Příloha č. 4.1 zadávací dokumentace – Návrh smlouvy na plnění zakázky

SMLOUVA
o dodávce a implementaci IT infrastruktury

uzavřená níže uvedeného dne, měsíce a roku

dle ustanovení § 1746 a násl. zákona č. 89/2012 Sb., Občanského zákoníku

1) Smluvní strany

Kupující:	**Město Kadaň**	
	Sídlo:	432 01 Kadaň, Mírové náměstí 1
	IČO / DIČ:	00261912 / CZ00261912
	Zastoupený:	Mgr. Janem Losenickým, starostou města
	Kontaktní osoba:	Ing. Petr Panuška, vedoucí odboru vnitřních věcí
	Bankovní spojení:	Komerční banka a.s.; č.ú.: 1725441/0100
	jako kupující, na straně jedné	
	(dále jen kupující)	

a

Prodávající:	**O2 Czech Republic a.s.**	
	Se sídlem / místem podnikání:	Za Brumlovkou 266/2, 140 22, Praha 4 - Michle
	IČO / DIČ:	60193336 / CZ60193336
	Zastoupený/jednající: pověření ze dne 01.12.2023	Bc. Jitka Marešová, Account Manager, na základě
	Bankovní spojení:	Komerční banka, č.ú. 27-4908440207/0100
	Zapsán v obchodním rejstříku, vedeném u městského soudu v Praze, oddíl B, vložka 2322	
	Zhotovitel je plátce DPH:	ANO
	Kontaktní osoba:	Bc. Jitka Marešová
	Telefon:	+420 734 273 238
	E-mail:	jitka.maresova@O2.cz
	jako prodávající na straně druhé	
	(dále jen prodávající)	

2) Účel smlouvy

2.1 Tato smlouva je uzavírána v návaznosti na veřejnou zakázku s názvem „**Zajištění kybernetické bezpečnosti pro město Kadaň**“, zadávanou zadavatelem (dále jen také „Zakázka“). Kupující připomíná, že Zakázka je vedena potřebou kupujícího (coby zadavatele) zajistit takové plnění, které bude v souladu s příslušným projektem. Předmětem Zakázky je tedy dodávka a implementace opatření v oblasti kybernetické bezpečnosti s cílem posílit zabezpečení informačních a komunikačních systémů městského úřadu, a tedy zesílit schopnost a připravenost městského úřadu předcházet kybernetickým útokům a dalším potenciálním hrozbám. Technická specifikace požadovaného řešení reflektuje především záměr centrálního řízení a sjednocení konfigurační správy aktivních síťových prvků a s tím související nasazení systému pro řízení přístupu koncových stanic a uživatelů a centrálního systému pro sběr a uchovávání logů z aktivních síťových prvků a koncových stanic.

Všechny zamýšlené aktivity projektu musí mít přímou vazbu na zvýšení úrovně kybernetické bezpečnosti dle mezinárodních standardů. Základní standardy dosahování kybernetické bezpečnosti ICT systémů formuluje zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii („Směrnice NIS“)

2.2 Podkladem pro uzavření této smlouvy je, ač k ní pevně jako její příloha vzhledem k jejímu rozsahu nepřipojena, je také zadávací dokumentace kupujícího (coby zadavatele Zakázky) pro Zakázku ve znění případných pozdějších úprav a upřesnění, např. po žádostech o dodatečné informace, (dále také jen „Zadávací dokumentace“), a v rámci Zadávací dokumentace pak zejména **Technická specifikace kupujícího (zadavatele)**, která bude při sporech o výklad této smlouvy závazným vodítkem**.** Podkladem pro uzavření této smlouvy je pak také nabídka prodávajícího (coby účastníka, resp. vybraného dodavatele Zakázky) podaná v rámci zadávacího řízení na Zakázku (dále jen také „Nabídka“). Nabídka prodávajícího je také závazným vodítkem v případě sporného výkladu této smlouvy, ač k ní také není vzhledem k jejímu rozsahu pevně připojena, jako její příloha. V případě rozporu Nabídky prodávajícího s podklady kupujícího (zejm. se Zadávací dokumentací), mají ovšem přednost podklady kupujícího.

2.3 Prodávající prohlašuje, že se důkladně a podrobně seznámil v rámci zadávacího řízení s celou zadávací dokumentací. Předpokládá se tedy, že prodávající, podáním své nabídky a podpisem této smlouvy, se coby osoba odborně způsobilá, podrobně seznámil se všemi informacemi, údaji a jinými dokumenty, které byly součástí zadávací dokumentace nebo byly v souvislosti s ní kupujícím poskytnuty. Dále se pak předpokládá, že pokud některé informace, údaje nebo hodnoty dodané kupujícím (coby zadavatelem) byly nedostatečné, nekompletní nebo nepřesné do té míry, že by to mohlo ovlivnit řádné plnění zakázky, měl v takovém případě možnost (v návaznosti na jeho odbornost a na ust. § 2594 obč. zák., resp. § 4 a 5 obč. zák. a § 98 ZZVZ) upozornit kupujícího (zadavatele), resp. vznést žádost o dodatečné informace, resp. upřesnění k zadávacím podmínkám a že tak učinil; pokud tak neučinil, bylo to z toho důvodu, že uvedené informace, údaje nebo hodnoty dodané kupujícím (zadavatelem) neshledal jako nedostatečné, nekompletní nebo nepřesné.

3) Vlastnické vztahy

3.1 Prodávající prohlašuje, že je výlučným vlastníkem movitého předmětu koupě a jeho příslušenství, resp. oprávněným poskytovatelem nehmotného předmětu koupě.

3.2 Detailní technická specifikace předmětu plnění této smlouvy a počtu kusů jednotlivého zboží a jeho příslušenství je obsažena v příloze č. 1, č. 2 a č. 3 této smlouvy a je její nedílnou součástí. V případě rozporu vzniklého mezi přílohami č. 1 a 2 této smlouvy v podobě technické specifikace platí vždy specifikace kupujícího obsažená v příloze č. 1 této smlouvy.

4) Předmět plnění

4.1 Předmětem plnění dle této smlouvy je hmotný majetek v podobě zařízení (dále jen také „zařízení“) a nehmotný majetek v podobě licencí k software (dále jen také „licence“, „SW“), obojí včetně příslušenství. Předmět plnění je detailně specifikován v příloze č. 1 a č. 3 této smlouvy, včetně příslušenství. Prodávající je tímto povinen odevzdat kupujícímu zařízení, resp. dodat SW a poskytnout k němu licence, a umožnit mu nabytí vlastnického práva k zařízení, resp. oprávnění užívat SW, a současně závazek kupujícího Předmět plnění převzít a zaplatit za něj prodávajícímu kupní cenu.

Předmět plnění této Smlouvy je spolufinancován prostřednictvím Národního plánu obnovy (NPO) ve výzvě č. 41 „Kybernetická bezpečnost – obce“ v rámci projektu „Zajištění kybernetické bezpečnosti pro město Kadaň, reg. č.: CZ.31.2.0/0.0/0.0/23_093/0008377.

4.2 Součástí Předmětu plnění jsou dále služby a práce prodávajícího, zejm. instalace, implementace a montáž, s Předmětem plnění přímo související a nezbytné k jeho řádnému uvedení do provozu, blíže specifikované v příloze č. 1 této smlouvy (dále jen také společně „služby“). Bez provedení těchto služeb nebude Předmět plnění považován za řádně dodaný.

4.3 Prodávající se zavazuje dodat Předmět plnění kupujícímu s veškerými doklady nutnými k převzetí a zejména k užívání dodaných zařízení a software a provést všechny požadované související služby. Prodávající se zavazuje dodat zařízení nové, nepoužité, nerepasované, nezatížené jakýmkoli právy třetích osob, a dodat SW, resp. poskytnout licence, aniž by jakkoli porušil jakákoli práva třetích osob.

4.4 Prodávající touto smlouvou tedy odevzdává kupujícímu do výlučného vlastnictví zařízení, a to včetně příslušenství a Kupující jej kupuje za dohodnutou cenu a přijímá do svého výlučného vlastnictví.

4.5 Prodávající prohlašuje, že neví ke dni podpisu této kupní smlouvy o žádných vadách Předmětu plnění, na které by kupujícího měl upozornit.

4.6 Prodávající se zavazuje k řádnému a úplnému splnění Předmětu plnění (řádnému a úplnému dodání) tedy tak, aby odpovídal příslušným právním předpisům, podmínkám této smlouvy, technickým normám i doporučujícím a obchodním zvyklostem a aby jej bylo možné užívat za účelem, ke kterému je kupujícím určen a požadován.

4.7 Prodávající prohlašuje, že Předmět plnění splňuje technické, hygienické, humánní, bezpečnostní a další standardy dle předpisů Evropské unie a odpovídá požadavkům

stanoveným právními předpisy České republiky, harmonizovanými českými technickými normami a ostatními ČSN, které se vztahují k Předmětu plnění.

4.8 Předmětem plnění je dále také:

a) dodávka, instalace, implementace a montáž všech dalších přímo souvisejících přístrojů a prvků souvisejících s Předmětem plnění, nutných k uvedení Předmětu plnění do provozu, neuvedených přímo v Příloze č. 1 této smlouvy tak, aby byl naplněn účel smlouvy; případné vícenáklady související s plněním dle tohoto odstavce budou řešeny dodatek k této smlouvě při respektování § 222 ZZVZ.

b) provedení veškerých předepsaných zkoušek včetně vystavení dokladů o jejich provedení, doložení atestů, certifikátů, prohlášení o shodě a podobných listin, a jejich předání zadavateli ve 3 vyhotoveních v českém jazyce;

c) provedení zaškolení pracovníků zadavatele k používání Předmětu plnění, případně dalších činností, nutných k jeho provozu, a popsaných v jeho technické specifikaci, uvedené v Příloze č. 1 této smlouvy, jako součást předmětu plnění. O zaškolení a provedení uvedených činností bude stranami sepsán protokol;

d) doprava do sídla kupujícího, pojištění spojené s dodávkou, veškeré poplatky spojené s dovozem, resp. odevzdáním Předmětu plnění, cla, daně, dovozní a vývozní přirážky až do jeho funkčního předání v místě plnění, licenční a veškeré další poplatky spojené s dodávkou a následným užíváním Předmětu plnění, technická dokumentace - prohlášení o shodě a uživatelské příručky v českém jazyce (2x v písemné podobě a 1x elektronicky); součástí plnění je i předání všech vstupních a přístupových adres, uživatelských jmen, hesel či kódů nutných k ovládání a servisu dodaného Předmětu plnění, jakož i veškerého software, potřebného ke stejné činnosti;

e) plný záruční servis zařízení a souvisejícího vybavení v záruční době (tzn. plné servisní pokrytí včetně dodávky všech náhradních dílů).

