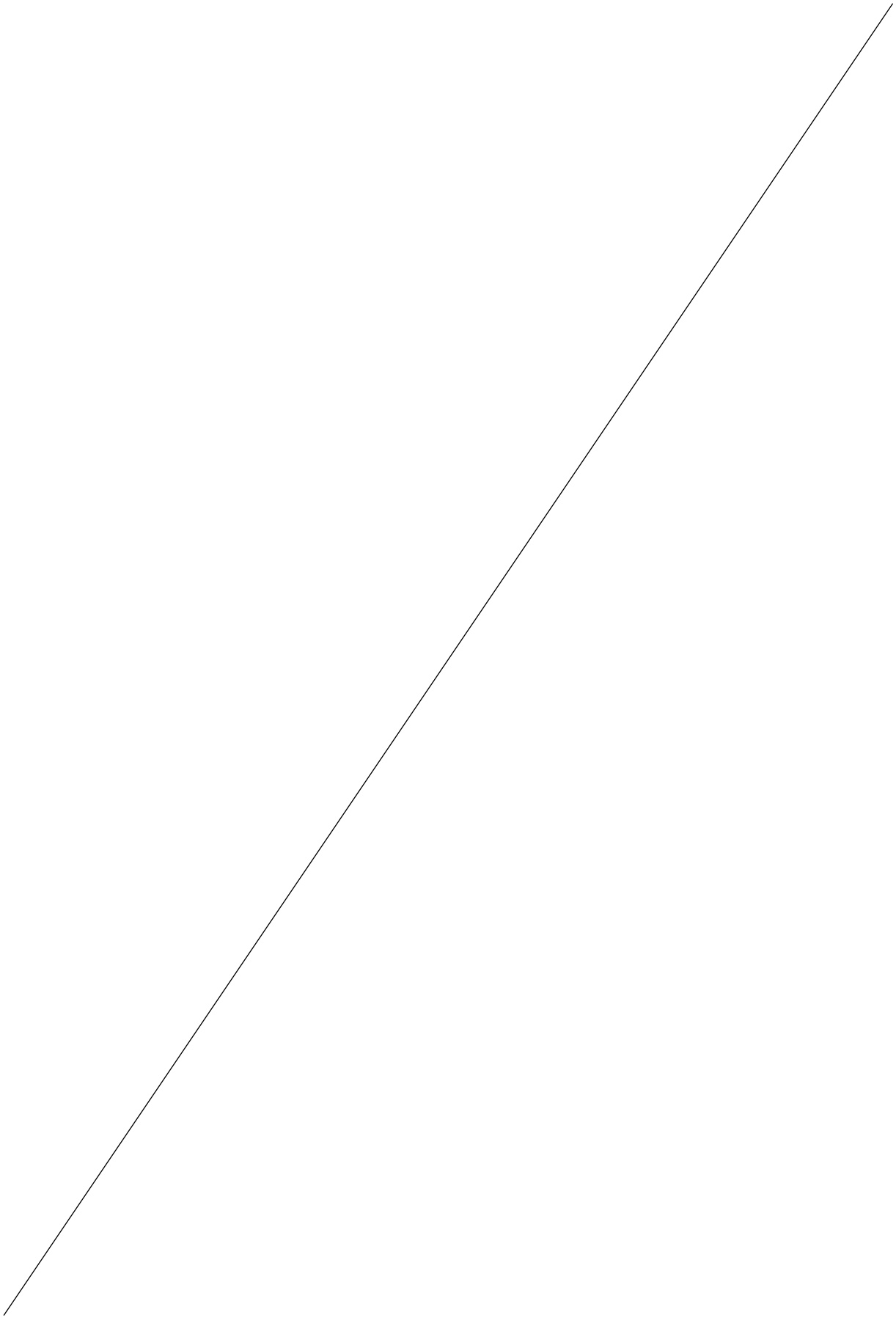
- Společná víceúrovňová ochrana celého serveru – databáze schránek, transportu zpráv i souborového systému serveru
- Podpora MS Exchange 2007, 2010, 2013 a 2016, 2019
- Antivirus, antispyware a antispoofing technologie
- Antispam s funkcí graylisting
- Blokace nevyžádané pošty a phishingu bez potřeby manuálně upravovat SCL (Spam Confidenace Level) hodnoty
- Možnost vytváření vlastních pokročilých antispamových pravidel (vyhodnocení více podmínek v jenom pravidlu)
- Kontrola jednotlivých MBX databází, případně konkrétní schránky uživatele
- Umožnit uživateli poštovní schránky pracovat pomocí samostatného prohlížeče se spamovými a potenciálně infikovanými zprávami, které nebyly doručeny do emailové schránky
- Možnost vlastních pravidel s vlastním hodnocením obsahu
- Detekce škodlivých souborů v reálném čase
- Možnost správy přes příkazovou řádku (Podpora edice Windows Server Core)
- **Komplexní protokoly blokovaného spamu a zobrazení greylistingovaných odesílatelů; protokoly všech zpráv, nejen blokovaných**
- Sledování výkonu serveru v reálném čase
- Možnosti pro nastavení pravidel inspekce souborů – mazání spustitelných souborů, skriptů atp.
- Cloudová reputační služba pro kontrolu příloh emailových zpráv
- **Možnost spravovat ochranu na Exchange Serveru samostatně nebo prostřednictvím management konzole v cloudu**
- Možnost exportu protokolu událostí produktu do protokolu operačního systému
- **Tvorba pravidla "Z hlavičky" a vyhodnocovat pole From: pro přesnější detekci podvržených e-mailů**
- Backscatter ochrana
- Synchronizace lokální karantény zpráv napříč uzly clusteru
- **Podpora hybridního prostředí s možností kontroly poštovních schránek v Office 365**
- Možnost zasílání přehledů o zachycených e-mailových hrozbách koncovým uživatelům
- Možnost zabezpečit heslem ochranu poštovního serveru a jeho komponent proti náhodné či chtěné modifikaci neautorizovaného uživatele
- Možnost zabezpečení heslem musí být možné přes konzoli dočasně deaktivovat pro vybrané uživatele na základě ověření administrátora vůči doméně
- Správa karantény prostřednictvím webového portálu pro vybrané uživatele i administrátory
- Ochrana nastavení dodatečným heslem před neoprávněnou změnou konfigurace produktu
- Možnost editovat zasílané zprávy o stavu karantény a zachycených souborů v karanténě (editace těla emailu, předmětu a odkazu na blokovaný e-mail)
- součástí e-mailové ochrany je také integrovaná funkce cloudového sandboxu, tzn. cloudový sandbox nemá vlastního agenta, nevyžaduje instalaci další komponenty ať už v rámci produktu nebo implementace HW prvku do sítě
- **Data odesílané v rámci cloudového sandboxu jsou zpracovávány v rámci EU**
- Sandbox umožňující spuštění vzorků malwaru pro: Windows, macOS, Linux

