Príloha č. 2: Štruktúra ceny

Cena celkom v EUR bez DPH	**127 356,00**

Verejný obstarávateľ stanovil rozsah služieb a požadovaného vybavenia nasledovne:

Analýza a dizajn

P.č.	Názov výdavku	MJ	Množstvo	Jednotková cena v EUR bez DPH	Suma v EUR bez DPH	Menný zoznam odborníkov
1.	IT analytik	ČD	31	390,00	12 090,00	Ing. Branislav Anwarzai
2.	IT konzultant	ČD	7	350,00	2 450,00	Vladimír Staňo

Nákup technických prostriedkov, programových prostriedkov a služieb

P.č.	Názov výdavku	MJ	Množstvo	Jednotková cena v EUR bez DPH	Suma v EUR bez DPH	Návrh riešenia zo strany uchádzača (vrátane špecifikácie parametrov ponúkaného HW/SW) a názvu výrobcu a verzie HW/SW
3.	Nástroj pre manažment siete ŠNOP vrátane GUI rozhrania na správu (najmä existujúcich Aruba zariadení)	ks	1	3 000,00	3 000,00	Nástroj pre manažment siete ŠNOP vrátane GUI rozhrania na správu (najmä existujúcich Aruba zariadení) 3x Aruba HP J9775A 2530-48G 2x HP J9776A 2530-24G Switch 2x HP J9773A 2530-24G-PoEP 1x CBS220-16P-2G-Cisco-16p 1x CBS220-16T-2G-SwitchB2428E
	Licencia	mesiac	36	200,00	7 200,00	Licencia aruba wifi
4.	Hardvér na SIEM/SOC vrátane rozšírenia LMS	ks	1	18 750,00	18 750,00	Hardvér na SIEM/SOC vrátane rozšírenia LMS

5.	Softvérový nástroj na skenovanie zraniteľností (vulnerability scanner)	ks	1	9 450,00	9 450,00	Softvérový nástroj na skenovanie zraniteľností (vulnerability scanner)
	Licencia	mesiac	36	250,00	9 000,00	Licencia
6.	Patch manažment systém pre platformu Windows - System Center Configuration Manager (SCCM)	ks	1	3 690,00	3 690,00	Patch manažment systém pre platformu Windows - System Center Configuration Manager (SCCM)
	Licencia	mesiac	36	436,00	15 696,00	Licencia MSCC

Implementácia a testovanie

P.č.	Názov výdavku	MJ	Množstvo	Jednotková cena v EUR bez DPH	Suma v EUR bez DPH	Menný zoznam odborníkov
7.	IT programátor	ČD	11	350,00	3 850,00	Ing. Peter Šedivý
8.	Špecialista pre bezpečnosť IT	ČD	1	500,00	500,00	doc. Ing. Katarína Kampová, PhD.
9.	IT/IS konzultant	ČD	55	350,00	19 250,00	Vladimír Staňo
10.	IT architekt	ČD	2	390,00	780,00	Ing. Branislav Anwarzai / Ing. Peter Feciľak, PhD.
11.	IT analytik	ČD	40	390,00	15 600,00	Ing. Branislav Anwarzai

Nasadenie

P.č.	Názov výdavku	MJ	Množstvo	Jednotková cena v EUR bez DPH	Suma v EUR bez DPH	Menný zoznam odborníkov

12.	Špecialista pre bezpečnosť IT	ČD	10	500,00	5 000,00	doc. Ing. Katarína Kampová, PhD.
13.	IT programátor	ČD	3	350,00	1 050,00	Ing. Peter Šedivý

Komentár k položkám štruktúry ceny:

1.	Inventarizácia, klasifikácia a kategorizácia, vykonanie aktualizácie analýzy rizík a analýzy dopadov, návrh katalógu rizík a spôsobov ich riadenia (okrem vývoja)
2.	Vykonanie koordinácie a konsolidácia interných procesov riadenia bezpečnostných incidentov a interných procesov riadenia prevádzky IKT
3.	Obstaranie nástroja, ktorý bude zabezpečovať manažment siete ŠNOP vrátane GUI rozhrania na správu (najmä existujúcich Aruba zariadení) a implementáciu SW podpory
4.	HW na vyhodnocovanie bezpečnostných incidentov (SIEM), zber, parsovanie a koreláciu logov
5.	Softvérový nástroj na skenovanie zraniteľností (vulnerability scanner)
6.	Patch manažment systém pre platformu Windows - System Center Configuration Manager (SCCM)
7.	Revízia segmentácie siete, konfiguračných a prestupových pravidiel a prípadné doplnenie IDS/IPS.
8.	Zavedenie služby SIEM/SOC „as a service“, vrátane externej podpory riešenia bezpečnostných incidentov