5) Licence

5.1 Prodávající v rámci plnění této smlouvy dodává software podléhající ochraně podle zákona č. 121/2000 Sb. (autorský zákon) a ustanovení § 2358 a následující zákona č. 89/2012, občanského zákoníku, proto poskytuje kupujícímu licenci (tj. oprávnění k výkonu práva duševního vlastnictví (licenci) v ujednaném rozsahu), a to formou licenčního ujednání v této kupní smlouvě. Prodávající prohlašuje, že se jedná o licenci:

a) nevýhradní k veškerým známým způsobům užití takového software, a to v rozsahu minimálně nezbytném pro řádné užívání software kupujícím dle účelu této smlouvy;

b) neomezenou územním či množstevním rozsahem (není-li v této smlouvě uvedeno jinak) a rovněž tak neomezenou způsobem nebo rozsahem užití;

c) udělenou na dobu určitou, tedy po dobu držení vlastnických práv,

d) převoditelnou a postupitelnou, tj. která je udělena s právem postoupení třetí osobě

e) kterou není kupující povinen využít.

5.2 Licence je poskytnutá v maximálním rozsahu povoleném platnými právními předpisy.

5.3 Prodávající prohlašuje, že odměna za poskytnutí licence kupujícímu je již zahrnuta v ceně plnění za poskytnuté plnění dle této smlouvy.

6) Cena plnění a platební podmínky

6.1 Cena plnění (dále jen také „Cena“) je nabídkovou cenou předloženou prodávajícím v jeho nabídce na veřejnou zakázku uvedenou v článku 0 této smlouvy, přičemž se skládá z ceny dodávky jednotlivých zařízení a poskytnutí licencí.

6.2 Kupující se zavazuje zaplatit prodávajícímu za Předmět plnění dle této smlouvy Cenu ve výši:

5 687 000,- Kč bez DPH,

tj. 6 881 270,- Kč včetně DPH,

když DPH ve výši 21 % činí 1 194 270,- Kč.

6.3 Cena je stanovena jako konečná a úplná, zahrnuje veškeré dodávky, služby s dodávkami související, poskytnutí příslušných práv dle této smlouvy, a veškeré jiné náklady nezbytné pro řádnou a úplnou realizaci Předmětu plnění včetně všech rizik a vlivů s plněním této smlouvy souvisejících. Kompletní skladba Ceny a její rozklad je obsažen v příloze č. 3 této smlouvy.

6.4 Prodávající není oprávněn požadovat po kupujícím poskytnutí zálohy.

6.5 Prodávající na sebe bere odpovědnost za to, že sazba a výše daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy. V případě, že dojde mezi dnem podpisu kupní smlouvy a dnem uskutečnění zdanitelného plnění ke změně sazby DPH podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, bude daň z přidané hodnoty připočtena ke kupní ceně ve výši dle právní úpravy platné ke dni uskutečnění zdanitelného plnění.

6.6 Cenu zaplatí kupující prodávajícímu bankovním převodem na bankovní účet prodávajícího uveden v článku 1 této smlouvy na základě daňového dokladu (faktury) vystaveného prodávajícím ke dni uskutečnění zdanitelného plnění, který je dnem podepsání předávacího protokolu na Předmět plnění. Daňový doklad je považován za proplacený okamžikem odepsání příslušné částky z účtu kupujícího ve prospěch účtu prodávajícího.

6.7 Prodávající na základě svého práva vystavit daňový doklad (fakturu) vystaví samostatnou fakturu za Předmět plnění.

6.8 Na daňovém dokladu (faktuře) bude uveden rozklad fakturované částky na jednotlivá zařízení, SW, resp. licence tak, aby byly zřejmé jednotlivé ceny (zařízení, SW, resp. licence) a tak aby bylo kupujícímu usnadněno zavedení do majetkové evidence. Součástí daňového dokladu rovněž musí být název projektu *„Zvýšení kybernetické bezpečnosti města Kadaň“* a číslo projektu CZ.31.2.0/0.0/0.0/23_093/0008377.

6.9 Splatnost daňového dokladu je 30 dnů ode dne jeho doručení kupujícímu.

6.10 Daňový doklad bude obsahovat náležitosti daňového a účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, bude mít náležitosti obchodní listiny dle § 435 zákona č. 89/2012 Sb., občanského zákoníku. V případě, že daňový doklad takové náležitosti nebude splňovat, bude kupujícím vrácen do dne splatnosti daňového dokladu k opravení bez jeho proplacení. V takovém případě lhůta splatnosti počíná běžet znovu ode dne doručení opraveného či nového vyhotovení daňového dokladu.

6.11 Pro případ, že prodávající je, nebo se od data uzavření smlouvy do dne uskutečnění zdanitelného plnění stane na základě rozhodnutí správce daně „nespolehlivým plátcem“ ve smyslu ustanovení § 106a zákona č. 235/2004 Sb., o DPH, ve znění pozdějších předpisů, souhlasí prodávající s tím, že mu kupující uhradí cenu plnění bez DPH a DPH v příslušné výši odvede za nespolehlivého plátce přímo příslušnému správci daně. V souvislosti s tímto ujednáním nebude prodávající vymáhat od kupujícího část z ceny plnění rovnající se výši odvedeného DPH a souhlasí s tím, že tímto bude uhrazena část jeho pohledávky, kterou má vůči kupujícímu, a to ve výši rovnající se výši odvedené DPH.

7) Předání a převzetí věci a vlastnické právo

7.1 Prodávající předá kupujícímu Předmět plnění nejpozději do 31.12.2025, a to včetně realizace všech souvisejících služeb. Bez dodávky příslušenství a realizovaného požadovaného rozsahu služeb nebude možné ze strany kupujícího považovat předmětu plnění za realizovaný a předmět koupě nebude z jeho strany možné převzít.

7.2 Místem dodání a předání Předmětu plnění je sídlo kupujícího, resp. jím využívané prostory ve městě a bude kupujícím konkrétně uvedeno. Před zahájením plnění je tedy prodávající povinen vyzvat kontaktní osobu kupujícího k potvrzení rozdělení jednotlivých dodávek mezi jednotlivé lokality kupujícího.

7.3 Vlastnické právo k zařízení přechází na kupujícího v okamžiku jeho předání prodávajícím a převzetí kupujícím potvrzeného na předávacím protokolu.

7.4 Nebezpečí nahodilé zkázy a nahodilého zhoršení vlastností zařízení včetně užitku přechází na kupujícího současně s nabytím vlastnictví.

7.5 Náklady spojené s předáním Předmětu plnění, zejména dopravu, nese prodávající a náklady spojené s převzetím nese kupující.

7.6 O předání a převzetí Předmětu plnění a souvisejících dokladů bude sepsán předávací protokol podepsaný zástupci obou smluvních stran. Za kupujícího je předávací protokol oprávněn podepsat a Předmět plnění převzít kontaktní osoba kupujícího uvedená v článku 1. této smlouvy.

7.7 Prodávající splní svou povinnost řádně a úplně dodat Předmět plnění splněním všech závazků dle této smlouvy, tedy zejm. jeho dodáním do místa plnění, montáží, nainstalováním, uvedením do provozu a zaškolením obsluhy tak, jak předpokládá tato smlouva, a dále předáním všech listin, osvědčení a dokumentů, které právní předpisy k provozování příslušných částí Předmětu plnění vyžadují nebo kterých je k jejich provozování zapotřebí (včetně návodů k obsluze a podobně).

7.8 Pokud se týče příslušného SW, splní prodávající svou povinnost takový SW dodat okamžikem, kdy takové SW nainstaluje do příslušného zařízení případně dalších přístrojů kupujícího, do kterých to bude potřebné pro uvedení zařízení do plně funkčního provozu v návaznosti na ostatní vybavení kupujícího, takový SW plně zprovozní (včetně synchronizace s ostatním potřebným software a technickým vybavením kupujícího) a převede na kupujícího licenční práva k plnému užívání takového SW za účelem potřebným pro realizaci záměru kupujícího, pro který je kupujícím pořizován, tedy nejpozději podpisem protokolu o předání a převzetí Předmětu plnění.

7.9 Smluvní strany se výslovně dohodly, že před obdržením pokynu kupujícího k poskytnutí plnění není prodávající oprávněn Předmět plnění dle této smlouvy dodat a kupující jej převzít, nedohodnou-li se jinak.

8) Součinnost

Kupující požaduje, aby maximum prací odvedl prodávající samostatně, bez zatěžování pracovníků kupujícího. Kupující poskytne maximální součinnost s ohledem na jeho kapacitní a časové možnosti.

9) Projektový tým (seznam techniků)

9.1 Prodávající se zavazuje předmět plnění smlouvy realizovat prostřednictvím projektového týmu (seznamu techniků), kterým prokázal kvalifikaci v Zakázce. Projektový tým (seznam techniků) prodávajícího je odpovědný za plnění této smlouvy.

9.2 Prodávající se zavazuje realizovat předmět plnění této smlouvy prostřednictvím projektového týmu (seznamu techniků) v tomto složení na těchto pozicích:

Projektový manažer: Ing. Petr Mlateček

Technický specialista bezpečnosti: Matěj Kouba

Technický specialista – síťových technologií: Ing. Pavel Potůček

9.3 Změna konkrétní osoby na pozici člena projektového týmu prodávajícího je možná pouze za předpokladu prokázání potřebné kvalifikace novou osobou v rozsahu stanoveném pro danou pozici člena projektového týmu stanovenou ve veřejné zakázce, na jejímž základě je uzavřena tato smlouva. Taková změna musí být prodávajícím řádně iniciována, písemně dokladována a prokázána kvalifikace nové osoby na pozici člena projektového týmu před jeho zapojením do realizace plnění dle této smlouvy (včetně všech souvisejících požadavků na projektový tým stanovený v zadávacích podmínkách, na jejichž základě je uzavřena tato smlouva, jako např. max. počet pozic obsazených jednou osobou apod.).

10) Další práva a povinnosti smluvních stran

10.1 Prodávající se dále zavazuje předat kupujícímu listinné potvrzení dodaných licencí, které jsou Předmětem plnění.

10.2 Prodávající se zavazuje v rámci realizace plnění dodržovat veškeré předpisy, a požadavky výzvy dotačního titulu Národního plánu obnovy v oblasti kybernetické bezpečnosti.

10.3 Prodávající je povinen zajistit i veškerá bezpečnostní opatření na ochranu osob a majetku v areálu kupujícího, jsou-li tato dotčena dodáním zboží prodávajícího.

10.4 Prodávající je povinen k náhradě újmy způsobené činností svou i svých poddodavatelů.

10.5 Prodávající je povinen k náhradě újmy způsobné okolnostmi, které mají důvod v povaze strojů, přístrojů nebo jiných věcí, které prodávající použil.

10.6 Smluvní strany sjednávají, že prodávající není oprávněn započíst si jakoukoliv svoji peněžitou pohledávku za kupujícím, a to ani část své pohledávky, včetně pohledávek získaných postoupením, vůči jakékoliv peněžité pohledávce kupujícího za prodávajícím.

10.7 Prodávající není oprávněn postoupit jakoukoliv svoji pohledávku, a to ani část pohledávky, za kupujícím, která vznikne na základě a/nebo v souvislosti s touto smlouvou, ani k ní zřídit smluvní zástavní právo, ani postoupit svoje smluvní postavení z této smlouvy na třetí osobu.

10.8 Prodávající je povinen uchovávat veškerou dokumentaci související s realizací projektu (Předmětu plnění včetně účetních dokladů minimálně do konce roku 2040.

10.9 Prodávající je povinen minimálně do konce roku 2040 poskytovat požadované informace a dokumentaci související s realizací projektu (Předmětu plnění) 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 (Předmětu plnění) a poskytnout jim při provádění kontroly součinnost.