- Možnost využití na koncových bodech a Exchange serveru pro aktivní detekci škodlivých souborů v e-mailech
- Analýza neznámých vzorků v řádu jednotek minut
- Optimalizace pro znemožnění obejití anti-sandbox mechanismy
- Schopnost analýzy rootkitů a ransomwaru
- Schopnost detekce a zastavení zneužití nebo pokusu o zneužití zero day zranitelnosti
- Řešení pracuje s behaviorální analýzou
- Kompletní výsledek o zanalyzovaném souboru dostupný v centrálním managementu včetně informace o nalezeném i nenalezeném škodlivém chování daného souboru
- Možnost manuálního odeslání vzorku do sandboxu
- Možnost proaktivní ochrany, kdy je potenciální hrozba blokována, dokud není znám výsledek analýzy ze sandboxu
- Neomezené množství odesílaných souborů
- Veškerá komunikace probíhá šifrovaným kanálem
- Možnost okamžitého odstranění souboru po dokončení analýzy z cloudovém sandboxu
- Možnost volby, jaké kategorie souborů do cloudového sandboxu budou odcházet (spustitelné soubory, archivy, skripty, pravděpodobný spam, dokumenty atp.)
- Velikost odeslaných souborů do cloudového sandboxu může dosahovat až 64MB.
Ochrana pro cloudový e-mail a cloudová úložiště v Microsoft 365 a Google Workspace
Řešení poskytuje komplexní ochranu pro cloudové aplikace v Microsoft 365
Exchange Online
Business OneDrive
SharePoint Online
Microsoft Teams
Řešení poskytuje komplexní ochranu pro prostředí Google Workspace
Gmail
Google Drive
Nezávislá cloudová správa pro vyhodnocení zachycených hrozeb
Neinvazivní technologie – nesmí při nedostupnosti ovlivnit fungování samotného M365 nebo Google tenantu
Funkce Antimalware, Antispam, Antiphishing
Detekce útoků využívající homoflyf technik, skenování QR kódů
Možnost zasílání pravidelných reportů
Vícenásobná kontrola podezřených emailů
Export událostí, detekcí a audit logů přes Syslog
Možnost ochránit celý tenant nebo jednotlivé uživatele
Automatická aplikace ochrany pro nově vzniklé uživatele v MS365 nebo Google Workspace
Integrovaná funkce analýzy neznámých vzorků v prostředí cloudového sandboxu
Systém pro detekci a správu zranitelností a záplat
Řešení je součástí agenta poskytovatele bezpečnostní platformy bez nutnosti instalace dalších komponent
Podpora operačních systémů Windows, Linux a MacOS