9.	Zavedenie služby SIEM/SOC „as a service", vrátane externej podpory riešenia bezpečnostných incidentov
10.	Vykonanie revízie siete a návrh novej segmentácie siete aj na základe výsledkov AR/BIA
11.	Zavedenie služby SIEM/SOC „as a service", vrátane externej podpory riešenia bezpečnostných incidentov
12.	Návrh a zabezpečenie SW/HW riešenia 2FA
13.	Revízia segmentácie siete, konfiguračných a prestupových pravidiel a prípadné doplnenie IDS/IPS

Zhotoviteľ potvrdzuje , že cena zohľadňuje aj nasledovné skutočnosti:

- konsolidácia zákazky so zavedeným integrovaným manažérskym systémom kvality v rámci ŠNOP,
- kompatibilita navrhovaných riešení s existujúcim HW a SW vybavením ŠNOP,
- spolupráca s externou spoločnosťou, ktorá zabezpečuje správu siete IT v ŠNOP,
- spolupráca s personálom ŠNOP pri implementovaní zákazky.

Čestne prehlasujem, že náš návrh riešenia **„Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v zdravotníckych zariadeniach"** spĺňa minimálne kritériá a požiadavky, ktoré navrhuje verejný obstarávateľ, ktoré prikladáme v tomto dokumente.

ID	Aktivita	Minimálna požiadavka
1.1	**Vytvorenie stratégie informačnej a kybernetickej bezpečnosti (IB a KyB)**	Vytvorenie vízie a koncepcie ŠNOP v oblasti riadenia IB a KYB na najbližšie 3-4 roky, v štruktúre podľa prílohy č. 1 vyhlášky NBÚ č. 362/2018 Z. z., vrátane záväzku vedenia o podpore v tejto oblasti a konsolidácia tohto dokumentu so zavedeným integrovaným manažérskym systémom kvality (ďalej len „IMS") v rámci ŠNOP.
1.2	**Vytvorenie, prípadne aktualizácia a konsolidácia existujúcej dokumentácie a bezpečnostných smerníc**	Vypracovanie, resp. konsolidácia smerníc pre vybrané oblasti riadenia IB a KyB v nadväznosti na zavedený IMS, min. pre nasledovné oblasti: • riadenie bezpečnostných incidentov, vrátane definovania postupov riešenia pre základné typy bezpečnostných incidentov (napr. malware, ransomware, phishing, spearphishing, vishing, DOS a DDoS, nedostupnosť systémov, prienik do systémov alebo siete, únik dát a informácií a pod.) a vrátane konsolidácie postupov riešenia bezpečnostných incidentov s dodávateľom služby SIEM/SOC – *aktualizácia interných smerníc IMS*, • zálohovanie – plán, spôsob, perióda zálohovania – *nový dokument z pohľadu IMS*, • BCM - BCM politika (*vrátane aktualizácie interných smerníc IMS*), stratégia obnovy (*nový dokument z pohľadu IMS*) a BCP a DRP plány pre najkritickejšie systémy (*nový dokument z pohľadu IMS*), • riadenie prístupových práv, vrátane riadenia prístupov privilegovaných používateľov a vrátane zadefinovania základných povinností pri odchode zamestnancov (najmä zmena hesiel, zmena zdieľaných hesiel, zrušenie VPN prístupov, zablokovanie prípadných externých služieb, oznámenie zmeny externým dodávateľom - ak relevantné pre danú rolu a pod.) – *aktualizácia internej smernice IMS*, • riadenie bezpečnosti prevádzky IKT - riadenie zmien, inštalácia SW/HW, riadenie kapacít, antivírusová ochrana, riadenie záplat a aktualizácií, technické zraniteľnosti atď. – *aktualizácia interných smerníc IMS*, • riadenie aktív a rizík – postupy klasifikácie informácií a kategorizácie informačných systémov a spôsob výkonu analýzy rizík a analýzy dopadov (AR/BIA), vrátane definovania základných parametrov (hrozby, dopadové kritéria, spôsob identifikácie a klasifikácie rizík, spôsob definovania RTO a RPO a pod.) – *aktualizácia internej smernice IMS*, • bezpečnostná politika pre koncových používateľov – *aktualizácia internej Smernice IMS*.
1.3.		