10.10 Zhotovitel předloží objednateli při podpisu této smlouvy doklad o uzavření pojistné smlouvy pro případnou újmu způsobenou kupujícímu v souvislosti s plněním této smlouvy s minimálním limitem plnění z případné škodní události ve výši 10.000.000,- Kč.

11) Práva z vadného plnění a smluvní záruka

11.1 Kupující požaduje a prodávající se zavazuje držet záruku na Předmět plnění (zařízení) této smlouvy, není-li uvedeno dále jinak, v délce poskytované výrobcem, resp. dodavatelem takového zařízení, minimálně však v délce 60 měsíců. Prodávající se dále v rámci prvních dvou let běhu této záruky zavazuje zajistit provedení zpětné montáže opraveného nebo nahrazeného zařízení z důvodu jeho vady, a to včetně provedení jeho konfigurace, ať už nahráním konfiguračního souboru nebo jinou vhodnou cestou.

11.2 Záruka na jednotlivá zařízení a služby počíná svůj běh dnem jejich předání kupujícímu na základě řádně oběma smluvními stranami podepsaného předávacího protokolu.

11.3 Prodávajícím poskytnutá záruka dle této smlouvy se vztahuje na funkčnost dodaného plnění, jakož i na jeho vlastnosti požadované kupujícím.

11.4 Na příslušenství a služby (provedené implementační a konfigurační práce) bude prodávajícím poskytována záruka v délce 24 měsíců. V případě vad příslušenství se prodávající zavazuje provést opravu nebo věc nahradit novou do 60 kalendářních dnů ode dne nahlášení vady kupujícím v sídle kupujícího. V případě vad provedených implementačních a konfiguračních prací se prodávající zavazuje provést opravu do 30 kalendářních dnů ode dne nahlášení vady kupujícím v místě plnění.

11.5 Po celou záruční dobu na samotná zařízení podle této smlouvy prodávající garantuje kupujícímu přijmout od něj nahlášení poruchy a garantuje realizaci opravy technikem v místě dodávky, a to nejpozději do 4 pracovních dnů od nahlášení.

11.6 Prodávající odpovídá kupujícímu za to, že dodaný předmět smlouvy bude mít vlastnosti zabezpečující jeho řádné užívání, stanovené v minimální konfiguraci v technické specifikaci kupujícího a v konečné konfiguraci ve specifikaci obsažené v nabídce prodávajícího.

11.7 Prodávající odpovídá kupujícímu dále za to, že dodaný Předmět plnění bude mít vlastnosti zabezpečující jeho řádné užívání a že je bez právních a faktických vad.

11.8 Prodávající se zavazuje zajistit, že veškerá komunikace na základě této kupní smlouvy bude z jeho strany vedena v českém jazyce, a to včetně uplatňování a řešení závad a reklamací jednotlivých zařízení a licencí na základě této smlouvy.

11.9 Vady musí kupující uplatnit u prodávajícího bez zbytečného odkladu poté, co se o nich dozví.

11.10 Uplatněním práv z odpovědnosti za vadné plnění není dotčeno právo kupujícího na náhradu škody.

12) Smluvní pokuty

12.1 Pro případ prodlení se zaplacením Ceny se kupující zavazuje uhradit prodávajícímu smluvní pokutu ve výši 0,01 % z fakturované ceny za každý den prodlení.

12.2 Nesplní-li prodávající svůj závazek dodat předmět plnění řádně a včas jako celek, je oprávněn kupující požadovat po prodávajícím (nad rámec smluvních pokut za nedodržení plnění dle termínů harmonogramu) zaplacení jednorázové smluvní pokuty ve výši 50.000,- Kč za nedodržení termínu plnění a dále k tomu smluvní pokuty ve výši 0,1 % ze sjednané ceny plnění dle této smlouvy za každý započatý den prodlení, až do řádného dokončení a předání celého předmětu plnění a prodávající je povinen takto požadovanou smluvní pokutu zaplatit.

12.3 V případě prodlení prodávajícího s odstraněním nahlášené závady ve lhůtě uvedené v čl. 11.5 smlouvy má kupující nárok na smluvní pokutu ve výši 1000,- Kč za každý, i jen započatý, den prodlení prodávajícího s odstraněním nahlášené závady.

12.4 V případě prodlení prodávajícího s odstraněním nahlášené závady na příslušenství se stanovuje smluvní pokuta ve výši 500,- Kč za každý i jen započatý den prodlení.

12.5 V případě prodlení prodávajícího s odstraněním nahlášené závady v podobě provedených implementačních a konfiguračních prací se stanovuje smluvní pokuta ve výši 500,- Kč za každý i jen započatý den prodlení.

12.6 V případě realizace předmětu plnění této smlouvy projektovým týmem prodávajícího v jiném složení, než které je uvedeno v článku 0 této smlouvy, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 20.000,- Kč za každý zjištěný případ.

12.7 V případě nedodržení komunikace v českém jazyce na základě této smlouvy podle článku 0 smlouvy je kupující oprávněn vyúčtovat smluvní pokutu ve výši 1.000,- Kč za každý případ.

12.8 Zaplacením smluvní pokuty nezaniká povinnost druhé strany závazek splnit a není tím dotčeno právo poškozené strany na náhradu škody, které nesplněním povinnosti vznikla.

12.9 Základem pro výpočet smluvní pokuty je na základě dohody smluvních stran cena v Kč včetně DPH. Výši smluvních pokut shodně považují obě smluvní strany za přiměřené. Smluvní pokuta je splatná do 30-ti dnů od doručení jejího vyúčtování.

13) Odstoupení od smlouvy

13.1 Odstoupení od smlouvy se řídí ustanoveními § 223 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, a dále § 2001 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů.

13.2 Nebude-li uhrazena Cena, na jejíž zaplacení vznikne oprávněný nárok, do 60 dnů ode dne splatnosti daňového dokladu prodávajícímu v důsledku zavinění kupujícího a ani do dalších 15 dnů po opakovaném vyzvání prodávajícím k takové úhradě, sjednává si prodávající právo odstoupit od této kupní smlouvy.

13.3 Právo odstoupit od této kupní smlouvy má kupující tehdy, jestliže jej prodávající ujistil, že Předmět plnění této smlouvy má určité vlastnosti, zejména vlastnosti kupujícím vymíněné, anebo prodávající kupujícího ujistil, že Předmět plnění této smlouvy nemá žádné vady, a toto ujištění se ukáže být nepravdivým.

14) Registr smluv – doložka

14.1 Prodávající tímto uděluje souhlas kupujícímu k uveřejnění všech podkladů, údajů a informací uvedených v této smlouvě, k jejichž uveřejnění vyplývá pro kupujícího povinnost dle právních předpisů.

14.2 Prodávající je současně srozuměn s tím, že kupující je oprávněn zveřejnit obraz smlouvy a jejich případných změn (dodatků) a dalších dokumentů od této smlouvy odvozených včetně metadata požadovaných k uveřejnění dle zákona č. 340/2015 Sb., o registru smluv.

14.3 Zveřejnění smlouvy a metadata v registru smluv zajistí kupující.

15) Závěrečná ustanovení

15.1 Tato smlouva je vyhotovena v elektronickém originále, jenž po podpisu druhou ze smluvních stran obdrží obě smluvní strany. Smluvní strany se dohodly, že k podpisu smlouvy bude použit kvalifikovaný elektronický podpis ve smyslu Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 (eIDAS).

15.2 Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti uveřejněním v registru smluv.

15.3 Právní vztahy touto smlouvou výslovně neupravené a s ní související nebo z ní vyplývající se řídí ustanoveními zákona č. 89/2012 Sb., občanského zákoníku, a to zejména ustanoveními o kupní smlouvě (zejména stran dodávky zařízení), licenční smlouvě (stran poskytnutí licencí k dodanému SW) a přiměřeně o smlouvě o dílo (zejm. stran služeb).

15.4 Tuto smlouvu je možno platně měnit pouze na základě dohody smluvních stran, formou písemných a vzestupně číslovaných dodatků, podepsaných oběma smluvními stranami. Písemná forma je nutná i ke změně ujednání v předchozí větě tohoto odstavce.

15.5 Přílohami této smlouvy jsou:

- Příloha č. 1 – Technická specifikace zadavatele (kupujícího)

- Příloha č. 2 – Technická specifikace účastníka zadávacího řízení (prodávajícího) z jeho vítězné nabídky, včetně jednotkových cen zařízení
- Příloha č. 3 – Cenová tabulka obsahující skladbu nabídkové ceny z nabídky prodávajícího

15.6 Strany této smlouvy berou na vědomí, že kupující jako správce osobních údajů je oprávněn zpracovávat zde uvedené osobní údaje v souladu s článkem 6 odst. 1 písm. b) Obecného nařízení (toto zpracování je nezbytné pro splnění smlouvy) a písm. c) (toto zpracování je nezbytné pro splnění právní povinnosti správce zveřejnit smlouvu na profilu zadavatele dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v registru smluv dle zákona č. 340/2015 Sb., o registru smluv, postupy podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím nebo na své úřední desce dle zákona č. 128/2000 Sb., o obcích).

15.7 V případě, že po podpisu této smlouvy na prodávajícího anebo jeho poddodavatele budou dopadat mezinárodní sankce podle zákona upravujícího provádění mezinárodních sankcí č. 69/2006 Sb. ve smyslu zákona č. 240/2022 Sb. účinného od 1. 9. 2022, je povinen to prodávající písemně oznámit kupujícímu. V případě, že oznámení neprovede a kupující zjistí, že na prodávajícího anebo jeho poddodavatele mezinárodní sankce dopadají, vyzve prodávajícího k vysvětlení nebo nápravě formou vyjmutí osoby ze sankčního seznamu. V případě že náprava není možná, odstoupí kupující od této smlouvy, přičemž účinnost odstoupení nastává doručením odstoupení prodávajícímu.

15.8 Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly a s celým jejím obsahem souhlasí. Dále prohlašují, že tato smlouva vyjadřuje jejich pravou a svobodnou vůli. Na důkaz toho připojují vlastnoruční podpisy na smlouvě.

Tato smlouva byla schválena usnesením rady města č. 84/25 ze dne 13.2. 2025.

Za kupujícího	**Za prodávajícího**
V ..... dne …….	V ..... dne …….
…….	…….
	Bc. Jitka Marešová
	Account Manager na základě pověření ze dne 01.12.2023

Příloha č. 1 smlouvy – Technická specifikace zadavatele (kupujícího)

Předmětem plnění této technické specifikace je dodávka a implementace opatření v oblasti kybernetické bezpečnosti, a to včetně nedílně souvisejících požadavků typu dodání licencí, zaškolení, zpracování dokumentace a služeb technické podpory.

Zadavatel požaduje dodávku jednotlivých komponent dle této technické specifikace včetně příslušenství v níže uvedené minimální specifikaci.

Musí se jednat o zařízení nová, nepoužitá, nerepasovaná a určená pro prodej v České republice.

Dodavatel jednoznačně určí, jaký typ nebo verze nabízeného řešení je předmětem jeho nabídky. V případě, že neexistuje veřejně dostupný podrobný popis nabízeného řešení, který umožní posoudit splnění zadávacích podmínek, je dodavatel povinen připojit tento popis jako součást nabídky.