Integrován v centrálním managementu bezpečnostního nástroje výrobce
Všechny detekované zranitelnosti a jejich dostupné záplaty jsou spravované přes centrální správu výrobce bezpečnostního řešení
informace o zranitelnosti je ve standardizovaném formátu CVE včetně data zařazení zranitelnosti, její povahy a odkaz na zdroj popisující zranitelnost
každá zranitelnost musí mít „bezpečnostní skóre“ dle databáze CVSS 3.0 či novější
možnost ručního spuštění záplaty podporované aplikace
možnost automatického spuštění záplaty podporované aplikace podle časových kritérií s možností vybrání aplikací logikou blacklist/whitelist
možnost automatizovaného spuštění záplaty vybrané aplikace podle vydefinované podmínky (např. podle skóringu zranitelnosti, podle konkrétních CVE, podle konkrétních verzí aplikací)
V případě potřeby restartu zařízení je možné uživateli umožnit restart odložit
V případě potřeby restartu aplikace je uživatel informován o této potřebě a aplikace není bez vyzvání rovnou restartována
Automatické záplatování Windows OS s možností definice typ aktualizací kritických/důležitých updatů
Možnost definovat minimální prostor na disku pro stáhnutí a aplikaci záplat
Vynucení instalace záplaty po uplynutí stanovené lhůty
Možnost spustit sken zranitelností na vyžádání
Správa mobilních zařízení (MDM) a antivirová ochrana
Požadavky na MDM
Zařízení je možné centrálně spravovat pomocí management konzole výrobce bezpečnostního řešení
Podpora MDM pro operačních systémy Android, iOS a iPadOS
Možnost zaregistrovat zařízení v režimu vlastníka nebo ABM
Application control s možností vynucení požadovaných aplikací
Lokalizace zařízení
Podpora anti-theft akcí (siréna, zámek telefonu, vzdálené smazání dat)
Detekce roamingu
Konfigurace restrikcí
Vynucení složitosti zámku obrazovky zařízení
Správa účtů (email, LDAP, Exchange,..)
Integrace s managementem zařízení Microsoft Intune
WebControl s možností filtrování obsahu webu
Filtrování hovorů a SMS s definicí časových slotů pro uplatnění pravidel
správa aktualizací systému
Ochrana před výměnou SIM karty (definice důvěryhodné SIM)
Možnost definovat informace na zamčené obrazovce (kontaktní údaje společnosti)
Požadavky na antivirové zabezpečení
Podpora antivirového zabezpečení pro operační systém Android
Rezidentní ochrana běžící a chránící zařízení v reálném čase
Možnost definice naplánovaných kontrol
Možnost kontroly výměnných zařízení

Detekce potenciálně nechtěných aplikací
Definice aktualizačního serveru
Antiphishing ochrana
Detekce phishingových URL v SMS zprávách
Instalace a odinstalace aplikací 3. stran.
Vyčítání informací o verzích softwaru 3. stran.
Možnost vyčítat informace o hardwaru na spravovaných zařízeních

Příloha č. 3 – Seznam poddodavatelů



Příloha č. 4 – Čestné prohlášení o dodržení zásad odpovědného veřejného zadávání

• Účastník (v této smlouvě také jako „Dodavatel“) tímto čestně prohlašuje, že nabízené plnění, které je předmětem výše uvedené veřejné zakázky neobsahuje v žádné své části látky, které jsou zařazeny na seznam látek vzbuzujících mimořádné obavy (SVHC), určených podle článku 57 nařízení (ES) č. 1907/2006 (nařízení REACH), včetně látek případně doplněných na seznam pro případné zahrnutí do přílohy XIV.

• Účastník tímto čestně prohlašuje, že zajistí dodržování pracovněprávních předpisů, zejména zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (se zvláštním zřetelem na regulaci odměňování, pracovní doby, doby odpočinku mezi směnami atp.), zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů (se zvláštním zřetelem na regulaci zaměstnávání cizinců), a to vůči všem osobám, které se na plnění zakázky podílejí a bez ohledu na to, zda jsou práce na předmětu plnění prováděny bezprostředně dodavatelem či jeho poddodavateli.

• Účastník tímto čestně prohlašuje, že zajistí dodržování mezinárodních úmluv o lidských právech, sociálních či pracovních právech, zejména úmluv Mezinárodní organizace práce (ILO).

• Účastník tímto čestně prohlašuje, že zohlední při plnění této zakázky dopady na životní prostředí, a to zejména požadavky na dlouhou životnost, požadavky na demontovatelnost, opravitelnost, modulárnost, ekoznačky (například certifikáty na dřevo FSC nebo PEFC) apod. Dodavatel bude při výrobě a dodávce předmětu této zakázky preferovat ekologicky šetrná řešení a minimalizovat vznik odpadu a obalových materiálů. Dodavatel bude likvidovat odpad a obalové materiály ekologicky. Pokud to bude možné, dodavatel se zavazuje kromě vlastní výroby použít metodu výroby z recyklátu, metodu repase anebo metodu redesignu.