	Vytvorenie bezpečnostného projektu pre systém NIS v súlade so zákonom č. 95/2019 Z. z. o ITVS	Vytvorenie nového dokumentu z pohľadu IMS a internej dokumentácie pre nemocničný informačný systém v súlade so zákonom č. 95/2019 Z. z. o ITVS
1.4	**Vykonanie aktualizácie existujúcej analýzy rizík (AR)**	Aktualizácia existujúcej analýzy rizík cez všetky procesy IMS ŠNOP a jej rozšírenie o klasifikáciu a najmä analýzu dopadov (BIA), vrátane určenia RTO (Recovery Time Objective) a RPO (Recovery Point Objective) a zapojenia vybraných vlastníkov procesov IMS. Minimálne požiadavky na aktualizáciu analýzy rizík: • identifikácia všetkých procesov nemocnice a v rámci útvarov identifikácia dátovo-procesných aktív (agend), • komunikáciu s vlastníkmi procesov (osobné stretnutia so všetkými vedúcimi pracovníkmi alebo inými poverenými pracovníkmi jednotlivých útvarov – odhadom približne 15 stretnutí) ohľadom verifikácie aktív a následnej realizácie ich klasifikácie, analýzy rizík a analýzy dopadov, vrátane určenia RTO, RPO a ďalších parametrov potrebných najmä pre určenie stratégie obnovy jednotlivých IS a plánu zálohovania, • komunikáciu s IT oddelením ohľadom väzby identifikovaných aktív a hrozieb na zdroje, ktoré tieto aktíva podporujú (IS a aplikácie), • konsolidáciu získaných výstupov z jednotlivých útvarov prierezovo cez celú organizáciu, • aktualizáciu existujúceho katalógu rizík a posúdenie aktuálnych reziduálnych rizík, • spracovanie kategorizácie IS na základe výsledkov klasifikácie, • odovzdanie know-how povereným zamestnancom nemocnice za účelom opakovaného výkonu aktualizácie AR/BIA v budúcnosti vlastnými silami.
1.5	**V oblasti BCM politiky**	Minimálne požiadavky pre oblasť BCM politiky (efektívne riadenie kontinuity činností/procesov): • Definícia stratégie obnovy pre všetky IS na základe výsledkov AR/BIA (najmä RTO). • Prehodnotenie a konsolidácia aktuálneho plánu a spôsobu zálohovania, prípadná definícia a nastavenie zmien (na základe identifikovaných RPO). • Definícia BCP pre najkritickejšie procesy a určenie prípadných „workaround" postupov. • Definícia DRP pre najkritickejšie systémy (NIS).

		• Otestovanie funkčnosti a správnosti navrhnutých BCP/DRP.
1.6.	**V oblasti riadenia prístupov a bezpečnosti prevádzky IKT**	Vykonanie revízie siete a návrh novej segmentácie siete aj na základe výsledkov AR/BIA: • identifikácia aktuálneho stavu a topológie siete, • návrh novej segmentácie a sieťových (prestupových) pravidiel medzi jednotlivými novými segmentami, kde nové segmenty budú navrhnuté na základe výsledkov klasifikácie a AR/BIA, • revízia FW pravidiel a VPN profilov, • doplnenie IDS/IPS do jednotlivých segmentov siete a ich napojenie na SIEM
1.7	**Implementácia centrálneho Log manažment systému (LMS)**	Implementácia systému za účelom zhrávania logov zo všetkých systémov, aplikácií a sieťových prvkov pre následné nasadenie Security Incident and Event Management (SIEM) • systém kompatibilný s už existujúcim AUDIT PLUS. • SIEM systém musí vykonávať analýzu nad všetkými záznamami ako celkom, teda analyzovať korelácie medzi udalosťami z Active Direcotry a udalosťami z iných systémov ako FW, SWITCHE atď. • musí mať podporu od dodávateľa na riešenie problémov min. 36 mesiacov, a na aktualizácie produktu min. 36 mesiacov, • min. podpora 8/5 NBD
1.8	**Vykonanie komplexnej konsolidácie všetkých logov**	Minimálne požiadavky na konsolidáciu všetkých logov pre efektívne a spoľahlivé fungovanie SIEM: • posúdenie existujúceho systému ManageEngine AD Audit Plus a jeho prípadné konfiguračné zmeny alebo rozšírenia tohto existujúceho systému o kompatibilnú funkcionalitu (rozšírenie existujúcej licencie produktu) ktorá by umožňovala analyzovať logy aj zo sieťových prvkov ako FW, SWITCHE atď. • analýza a návrh spôsobu zaznamenávania logov a auditných udalostí, ich centrálny zber a zhromažďovanie, ukladanie, uchovávanie, rotácia, • poskytovania analýz a reportovania, • parsovanie logov – pre definované OS, sieťové zariadenia, aplikácie a pod., • retenčná doba logov min. 6 mesiacov, • nasadenie prípadných agentov na zbieranie logov pre operačné systémy, • možnosť obohacovania logov o doplnkové informácie /geoip, threat intelligence,.../, • možnosť exportu logov,