1. New Generation Firewall

Předmětem veřejné zakázky je dodávka 2 ks Next Generation Firewallů. Dodané řešení musí splňovat následující minimální požadavky:

Plnění parametrů NGFW	Ano/Ne
HW požadavky	**---**
HW zařízení typu NGFW (VM appliance nebo jiné software řešení není akceptovatelné). Součástí nabídky musí být 2 kusy identických zařízení pro využití v režimu HA s licencemi tak, aby byl tento režim plně podporován včetně všech níže požadovaných funkcí.	
Podpora výrobce (min. všechny požadované funkce, aktualizace firmware, technické problémy) po dobu 5 let	
Podpora režimu vysoké dostupnosti minimálně jako active/active a active/passive, HA cluster o dvou fyzických zařízeních. NGFW cluster musí být schopen odbavovat 100% datového toku bez omezení i v případě výpadku jakéhokoliv z HA nodů, překlopení v rámci clusteru musí být plně automatické bez nutnosti jakéhokoliv zásahu administrátora.	
Velikost HW appliance maximálně 1 RU	
Podpora duálního napájení (redundantní zdroj). Zdroje jsou součástí nabízeného zařízení	
Maximalní spotřeba 40W	
Minimálně 4x 10GE SFP+	
Minimálně 8x 1Gbps SFP	
Minimálně 16x 1Gbps GE-RJ45	
Dedikované síťové porty pro HA, management a konzolovou konektivitu	

USB port	
TPM modul pro generování a ukládání kryptografických klíčů	
Výkonové požadavky (výkonové parametry je nutné doložit produktovým listem výrobce, nebo oficiální dokumentací výrobce)	**---**
Požadovaná propustnost poptávaného zařízení pro IPv4 i IPv6 provoz je 39 Gbps (UDP paket o velikosto 512B)	
NGFW propustnost 3 Gbps	
IPS propustnost 5 Gbps (včetně zapnutého logování provozu)	
Threath protection propustnost 2,8 Gbps	
Počet současně navázaných TCP spojení firewallu min. 3 mil.	
Počet nových TCP spojení za sekundu min. 140 000	
Propustnost funkce SSL inspekce 3 Gbps.	
Minimální Počet současně navázaných spojení kontrolovaných pomocí SSL inspekce – 315 000	
Požadavky na VPN funkce	**---**
Minimální propustnost IPSEC VPN 35 Gbps	
Minimální propustnost SSL VPN 1,5 Gbps	
Minimálně 450 současně připojených uživatelů SSL VPN (pokud funkce vyžaduje licenci, musí být součástí nabídky.)	
Klient pro SSL VPN musí je součásti dodávky (bezplatný, případně pro 450 uživatelů)	
Vícefaktorová autentizace pro 20 privilegovaných uživatelů je součástí dodávky - druhý faktor formou OTP mobilní aplikace integrované s dodávaným NGFW řešením (řešení pomocí samostatného IAM řešení není akceptováno)	
Podpora push notifikací u OTP mobilní aplikace bez nutnosti opisovat OTP kód	
Podpora iOS a Android OS u OTP mobilní aplikace	
Požadavky na obecné funkce	**---**
Konsolidované bezpečnostní řešení obecně značené jako firewall nové generace (next generation firewall, NGFW)	
Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů. Klíčovým požadavkem je možnost plnohodnotné správy v rámci GUI i CLI bez nutnosti instalovat management aplikaci na koncovou stanici.	
Podpora logických domén (kontextů) na nabízením fyzickém zařízení v počtu alespoň 10 v ceně nabízeného zařízení; každá logická doména musí pracovat izolovaně s možností propojovat jednotlivé logické domény pomocí interních virtuálních propojů bez nutnosti použití fyzických interface	
Podpora více routovacích kontextů, tzv VRF	
Podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46, plnohodnotná podpora IPv6	
Možnost nasazení ve všech z následujících režimu (kombinace možné pomocí použití různých režimů pro různé logické domény): L2 bridge režim (inline), L3 router/NAT režim (inline), explicitní proxy (inline/out of path), transparentní proxy (inline)	
Plnohodnotná správy z lokálního management rozhraní (a to i v případě využití nástroje centrální správy, neboť i v takovém případě musí být možné firewall, resp. firewall cluster, plnohodnotně konfigurovat ve chvíli, kdy z jakéhokoliv důvodu centrální správa nebude dostupná)	

Obousměrná integrace (min. ve smyslu sdílení informací o odhalených hrozbách a provozně/telemetrický informací) nabízeného NGFW s dalšími instalovanými bezpečnostní prvky (nástroj pro sběr a vyhodnocování logů, nástroj pro centrální správu)	
Požadavky na sítové funkce	**---**
Podpora VLAN dle IEE 802.1Q	
Podpora QinQ dle IEE 802.1ad	
Podpora agregovaných interface (LACP) IEE802.3ad	
Podpora redundatních rozhraní	
Podpora looback rozhraní	
Možnost spojit vybrané fyzivké porty do virtuálního switche	
Možnost práce se zónamy (logická skupina sítových rozhraní zastoupená objektem v konfiguraci)	
Podpora vytvoření tzv. wire pair pro L2 transparetní inspekci	
Podpora VXLAN (enkapsulace L2 sítových rámců do L3 IP paketů za účelem transportu do vzdáléné sítě)	
Podpora dynamických směrovacích protokolů min v rozsahu: RIP, OSPF, BGP, IS-IS; podpora BFD	
Podpora LLDP	
Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single sign-on	
Podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů	
Funkce QoS a traffic shaping min. ve variantě policing a queuing, aplikace politiky globálně nebo pomocí pravidel, podpora DSCP v pravidlech	
Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3	
Podpora tunelování provozu pomocí technologie GRE s možností terminace tunelu do specifické VRF	
Požadavky na bezpečnostní funkce	**---**
Antivirový engine musí být vybaven lokální databází vzorků malware a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků	
Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče. Sandboxovací funkce musí být součástí nabídky (možno jako službu výrobce poskytovanou z cloud prostředí)	
Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 4000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace	
Možnost definice zakázaných slov pro vyhledávání na internetu	

Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu; požadované akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost autentizace uživatele pro určitou kategorii, možnost definice časových kvót pro uživatele a kategorie webu	
Podpora kategorizace stremovaných videí a kanálů min. pro platformu Youtube a Vimeo	
Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů	
Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času	
Funkce ochrany před unikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě vodoznaků, popisu regulárním výrazem, výskytem nežádané komunikace v čase atd. s podporou pro protokoly HTTP, FTP, IMAP, POP3, SMTP, NNTP, MAPI, CIFS, SFTP/SCP), rozlišování souborů podle jejich přípony a podle jejich vnitřní struktury, možnost logovat i blokovat nežádoucí provoz, podpora vytváření logických vzahů v pravidlech.	
Analýza a zabezpečení DNS dotazů (ochrana před DNS poisoningem), filtrování DNS dotazů na základě kategorizace	
Podpora režimu nasazení v režimu WCCP (WCCP v2)	
Podpora konfiguračních PAC souborů pro režim nasazení explicitní proxy	
Podpora ICAP rozhraní pro obousměrnou integraci s externími inspekčními servery dle RFC 3507	
Podpora automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí	
Možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu	
Integrovaná funkce load balancingu (reverzní proxy) s podporou základní algorimtů pro rozklad zátěže (round robing, váhování, nejkratší odezva, nejmenší počet aktivních spojení) s detekcí stavu reálných serverů na pozadí, podpora funkce ssl offloading a ssl inspekce pro rozkládaný provoz	
Integrovaná funkce filtrování přenášených souborů pro protokoly CIFS, FTP, HTTP, IMAP, MAPI, POP3, SMTP a SSH; možnost konfigurace různého chování pro příchozí a odchozí směr, možnost práce s heslem chráněnými soubory, možnost logovat a blokovat provoz	
Integrovaný web aplikační firewall pro ochranu publikovaných webových služeb proti sítovým útokům, možnost konfigurace ochrany proti útokům typu SQL injection, generické techniky, trojské koně, únik informací, známé zranitelnosti).	
Ochrana VoIP komunikace min. pro protokoly SIP a SCCP s podporou NAT46 a NAT64 SIP ALG, inspekce SIP komunikace, SIP pinholes, SIP over TLS, kontrola MSRP provozu	
Další požadavky	**---**
Všechny výkonové a funkční parametry nabízeného zařízení musí být ověřitelné z veřejně dostupných zdrojů výrobce zařízení	
Všechny licence potřebné ke spuštění požadovaných funkcionalit musí být součásti dodávky zařízení	
Podpora výrobce na nabízené zařízení funguje 24/7 a případná licence pro takovou podporu je součástí nabízeného zařízení	

2. Wifi AP a Switche

Předmětem veřejné zakázky je dodávka a instalace nových přístupových přepínačů – 10 ks wifi přístupových bodů a 11ks switchů pro možnost plošné implementace technologie 802.1X.

Plnění parametrů	Ano/Ne
Požadavky na centrální management přístupových bodů a switchů	**---**
AP plně integrované s firewall platformou poptávanou v tomto výběrovém řízení jak na funkční, tak na management úrovni	
automatická nebo manuální autorizace AP a switchů na základě auto discovery mechanismu	
jednotné management rozhraní, ze kterého lze spravovat AP, switche i firewally	
jednotné management rozhraní pro správu bezdrátové sítě a bezpečnostních politik souvisejících s konkrétním SSID a VLAN	
jednotné management rozhraní pro zobrazení stavu firewall zařízení a všech přístupových bodů včetně jim přiřazených SSID, asociovaných klientů interferujích SSID včetně síly signálu intereferujícího SSID vůči konkrétnímu AP	
možnost vyhledávání, v jednotném management rozhraní, konkrétních zařízení nebo uživatel na základě minimálně následujících parametrů: IP adresa, MAC adres, uživatelské jméno	
možnost automatické aktualizace operačního sytému AP a switchů po jeho registraci k firewall platformě	
možnost automaticky registrovat AP a switche po jeho registraci k firewall platformě na servisní portál výrobce AP a switchů	
možnost manuální karantény konkrétního uživatele z jednotného management rozhraní, která zamezí další možnosti připojení se uživatele k bezdrátové síti	
možnost hromadného upgrade firmware AP a switchů z jednotného management rozhraní	
Požadavky na AP	**---**
Formát AP: indoor s interními anténami	
Příslušenství k montáži na zeď/strop/T-Rail	
Počet rádií: minimálně 3 pro přenos v pásmech 2,4 a 5GHz a samostatné monitorovací rádio	
Minimálně 2x2 MIMO	
Dedikované rádio pro analýzu okolního provozu	
Dedikované Bluetooth/ZigBee rádio pro lokalizační služby	
Současná podpora 2,4 GHz a 5GHz pásma	
Podpora standardu 802.11ax	
2x 10/100/1000 Base-T RJ45 uplink porty s možností sestavení LAG	
1x seriový port RJ45	
Počet SSID: až 16	
Cellular Co-existence	
Podpora BSS Coloring	
Podpora TWT (Target Wake Time)	
Spektrální analýza přímo na AP	

Možnost zachytávání paketů na AP pro jejich analýzu	
Provoz všech rádií i při napájení pomocí 802.3af	
Podpora všech následujících standardů - 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az	
Kensigton lock	
Podpora výrobce na 5 let	
Požadavky na switche	**--**
Rack Mount provedení	
48 x 1 GE port (RJ45)	
4 x 10 GE SFP+ sloty Dedikovaný konzolový port (RJ45)	
Minimálně 24 portů POE (802.3af/at)	
PoE power budget 370W	
Switchovací propustnost minimálně 170 Gbps	
Paketová propustnost minimálně 260 Mpps	

3. Systém pro uchovávaní logů

Bude implementován nástroj pro správu logů (tzv. log management). Nástroj bude sbírat, normalizovat a spravovat logy a data síťových toků.

Plnění parametrů	Ano/Ne
Nástroj pro sběr provozních informací a reporting	**---**
HW appliance (řešení formou virutální appliance nebude akceptováno)	
Obousměrná integrace s poptávanou NGFW platformou, AP, switchi, agentem pro koncová zařízení a konzolí pro správu logů (řešení od stejného výrobce. V opačném případě musí být podpora oficiálně garantována oběma výrobci)	
Využitelná disková kapacita min. 2TB při využití min RAID1)	
Požadovaný výkon min. 25 GB logů za 24 h	
Min. 2x síťové rozhraní typu RJ-45, 1Gb propustnost	
Multitenantní přístup s podporou izolovaného kontextu	
Podpora výrobce (min. všechny požadované funkce, aktualizace firmware, technické problémy) po dobu 5 let	
Funkční požadavky	**---**
Centrální logovací prvek pro NGFW firewally	
Podpora syslog protokolu pro logování dalších zařízení	
Obousměrná (výrobcem podporovaná) integrace se všemi napojenými zařízeními. Obousměrnou integrací se rozumí min. odesílání logů z koncového zařízení a jejich zpětné načtení na zařízení)	
Centralizovaný monitoring a vhled do provozu v celé síti	
Korelace nasbíraných dat, vizualizace incidentů v časové ose	
Podpora SOC a NOC režimu	
Podpora automatizace (automatická reakce na incident v sítí)	
Min. 60 předdefinovaných reportů	

Min. 1500 předdefinovaných komponent použitelných v reportech	
Funkce pro práci s incidenty (incident management)	
Analytické a reportovací funkce	
Vizualizace informací v reálném čase	
Offline reporting	
Identifikace a vizualizace odhalených koncových zařízení v síti	
Podpora prohlížení statistických údajů nad logy	
Analýza hrozeb odhalených v síti	
Podpora reportů nad logy ve formátu HTML/CSV/XML/PDF, generování reportů v pravidelných intervalech, předefinované vzory pro reporty na nejčastější použití, možnost vytváření vlastních reportů na základě konkrétních SELECT dotazů do databáze	
Podpora SNMPv2, SNMPv3 minimálně pro reportování událostí a stavu zařízení	
Podpora REST API pro integraci se systémy zadavatele	
Správa přes webové rozhraní HTTPS	
Administrátorské účty musí být možné konfigurovat lokálně nebo na vzdáleném serveru (LDAP, RADIUS, Tacacs+)	

4. Nástroj pro zabezpečení koncových stanic

Plnění parametrů	Ano/Ne
Požadavky na centrální management řešení	**---**
Podpora multitenance - možnost oddělit jednotlivé stanice dle uživatele/typu atd.	
Možnost napojení na Active Directory	
Možnost definice lokálních skupin	
Možnost ověření uživatele proti AD při připojení k centrálnímu managementu	
Komunikace s klienty zabezpečena pomocí certifikátů	
Tvorba instalačních balíčků v prostředí centrálního managmentu	
Centrální správa připojených klientů (upgrade a odinstalování klienta z koncové stanice)	
Možnost definice politik a profilů	
Politiky aplikované dle členství v AD skupině/lokální skupině	
Detekce umístění klienta dle definovaných pravidel (ve firmě, home office atd.)	
Definice politik a profilů dle detekovaného umístění klienta (firma, home office atd.)	
Možnost definovat pravidla zjišťující stav koncové stanice: - přítomnost zranitelností na nainstalovaném software - informace z Windows Security Centra (stav antiviru a firewallu) - přítomnost konkrétního procesu, souboru, záznamu v registru - přítomnost certifikátu včetně definice Subjectu/CN - detekce uživatelské identity, skupiny, IP rozsahu	
Distribuce výsledku kontroly stavu koncových stanic na firewall	
Distribuce telemetrických dat připojených klientů na firewall	
Požadavky na klienta	**---**
Integrovaný Cloud Access Security Broker	
Skener zranitelností	

Podpora automatického patchingu nalezených zranitelností	
Lokální webfilter s reputační databází webových stránek výrobce	
Synchronizace webfilter profilu s firewallem	
IPSEC VPN klient s podporou 2FA	
SSL VPN s ověřením proti SAML IdP	
SSL VPN klient podporující firewall zadavatele s podporou 2FA	
Podpora always-on VPN - automatické připojení k VPN	
Podpora připojení k VPN před přihlášením k operačnímu systému Windows	
Split tunneling na základě rozpoznávání aplikací	
ZeroTrust agent - vzdálený přistup bez připojení k VPN	
Definice ZeroTrust pravidel manuálně nebo pomocí centrálního mangementu	
ZeroTrust komunikace zabezpečena certifikátem	
Podpora centrálního logování	
Antivirový engine musí být vybaven lokální databází vzorků malware a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků	
Podpora kontroly připojených USB zařízení	
Možnost spolupráce s dodávaným NGFW řešením ve formě automatické karantény napadené stanice	
Aplikační firewall	
Integrace se sandboxem výrobce ve formě cloudové služby	

5. Zálohovací server

Součástí veřejné zakázky je dodávka a instalace serveru určenému k zálohování VM strojů z Vmware

Plnění parametrů	Ano/Ne
server o max. velikosti 2U	
barevně značené hot-plug vnitřní komponenty	
rackmount příslušenství včetně pohyblivého ramene pro zachycení kabeláže	
CPU: jednosocketový systém osazený 16 Core CPU	
RAM: minimálně 128GB	
Diskový systém: server musí podporovat minimálně 12 x 3,5 palcových disků + 2 x 2,5 palcových disků SSD	
server musí akceptovat točící disky SAS, Near Line SAS, SATA i SSD zároveň	
server s hot-plug disky kapacita disků 3,5 palcových minmálně 24TB disk 2x SSD 500 GB	
Diskový řadič: minimální vlastnosti řadiče: · typu SAS, PCI Express 3.0 kompatibilní, dvoukanálový (2 konektory) · podpora RAID 0, 1, 5, 6, 10, 50, 60 · podpora 12Gbps technologie rozhraní disků (6Gbps se nepovoluje), 12Gbps na port · podpora Non-RAID (Pass-through) · podpora Online Capacity Expansion (OCE) · podpora Online RAID Level Migration (RLM) · podpora Auto resume po ztrátě napájení	

· podpora 4K native sector velikosti · podpora TRIM/UNMAP příkazů pro SAS/SATA SSDs · podpora NVRAM “Wipe” · podpora End Device Frame Buffering (EDFB) · podpora SED disků a SSD disků · Load balancing · podpora až 64 logických disků a 64TB LUN · podpora DDF compliant Configuration on Disk (COD) · podpora S.M.A.R.T. · podpora globálního i dedikovaného hot-spare · minimálně 1GB cache typu NV (cache to flash) možnost osadit i 2 řadiče na interní disky serveru	
Flash/USB Driver	
Síťové rozhraní: základní 2 x 1GbE + 2 x 10GbE 10GBASE-T (RJ-45)	
Management serveru nezávislý na operačním systému poskytující následující management funkce a vlastnosti: Local Updates Power Monitoring Backup & Restore Driver Pack Crash Screen Capture Virtual Console IPMI 2.0 Auto-Recovery Virtual Media Embedded Diagnostics Remote Config Remote File Share Local OS Install Remote Update PK Authentication Shared NIC Email Alerts Crash Video Playback Local Configuration via USC Encryption Console Chat Web GUI Power Control Virtual Folders Serial Redirection SNMP Gets/Alerts Enterprise Group Power Management Remote CLI Comprehensive Monitoring Power Capping local/SSH CLI Virtual Flash Partitions Boot Playback IPv6 Dedicated NIC 1Gbps Directory Services (AD, LDAP) Auto-Discovery Part Replacement Two-Factor Authentication nezávislý management je s dedikovaným ethernet portem, který není součástí požadovaných ethernet portů management nástroje musí umět poskytovat diagnostiku serveru bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích, tzn. i bezdiskový server poskytuje diagnostiku serveru; nepřipouští se diagnostika spouštěná z optické mechaniky nebo jiného externího zařízení (např. USB flash disk, SD karta, atd.) vyžadována je schopnost monitorovat a spravovat server out-of-band bez nutnosti instalace agenta do operačního systému jejich výměny vč. základové desky provoz serveru v přizpůsobeném datovém centru bez klimatizační jednotky až do 45 stupňů Celsia	

6. Klimatizace do servrovny

Plnění parametrů	Ano/Ne
provedení určené pro serverovny (provoz 24/7)	
Výkon minimálně 3 kW chlazení	
Rozměry servroven **Mírové náměstí čp. 1** (Radnice) d4m x s1.5m x v3m 18m³, **J. Švermy čp. 21** d4m x s 2m x 2,5m 20m³ a **J. Roháče 1381** d3m x s4m x v3m 36m³	---

7. NAS

Dedikovaný storage pro zálohování logů

Plnění parametrů	Ano/Ne
Rack mount provedení	
2 zdroje napájení	
4 x 1GB porty (RJ45)	
8 Slotů pro HDD/SSD	
8 x 4T HDD	

8. Systém pro Automatizaci Incidenčních Workflow

Předmětem dodávky je implementace Systému pro Automatizaci Incidenčních Workflow (SAIW). Jedná se o komunikační nadstavbu bezpečnostních komponent, která umožní automatizaci komunikace v rámci řešení incidentů vzniklých na dodaných bezpečnostních zařízeních

Plnění parametrů	Ano/Ne
Systém bude poskytovat funkce pro efektivní komunikaci a spolupráci mezi osobami odpovědnými za řešení incidentů a zúčastněnými stranami. Komunikace bude zajištěna v rozsahu: • Mailové notifikace • Rozesílání SMS • Automatizované hlasové volání	
Možnost rozšíření komunikačních kanálů o whatsapp – existující funkcionalita	
Systém bude poskytovat klienta pro mobilní zařízení typu Android, iOS. V těchto zařízeních umožnit přijetí nebo zamítnutí výzvy, náhled do historie oslovení a scénářů, výběr stavu (připraven, mimo službu atd.), změnu hesla, reportování polohy	
Systém bude umět zakládat bezpečnostní komunikační scénáře = předpisy komunikačních kroků/úkonů (sestavení hlasového volání, odeslání SMS, příjem odpovědní SMS, odeslání PUSH notifikace, odeslání zprávy ve WhatsApp, příjem zprávy z WhatsApp) a pracovat se zpětnou vazbou (přijímám úkol / nepřijímám úkol)	
Systém by měl umět nabírat a vyhodnocovat zpětnou vazbu k zaslaným bezpečnostním incidentům čímž realizuje funkci rozhodovacího uzlu (ano/ne, resp. úspěch/neúspěch). Komunikační kroky lze provádět sekvenčně (jeden po druhém) či paralelně (současně na určitou množinu osob), následující komunikační kroky je možno definovat pro oba výsledky rozhodovacího uzlu a dále je možné podmínit je požadovanými parametry (odbornost, operační stav, dosažení potřebného skóre = situace, kdy výzvu přijme potřebný počet pracovníků.	
Systém bude mít možnost spustit bezpečnostní komunikační scénář automaticky (bez zásahu lidské obsluhy) v případě mailového notifikačního alertu generovaného ze systémů NGFW, Log Manager či zálohování. Událost či incident zaslaný z uvedených systémů automaticky spustí nadefinované bezpečnostní komunikační scénáře	
Možnost spouštění předem nadefinovaných bezpečnostních komunikačních scénářů lidskou obsluhou odkudkoliv z webového prohlížeče, z mobilního telefonu zasláním SMS: • Spuštěním zcela předpřipraveného bezpečnostní scénáře – ke spuštění stačí jeden klik • Doplněním proměnných v operačním dashboardu a následným spuštěním bezpečnostního komunikačních scénáře – dashboard lze ovládat jak z dotykové obrazovky, tak i z pracovní stanice	