		• možnosť kompresie logov, • možnosť automatického zálohovania logov na externé úložisko, atď..
1.9	**Zavedenie služby SIEM/SOC „as a service", vrátane externej podpory riešenia bezpečnostných incidentov**	Základné požiadavky na zavedenie služby SIEM: • Zakúpenie kompatibilného SIEM s existujúcim ManageEngine AD Audit plus do majetku ŠNOP a inštalácia do siete ŠNOP. • Prevádzka a správa SIEM zabezpečená v režime 24/7. • Konfigurovateľná funkcionalita detekcie hrozieb a reakcie na bezpečnostné incidenty pomocou „real time" vyhodnocovania a korelácie logov z LMS systému pre širokú škálu hrozieb a útokov. • Čítanie informácií zo sieťovej prevádzky v rámci OSI modelu s možnosťou odhalenia pokročilých útokov maskujúcich sa za inú aplikáciu, resp. službu. • Možnosť monitorovať virtuálne, ale aj fyzické systémy infraštruktúry ŠNOP. • Monitorovanie a korelovanie všetkých typov logovaných udalostí, vrátane rôznych OS (Windows, Unix) a zariadení (IDS/IPS, FW a pod.). • Predpokladaný počet Events per second (EPS) min. 250-500. • SOC (Security Operation Service) - poskytnutie služby s minimálnymi požiadavkami: ▪ výkon bezpečnostného monitoringu a zasielania notifikácií o prípadných bezpečnostných incidentoch na zodpovedného zamestnanca alebo povereného zamestnanca nemocnice (mail, telefón, SMS, ticketing systém) a ▪ podpora pri riešení a analyzovaní bezpečnostných incidentov.
1.10	**Vykonanie koordinácie a konsolidácia interných procesov riadenia bezpečnostných incidentov a interných procesov riadenia prevádzky IKT**	Koordinácia SOC služby v oblasti podpory riešenia bezpečnostných incidentov a ich analýzy s externou spoločnosťou, ktorá zabezpečuje správu siete IKT v ŠNOP a internými postupmi ŠNOP.

1.11	**V oblasti riadenia prístupov a bezpečnosti prevádzky IKT**	Implementácia SW podpory a nástroja pre manažment siete ŠNOP vrátane GUI rozhrania na správu (najmä existujúcich Aruba zariadení). Manažment musí umožňovať min. aktualizáciu firmware a nasadenie konfigurácií na Aruba switchoch. Podpora pri zavádzaní a konfigurácii autentifikácie zariadení v sieťach ŠNOP (implementácia protokolu 802.1x) rovnako v pevných sieťach ako aj vo wifi sieti (ŠNOP disponuje zariadeniami, sieťovými prepínačmi Aruba radu 2530 a rovnako aj certifikačnou autoritou v rámci Active Directory). Licencia s podporou min. 36 mesiacov
1.12	**HW na vyhodnocovanie bezpečnostných incidentov (SIEM), zber, parsovanie a koreláciu logov**	Navrhnutie hardvérového riešenia pre vyhodnocovanie bezpečnostných incidentov (SIEM), zber, parsovanie a koreláciu logov. Minimálne HW požiadavky sú min. 16GB RAM, min. SSD disky.
1.13	**Návrh a zabezpečenie SW/HW riešenia 2FA**	Zabezpečenie SW/HW riešenia 2FA (napr. formou mobilnej autentifikácie) na strane používateľov (pre VPN min. 20 používateľov) a na strane externého správcu (admin prístupy k IS – min. 5 administrátorov, resp. privilegovaných používateľov). Implementácia navrhnutého riešenia do existujúceho riešenia ESET protect console v nemocnici. 2FA v rámci domény pre privilegované účty je možné napr. pomocou SMART card
1.14	**Patch manažment systém pre platformu Windows - System Center Configuration Manager (SCCM)**	Súčasný stav: • správa min. 11x Windows Server 2019 Standard 16 Cores • správa min. 70x PC/NB Windows 10 • licencia s podporou na min. 36 mesiacov
1.15	**Softvérový nástroj na skenovanie zraniteľností (vulnerability scanner)**	• interný alebo cloudový (s interným scannerom) nástroj na skenovanie zraniteľností (vulnerability scaner) • skenovanie interných zariadení OS Windows, OS Linux, HW vrátane pracovných staníc používateľov (rádovo 100 IP adries – min. 11x Windows Server 2019 + min. 70x PC/NB Windows 10 + min. 4x Linux, FW a iné aktívne, konfigurovateľné sieťové prvky)

		• iný alebo rovnaký produkt na pravidelné skenovanie www.snop.sk • nástroj podporovaný výrobcom s prístupom k aktuálnym databázam hrozieb a zraniteľností systémov, • licencia na aktualizáciu DB hrozieb počas doby trvania 5 rokov, • agent pre vnútorné skenovanie zraniteľností operačného systému windows, konfigurovateľný z centrálneho manažmentu systému • realizácia iniciálneho vulnerability testu (scanu) interných systémov a web stránky a zaškolenie administrátora ŠNOP. • licencia s podporou na min. 36 mesiacov

V Mojši, dňa 22.6.2023

.....

Vladimír Staňo – predseda predstavenstva