Systém bude mít možnost využití následujících komunikačních kanálů: • Mailové notifikace, • SMS zprávy s možností požadování odpovědní SMS • telefonický hovor s funkcí TTS (Text To Speech) s možností požadování odpovědi interaktivní DTMF volbou • PUSH notifikace v mobilním telefonu, s možností požadování odpovědi na zaslanou zprávu • Automatické zasílání varovných zpráv na PC stanice, vybavené samostatnou aplikací (tlustý klient), která umožňuje akustickou a optickou vizualizaci varovného hlášení na PC stanici	
Real-timový přehled o aktuálním stavu odpovědí, průběhu převzetí informace o incidentech včetně zachování evidence a záznamu historie (kompletní přehled o průběhu a historii informování)	
Tvorba reportů obsahujících veškeré dostupné informace o komunikaci, vyrozumění a průběhu scénářů. Součástí reportu je i detailní historie odpovědí účastníků. Výběr z několika předdefinovaných reportů.	
Možnost automatického vkládání dynamických informací do textu zprávy (datum a čas spuštění/jméno uživatele, který scénář spustil/druh a typ bezpečnostního incidentu …)	
Možnost a podpora zadávání operačního stavu informované osoby („připraven / nepřipraven“; respektive „ve službě / mimo službu“ nebo respektive „v pohotovosti/ mimo pohotovost“	
Systém automatizace komunikace SAIW bude provozován v režimu on-premis. Systém tedy bude umístěn v infrastruktuře zákazníka. Nicméně komunikační služby SMS konektor a SIP trunk budou provozovány formou služby a systém automatizace komunikace na ně bude napojen. Součástí řešení je i volná měsíční kapacita 100 SMS a 30 min volání zdarma.	

9. Instalace, konfigurace, zaškolení:

Součástí dodávky níže uvedených technologií budou i dále uvedené služby.

Plnění parametrů	Ano/Ne
Doprava do místa plnění (technologická místnost na adrese sídla zadavatele	
Montáž HW zařízení do racku, připojení k UPS, připojení sítě,	
Provedení SW instalace, základní konfigurace na úrovni zapojení, oživení, aktualizací firmware a přípravy prostředí pro provoz virtuálních serverů a služeb zálohování.	
Dodávka požadovaných SW licencí.	
Zaškolení administrátorů na dodané technologie	
Instalace serveru k zálohování VM	
Implementace nových pravidel a konfigurací zálohování do všech relevantních úrovní procesů zálohování	
Zpracování dokumentace k dodávanému řešení	
Zajištění testovacího provozu	
Provedení akceptačních testů	

10. Zajištění kybernetického auditu:

Po ukončení plnění technických dodávek projekt je součástí plnění provedení nezávislého auditu kybernetické bezpečnosti.

Plnění parametrů	Ano/Ne
Provedení auditu kybernetické bezpečnosti v souladu s vyhláškou č. 82/2018 Sb., podle požadavků § 7 ods. 4. vyhlášky	
Certifikace prokazující odpovídající kvalifikaci pro provedení auditu kybernetické bezpečnopsti (Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified in Risk and Information Systems Control (CRISC), Lead Auditor Information Security Management Systém (Lead Auditor ISMS), Auditor BI (akreditační schéma ČIA)	

Příloha č. 2 smlouvy – Technická specifikace z nabídky (prodávajícího)

Předmětem plnění této technické specifikace je dodávka a implementace opatření v oblasti kybernetické bezpečnosti, a to včetně nedílně souvisejících požadavků typu dodání licencí, zaškolení, zpracování dokumentace a služeb technické podpory.

Zadavatel požaduje dodávku jednotlivých komponent dle této technické specifikace včetně příslušenství v níže uvedené minimální specifikaci.

Musí se jednat o zařízení nová, nepoužitá, nerepasovaná a určená pro prodej v České republice.

Dodavatel jednoznačně určí, jaký typ nebo verze nabízeného řešení je předmětem jeho nabídky. V případě, že neexistuje veřejně dostupný podrobný popis nabízeného řešení, který umožní posoudit splnění zadávacích podmínek, je dodavatel povinen připojit tento popis jako součást nabídky.

1. New Generation Firewall

Předmětem veřejné zakázky je dodávka 2 ks Next Generation Firewallů. Dodané řešení musí splňovat následující minimální požadavky:

Plnění parametrů NGFW	Ano/Ne

HW požadavky	**---**
HW zařízení typu NGFW (VM appliance nebo jiné software řešení není akceptovatelné). Součástí nabídky musí být 2 kusy identických zařízení pro využití v režimu HA s licencemi tak, aby byl tento režim plně podporován včetně všech níže požadovaných funkcí.	Ano
Podpora výrobce (min. všechny požadované funkce, aktualizace firmware, technické problémy) po dobu 5 let	Ano
Podpora režimu vysoké dostupnosti minimálně jako active/active a active/passive, HA cluster o dvou fyzických zařízeních. NGFW cluster musí být schopen odbavovat 100% datového toku bez omezení i v případě výpadku jakéhokoliv z HA nodů, překlopení v rámci clusteru musí být plně automatické bez nutnosti jakéhokoliv zásahu administrátora.	Ano
Velikost HW appliance maximálně 1 RU	Ano
Podpora duálního napájení (redundantní zdroj). Zdroje jsou součástí nabízeného zařízení	Ano
Maximalní spotřeba 40W	Ano
Minimálně 4x 10GE SFP+	Ano
Minimálně 8x 1Gbps SFP	Ano
Minimálně 16x 1Gbps GE-RJ45	Ano
Dedikované síťové porty pro HA, management a konzolovou konektivitu	Ano
USB port	Ano
TPM modul pro generování a ukládání kryptografických klíčů	Ano
Výkonové požadavky (výkonové parametry je nutné doložit produktovým listem výrobce, nebo oficiální dokumentací výrobce)	**---**
Požadovaná propustnost poptávaného zařízení pro IPv4 i IPv6 provoz je 39 Gbps (UDP paket o velikosto 512B)	Ano
NGFW propustnost 3 Gbps	Ano
IPS propustnost 5 Gbps (včetně zapnutého logování provozu)	Ano
Threath protection propustnost 2,8 Gbps	Ano
Počet současně navázaných TCP spojení firewallu min. 3 mil.	Ano
Počet nových TCP spojení za sekundu min. 140 000	Ano
Propustnost funkce SSL inspekce 3 Gbps.	Ano
Minimální Počet současně navázaných spojení kontrolovaných pomocí SSL inspekce – 315 000	Ano
Požadavky na VPN funkce	**---**
Minimální propustnost IPSEC VPN 35 Gbps	Ano
Minimální propustnost SSL VPN 1,5 Gbps	Ano
Minimálně 450 současně připojených uživatelů SSL VPN (pokud funkce vyžaduje licenci, musí být součástí nabídky.)	Ano
Klient pro SSL VPN musí je součásti dodávky (bezplatný, případně pro 450 uživatelů)	Ano
Vícefaktorová autentizace pro 20 privilegovaných uživatelů je součástí dodávky - druhý faktor formou OTP mobilní aplikace integrované s dodávaným NGFW řešením (řešení pomocí samostatného IAM řešení není akceptováno)	Ano
Podpora push notifikací u OTP mobilní aplikace bez nutnosti opisovat OTP kód	Ano
Podpora iOS a Android OS u OTP mobilní aplikace	Ano
Požadavky na obecné funkce	**---**

Konsolidované bezpečnostní řešení obecně značené jako firewall nové generace (next generation firewall, NGFW)	Ano
Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů. Klíčovým požadavkem je možnost plnohodnotné správy v rámci GUI i CLI bez nutnosti instalovat management aplikaci na koncovou stanici.	Ano
Podpora logických domén (kontextů) na nabízením fyzickém zařízení v počtu alespoň 10 v ceně nabízeného zařízení; každá logická doména musí pracovat izolovaně s možností propojovat jednotlivé logické domény pomocí interních virtuálních propojů bez nutnosti použití fyzických interface	Ano
Podpora více routovacích kontextů, tzv VRF	Ano
Podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46, plnohodnotná podpora IPv6	Ano
Možnost nasazení ve všech z následujících režimu (kombinace možné pomocí použití různých režimů pro různé logické domény): L2 bridge režim (inline), L3 router/NAT režim (inline), explicitní proxy (inline/out of path), transparentní proxy (inline)	Ano
Plnohodnotná správy z lokálního management rozhraní (a to i v případě využití nástroje centrální správy, neboť i v takovém případě musí být možné firewall, resp. firewall cluster, plnohodnotně konfigurovat ve chvíli, kdy z jakéhokoliv důvodu centrální správa nebude dostupná)	Ano
Obousměrná integrace (min. ve smyslu sdílení informací o odhalených hrozbách a provozně/telemetrický informací) nabízeného NGFW s dalšími instalovanými bezpečnostní prvky (nástroj pro sběr a vyhodnocování logů, nástroj pro centrální správu)	Ano
Požadavky na sítové funkce	**---**
Podpora VLAN dle IEE 802.1Q	Ano
Podpora QinQ dle IEE 802.1ad	Ano
Podpora agregovaných interface (LACP) IEE802.3ad	Ano
Podpora redundatních rozhraní	Ano
Podpora looback rozhraní	Ano
Možnost spojit vybrané fyzivké porty do virtuálního switche	Ano
Možnost práce se zónamy (logická skupina sítových rozhraní zastoupená objektem v konfiguraci)	Ano
Podpora vytvoření tzv. wire pair pro L2 transparetní inspekci	Ano
Podpora VXLAN (enkapsulace L2 sítových rámců do L3 IP paketů za účelem transportu do vzdáléné sítě)	Ano
Podpora dynamických směrovacích protokolů min v rozsahu: RIP, OSPF, BGP, IS-IS; podpora BFD	Ano
Podpora LLDP	Ano
Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single sign-on	Ano
Podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů	Ano
Funkce QoS a traffic shaping min. ve variantě policing a queuing, aplikace politiky globálně nebo pomocí pravidel, podpora DSCP v pravidlech	Ano
Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3	Ano
Podpora tunelování provozu pomocí technologie GRE s možností terminace tunelu do specifické VRF	Ano
Požadavky na bezpečnostní funkce	**---**

Antivirový engine musí být vybaven lokální databází vzorků malware a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků	Ano
Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče. Sandboxovací funkce musí být součástí nabídky (možno jako službu výrobce poskytovanou z cloud prostředí)	Ano
Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 4000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace	Ano
Možnost definice zakázaných slov pro vyhledávání na internetu	Ano
Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu; požadované akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost autentizace uživatele pro určitou kategorii, možnost definice časových kvót pro uživatele a kategorie webu	Ano
Podpora kategorizace stremovaných videí a kanálů min. pro platformu Youtube a Vimeo	Ano
Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů	Ano
Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času	Ano
Funkce ochrany před unikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě vodoznaků, popisu regulárním výrazem, výskytem nežádané komunikace v čase atd. s podporou pro protokoly HTTP, FTP, IMAP, POP3, SMTP, NNTP, MAPI, CIFS, SFTP/SCP), rozlišování souborů podle jejich přípony a podle jejich vnitřní struktury, možnost logovat i blokovat nežádoucí provoz, podpora vytváření logických vzahů v pravidlech.	Ano
Analýza a zabezpečení DNS dotazů (ochrana před DNS poisoningem), filtrování DNS dotazů na základě kategorizace	Ano
Podpora režimu nasazení v režimu WCCP (WCCP v2)	Ano
Podpora konfiguračních PAC souborů pro režim nasazení explicitní proxy	Ano
Podpora ICAP rozhraní pro obousměrnou integraci s externími inspekčními servery dle RFC 3507	Ano
Podpora automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí	Ano
Možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu	Ano
Integrovaná funkce load balancingu (reverzní proxy) s podporou základní algorimtů pro rozklad zátěžě (round robing, váhování, nejkratší odezva, nejmenší počet aktivních spojení) s detekcí stavu reálných serverů na pozadí, podpora funkce ssl offloading a ssl inspekce pro rozkládaný provoz	Ano

Integrovaná funkce filtrování přenášených souborů pro protokoly CIFS, FTP, HTTP, IMAP, MAPI, POP3, SMTP a SSH; možnost konfigurace různého chování pro příchozí a odchozí směr, možnost práce s heslem chráněnými soubory, možnost logovat a blokovat provoz	Ano
Integrovaný web aplikační firewall pro ochranu publikovaných webových služeb proti sítovým útokům, možnost konfigurace ochrany proti útokům typu SQL injection, generické techniky, trojské koně, únik informací, známé zranitelnosti).	Ano
Ochrana VoIP komunikace min. pro protokoly SIP a SCCP s podporou NAT46 a NAT64 SIP ALG, inspekce SIP komunikace, SIP pinholes, SIP over TLS, kontrola MSRP provozu	Ano
Další požadavky	**---**
Všechny výkonové a funkční parametry nabízeného zařízení musí být ověřitelné z veřejně dostupných zdrojů výrobce zařízení	Ano
Všechny licence potřebné ke spuštění požadovaných funkcionalit musí být součásti dodávky zařízení	Ano
Podpora výrobce na nabízené zařízení funguje 24/7 a případná licence pro takovou podporu je součástí nabízeného zařízení	Ano

2. Wifi AP a Switche

Předmětem veřejné zakázky je dodávka a instalace nových přístupových přepínačů – 10 ks wifi přístupových bodů a 11ks switchů pro možnost plošné implementace technologie 802.1X.

Plnění parametrů	Ano/Ne
Požadavky na centrální management přístupových bodů a switchů	**---**
AP plně integrované s firewall platformou poptávanou v tomto výběrovém řízení jak na funkční, tak na management úrovni	Ano
automatická nebo manuální autorizace AP a switchů na základě auto discovery mechanismu	Ano
jednotné management rozhraní, ze kterého lze spravovat AP, switche i firewally	Ano
jednotné management rozhraní pro správu bezdrátové sítě a bezpečnostních politik souvisejících s konkrétním SSID a VLAN	Ano
jednotné management rozhraní pro zobrazení stavu firewall zařízení a všech přístupových bodů včetně jim přiřazených SSID, asociovaných klientů interferujích SSID včetně síly signálu intereferujícího SSID vůči konkrétnímu AP	Ano
možnost vyhledávání, v jednotném management rozhraní, konkrétních zařízení nebo uživatel na základě minimálně následujících parametrů: IP adresa, MAC adres, uživatelské jméno	Ano
možnost automatické aktualizace operačního sytému AP a switchů po jeho registraci k firewall platformě	Ano
možnost automaticky registrovat AP a switche po jeho registraci k firewall platformě na servisní portál výrobce AP a switchů	Ano
možnost manuální karantény konkrétního uživatele z jednotného management rozhraní, která zamezí další možnosti připojení se uživatele k bezdrátové síti	Ano
možnost hromadného upgrade firmware AP a switchů z jednotného management rozhraní	Ano
Požadavky na AP	**---**
Formát AP: indoor s interními anténami	Ano
Příslušenství k montáži na zeď/strop/T-Rail	Ano

Počet rádií: minimálně 3 pro přenos v pásmech 2,4 a 5GHz a samostatné monitorovací rádio	Ano
Minimálně 2x2 MIMO	Ano
Dedikované rádio pro analýzu okolního provozu	Ano
Dedikované Bluetooth/ZigBee rádio pro lokalizační služby	Ano
Současná podpora 2,4 GHz a 5GHz pásma	Ano
Podpora standardu 802.11ax	Ano
2x 10/100/1000 Base-T RJ45 uplink porty s možností sestavení LAG	Ano
1x seriový port RJ45	Ano
Počet SSID: až 16	Ano
Cellular Co-existence	Ano
Podpora BSS Coloring	Ano
Podpora TWT (Target Wake Time)	Ano
Spektrální analýza přímo na AP	Ano
Možnost zachytávání paketů na AP pro jejich analýzu	Ano
Provoz všech rádií i při napájení pomocí 802.3af	Ano
Podpora všech následujících standardů - 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az	Ano
Kensigton lock	Ano
Podpora výrobce na 5 let	Ano
Požadavky na switche	**--**
Rack Mount provedení	Ano
48 x 1 GE port (RJ45)	Ano
4 x 10 GE SFP+ sloty Dedikovaný konzolový port (RJ45)	Ano
Minimálně 24 portů POE (802.3af/at)	Ano
PoE power budget 370W	Ano
Switchovací propustnost minimálně 170 Gbps	Ano
Paketová propustnost minimálně 260 Mpps	Ano

3. Systém pro uchovávaní logů

Bude implementován nástroj pro správu logů (tzv. log management). Nástroj bude sbírat, normalizovat a spravovat logy a data síťových toků.

Plnění parametrů	Ano/Ne
Nástroj pro sběr provozních informací a reporting	**---**
HW appliance (řešení formou virutální appliance nebude akceptováno)	Ano
Obousměrná integrace s poptávanou NGFW platformou, AP, switchi, agentem pro koncová zařízení a konzolí pro správu logů (řešení od stejného výrobce. V opačném případě musí být podpora oficiálně garantována oběma výrobci)	Ano
Využitelná disková kapacita min. 2TB při využití min RAID1)	Ano
Požadovaný výkon min. 25 GB logů za 24 h	Ano

Min. 2x síťové rozhraní typu RJ-45, 1Gb propustnost	Ano
Multitenantní přístup s podporou izolovaného kontextu	Ano
Podpora výrobce (min. všechny požadované funkce, aktualizace firmware, technické problémy) po dobu 5 let	Ano
Funkční požadavky	**---**
Centrální logovací prvek pro NGFW firewally	Ano
Podpora syslog protokolu pro logování dalších zařízení	Ano
Obousměrná (výrobcem podporovaná) integrace se všemi napojenými zařízeními. Obousměrnou integrací se rozumí min. odesílání logů z koncového zařízení a jejich zpětné načtení na zařízení)	Ano
Centralizovaný monitoring a vhled do provozu v celé síti	Ano
Korelace nasbíraných dat, vizualizace incidentů v časové ose	Ano
Podpora SOC a NOC režimu	Ano
Podpora automatizace (automatická reakce na incident v sítí)	Ano
Min. 60 předdefinovaných reportů	Ano
Min. 1500 předdefinovaných komponent použitelných v reportech	Ano
Funkce pro práci s incidenty (incident management)	Ano
Analytické a reportovací funkce	Ano
Vizualizace informací v reálném čase	Ano
Offline reporting	Ano
Identifikace a vizualizace odhalených koncových zařízení v síti	Ano
Podpora prohlížení statistických údajů nad logy	Ano
Analýza hrozeb odhalených v síti	Ano
Podpora reportů nad logy ve formátu HTML/CSV/XML/PDF, generování reportů v pravidelných intervalech, předefinované vzory pro reporty na nejčastější použití, možnost vytváření vlastních reportů na základě konkrétních SELECT dotazů do databáze	Ano
Podpora SNMPv2, SNMPv3 minimálně pro reportování událostí a stavu zařízení	Ano
Podpora REST API pro integraci se systémy zadavatele	Ano
Správa přes webové rozhraní HTTPS	Ano
Administrátorské účty musí být možné konfigurovat lokálně nebo na vzdáleném serveru (LDAP, RADIUS, Tacacs+)	Ano

4. Nástroj pro zabezpečení koncových stanic

Plnění parametrů	Ano/Ne
Požadavky na centrální management řešení	**---**
Podpora multitenance - možnost oddělit jednotlivé stanice dle uživatele/typu atd.	Ano
Možnost napojení na Active Directory	Ano
Možnost definice lokálních skupin	Ano
Možnost ověření uživatele proti AD při připojení k centrálnímu managementu	Ano
Komunikace s klienty zabezpečena pomocí certifikátů	Ano
Tvorba instalačních balíčků v prostředí centrálního managmentu	Ano
Centrální správa připojených klientů (upgrade a odinstalování klienta z koncové stanice)	Ano
Možnost definice politik a profilů	Ano

Politiky aplikované dle členství v AD skupině/lokální skupině	Ano
Detekce umístění klienta dle definovaných pravidel (ve firmě, home office atd.)	Ano
Definice politik a profilů dle detekovaného umístění klienta (firma, home office atd.)	Ano
Možnost definovat pravidla zjišťující stav koncové stanice: - přítomnost zranitelností na nainstalovaném software - informace z Windows Security Centra (stav antiviru a firewallu) - přítomnost konkrétního procesu, souboru, záznamu v registru - přítomnost certifikátu včetně definice Subjectu/CN - detekce uživatelské identity, skupiny, IP rozsahu	Ano
Distribuce výsledku kontroly stavu koncových stanic na firewall	Ano
Distribuce telemetrických dat připojených klientů na firewall	Ano
Požadavky na klienta	**---**
Integrovaný Cloud Access Security Broker	Ano
Skener zranitelností	Ano
Podpora automatického patchingu nalezených zranitelností	Ano
Lokální webfilter s reputační databází webových stránek výrobce	Ano
Synchronizace webfilter profilu s firewallem	Ano
IPSEC VPN klient s podporou 2FA	Ano
SSL VPN s ověřením proti SAML IdP	Ano
SSL VPN klient podporující firewall zadavatele s podporou 2FA	Ano
Podpora always-on VPN - automatické připojení k VPN	Ano
Podpora připojení k VPN před přihlášením k operačnímu systému Windows	Ano
Split tunneling na základě rozpoznávání aplikací	Ano
ZeroTrust agent - vzdálený přistup bez připojení k VPN	Ano
Definice ZeroTrust pravidel manuálně nebo pomocí centrálního mangementu	Ano
ZeroTrust komunikace zabezpečena certifikátem	Ano
Podpora centrálního logování	Ano
Antivirový engine musí být vybaven lokální databází vzorků malware a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků	Ano
Podpora kontroly připojených USB zařízení	Ano
Možnost spolupráce s dodávaným NGFW řešením ve formě automatické karantény napadené stanice	Ano
Aplikační firewall	Ano
Integrace se sandboxem výrobce ve formě cloudové služby	Ano

5. Zálohovací server

Součástí veřejné zakázky je dodávka a instalace serveru určenému k zálohování VM strojů z Vmware

Plnění parametrů	Ano/Ne
server o max. velikosti 2U	Ano

barevně značené hot-plug vnitřní komponenty	Ano
rackmount příslušenství včetně pohyblivého ramene pro zachycení kabeláže	Ano
CPU: jednosocketový systém osazený 16 Core CPU	Ano
RAM: minimálně 128GB	Ano
Diskový systém: server musí podporovat minimálně 12 x 3,5 palcových disků + 2 x 2,5 palcových disků SSD	Ano
server musí akceptovat točící disky SAS, Near Line SAS, SATA i SSD zároveň	Ano
server s hot-plug disky kapacita disků 3,5 palcových minmálně 24TB disk 2x SSD 500 GB	Ano
Diskový řadič: minimální vlastnosti řadiče: · typu SAS, PCI Express 3.0 kompatibilní, dvoukanálový (2 konektory) · podpora RAID 0, 1, 5, 6, 10, 50, 60 · podpora 12Gbps technologie rozhraní disků (6Gbps se nepovoluje), 12Gbps na port · podpora Non-RAID (Pass-through) · podpora Online Capacity Expansion (OCE) · podpora Online RAID Level Migration (RLM) · podpora Auto resume po ztrátě napájení · podpora 4K native sector velikosti · podpora TRIM/UNMAP příkazů pro SAS/SATA SSDs · podpora NVRAM “Wipe” · podpora End Device Frame Buffering (EDFB) · podpora SED disků a SSD disků · Load balancing · podpora až 64 logických disků a 64TB LUN · podpora DDF compliant Configuration on Disk (COD) · podpora S.M.A.R.T. · podpora globálního i dedikovaného hot-spare · minimálně 1GB cache typu NV (cache to flash) možnost osadit i 2 řadiče na interní disky serveru	Ano
Flash/USB Driver	
Síťové rozhraní: základní 2 x 1GbE + 2 x 10GbE 10GBASE-T (RJ-45)	Ano
Management serveru nezávislý na operačním systému poskytující následující management funkce a vlastnosti: Local Updates Power Monitoring Backup & Restore Driver Pack Crash Screen Capture Virtual Console IPMI 2.0 Auto-Recovery Virtual Media Embedded Diagnostics Remote Config Remote File Share Local OS Install Remote Update PK Authentication Shared NIC Email Alerts Crash Video Playback Local Configuration via USC Encryption Console Chat Web GUI Power Control Virtual Folders Serial Redirection SNMP Gets/Alerts Enterprise Group Power Management Remote CLI Comprehensive Monitoring Power Capping local/SSH CLI Virtual Flash Partitions Boot Playback IPv6 Dedicated NIC 1Gbps Directory Services (AD, LDAP) Auto-Discovery Part Replacement Two-Factor Authentication nezávislý management je s dedikovaným ethernet portem, který není součástí požadovaných ethernet portů management nástroje musí umět poskytovat diagnostiku serveru bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích, tzn. i bezdiskový server poskytuje diagnostiku serveru; nepřipouští se diagnostika spouštěná z optické mechaniky nebo jiného externího zařízení (např. USB flash disk, SD karta, atd.) vyžadována je schopnost monitorovat a spravovat server out-of-band bez nutnosti instalace agenta do operačního systému	Ano

jejich výměny vč. základové desky provoz serveru v přizpůsobeném datovém centru bez klimatizační jednotky až do 45 stupňů Celsia	

6. Klimatizace do servrovny

Plnění parametrů	Ano/Ne
provedení určené pro serverovny (provoz 24/7)	Ano
Výkon minimálně 3 kW chlazení	Ano
Rozměry servroven **Mírové náměstí čp. 1** (Radnice) d4m x s1.5m x v3m 18m³, **J. Švermy čp. 21** d4m x s 2m x 2,5m 20m³ a **J. Roháče 1381** d3m x s4m x v3m 36m³	---

7. NAS

Dedikovaný storage pro zálohování logů

Plnění parametrů	Ano/Ne
Rack mount provedení	Ano
2 zdroje napájení	Ano
4 x 1GB porty (RJ45)	Ano
8 Slotů pro HDD/SSD	Ano
8 x 4T HDD	Ano

8. Systém pro Automatizaci Incidenčních Workflow

Předmětem dodávky je implementace Systému pro Automatizaci Incidenčních Workflow (SAIW). Jedná se o komunikační nadstavbu bezpečnostních komponent, která umožní automatizaci komunikace v rámci řešení incidentů vzniklých na dodaných bezpečnostních zařízeních

Plnění parametrů	Ano/Ne
Systém bude poskytovat funkce pro efektivní komunikaci a spolupráci mezi osobami odpovědnými za řešení incidentů a zúčastněnými stranami. Komunikace bude zajištěna v rozsahu: • Mailové notifikace • Rozesílání SMS • Automatizované hlasové volání	Ano
Možnost rozšíření komunikačních kanálů o whatsapp – existující funkcionalita	Ano
Systém bude poskytovat klienta pro mobilní zařízení typu Android, iOS. V těchto zařízeních umožnit přijetí nebo zamítnutí výzvy, náhled do historie oslovení a scénářů, výběr stavu (připraven, mimo službu atd.), změnu hesla, reportování polohy	Ano
Systém bude umět zakládat bezpečnostní komunikační scénáře = předpisy komunikačních kroků/úkonů (sestavení hlasového volání, odeslání SMS, příjem odpovědní SMS, odeslání PUSH notifikace, odeslání zprávy ve WhatsApp, příjem zprávy z WhatsApp) a pracovat se zpětnou vazbou (přijímám úkol / nepřijímám úkol)	Ano

Systém by měl umět nabírat a vyhodnocovat zpětnou vazbu k zaslaným bezpečnostním incidentům čímž realizuje funkci rozhodovacího uzlu (ano/ne, resp. úspěch/neúspěch). Komunikační kroky lze provádět sekvenčně (jeden po druhém) či paralelně (současně na určitou množinu osob), následující komunikační kroky je možno definovat pro oba výsledky rozhodovacího uzlu a dále je možné podmínit je požadovanými parametry (odbornost, operační stav, dosažení potřebného skóre = situace, kdy výzvu přijme potřebný počet pracovníků.	Ano
Systém bude mít možnost spustit bezpečnostní komunikační scénář automaticky (bez zásahu lidské obsluhy) v případě mailového notifikačního alertu generovaného ze systémů NGFW, Log Manager či zálohování. Událost či incident zaslaný z uvedených systémů automaticky spustí nadefinované bezpečnostní komunikační scénáře	Ano
Možnost spouštění předem nadefinovaných bezpečnostních komunikačních scénářů lidskou obsluhou odkudkoliv z webového prohlížeče, z mobilního telefonu zasláním SMS: • Spuštěním zcela předpřipraveného bezpečnostní scénáře – ke spuštění stačí jeden klik • Doplněním proměnných v operačním dashboardu a následným spuštěním bezpečnostního komunikačních scénáře – dashboard lze ovládat jak z dotykové obrazovky, tak i z pracovní stanice	Ano
Systém bude mít možnost využití následujících komunikačních kanálů: • Mailové notifikace, • SMS zprávy s možností požadování odpovědní SMS • telefonický hovor s funkcí TTS (Text To Speech) s možností požadování odpovědi interaktivní DTMF volbou • PUSH notifikace v mobilním telefonu, s možností požadování odpovědi na zaslanou zprávu • Automatické zasílání varovných zpráv na PC stanice, vybavené samostatnou aplikací (tlustý klient), která umožňuje akustickou a optickou vizualizaci varovného hlášení na PC stanici	Ano
Real-timový přehled o aktuálním stavu odpovědí, průběhu převzetí informace o incidentech včetně zachování evidence a záznamu historie (kompletní přehled o průběhu a historii informování)	Ano
Tvorba reportů obsahujících veškeré dostupné informace o komunikaci, vyrozumění a průběhu scénářů. Součástí reportu je i detailní historie odpovědí účastníků. Výběr z několika předdefinovaných reportů.	Ano
Možnost automatického vkládání dynamických informací do textu zprávy (datum a čas spuštění/jméno uživatele, který scénář spustil/druh a typ bezpečnostního incidentu …)	Ano
Možnost a podpora zadávání operačního stavu informované osoby („připraven / nepřipraven“; respektive „ve službě / mimo službu“ nebo respektive „v pohotovosti/ mimo pohotovost“	Ano
Systém automatizace komunikace SAIW bude provozován v režimu on-premis. Systém tedy bude umístěn v infrastruktuře zákazníka. Nicméně komunikační služby SMS konektor a SIP trunk budou provozovány formou služby a systém automatizace komunikace na ně bude napojen. Součástí řešení je i volná měsíční kapacita 100 SMS a 30 min volání zdarma.	Ano

9. Instalace, konfigurace, zaškolení:

Součástí dodávky níže uvedených technologií budou i dále uvedené služby.

Plnění parametrů	Ano/Ne
Doprava do místa plnění (technologická místnost na adrese sídla zadavatele	Ano
Montáž HW zařízení do racku, připojení k UPS, připojení sítě,	Ano

Provedení SW instalace, základní konfigurace na úrovni zapojení, oživení, aktualizací firmware a přípravy prostředí pro provoz virtuálních serverů a služeb zálohování.	Ano
Dodávka požadovaných SW licencí.	Ano
Zaškolení administrátorů na dodané technologie	Ano
Instalace serveru k zálohování VM	Ano
Implementace nových pravidel a konfigurací zálohování do všech relevantních úrovní procesů zálohování	Ano
Zpracování dokumentace k dodávanému řešení	Ano
Zajištění testovacího provozu	Ano
Provedení akceptačních testů	Ano

10. Zajištění kybernetického auditu:

Po ukončení plnění technických dodávek projekt je součástí plnění provedení nezávislého auditu kybernetické bezpečnosti.

Plnění parametrů	Ano/Ne
Provedení auditu kybernetické bezpečnosti v souladu s vyhláškou č. 82/2018 Sb., podle požadavků § 7 ods. 4. vyhlášky	Ano
Certifikace prokazující odpovídající kvalifikaci pro provedení auditu kybernetické bezpečnopsti (Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified in Risk and Information Systems Control (CRISC), Lead Auditor Information Security Management Systém (Lead Auditor ISMS), Auditor BI (akreditační schéma ČIA)	Ano

Příloha č. 3 smlouvy – Cenová tabulka Nabídková cena za plnění, které je předmětem zakázky, činí celkem:

- **cena bez DPH** **5 687 000 Kč**
- částka DPH 1 194 270 Kč
- cena včetně DPH 6 881 270 Kč