Príloha č. 1 Opis predmetu plnenia a požiadavky na spôsob plnenia

„Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v zdravotníckych zariadeniach"

1. Všeobecný popis zadania

1.1 Popis východiskovej situácie, relatívna dôležitosť kybernetickej bezpečnosti u žiadateľa

Špecializovaná nemocnica pre ortopedickú protetiku Bratislava, n.o. (ďalej len „ŠNOP" alebo „Objednávateľ") je špecializovaným a koncovým zdravotníckym zariadením, má celoslovenskú pôsobnosť a prednostne sa zameriava na pacientov s problémami oporno-pohybovej sústavy.

V nemocnici sa poskytuje zdravotná starostlivosť na:
- ambulantnom oddelení vrátane RTG pracoviska,
- lôžkovom oddelení,
- rehabilitačnom oddelení vrátane vodoliečby,
- operačnom oddelení.

ŠNOP má viacero kritických informačných systémov:
- Nemocničný informačný systém:
  - Winambulancia
  - Winrecepcia
  - Winoddelenie
- Synapse RIS (Oracle)
- DQC monitor
- Pluscomp - mzdový a personálny systém (MSSQL)
- Pohoda – SW na vedenie účtovníctva (MSSQL)
- Kamerový systém - Hikvision
- Attis – SW na dokumentáciu IMS
- Web stránka ŠNOP

Okrem vyššie uvedených IS spravuje ŠNOP v elektronickej forme (prevažne MS excel) aj ďalšie evidencie, ktoré obsahujú citlivé osobné a zdravotné dáta, ktorým je z pohľadu IB a KyB rovnako potrebné venovať patričnú pozornosť. Ide najmä o:
- Schvaľovanie hospitalizácií a výkonov JZS
- Operačný program JZS
- Podosat4 - Eclipse meranie nôh
- Systém rekondičných aktivít
- Registratúrny systém

Dôležitosť IT a kybernetickej bezpečnosti a reálne zavedenie fungujúcich a efektívnych bezpečnostných opatrení do praxe je nevyhnutné. Ohrozenie bezpečnosti informačných systémov a hlavne citlivých osobných a zdravotných údajov pacientov (napr. neautorizovaná zmena integrity alebo nedostupnosť údajov) chápeme primárne aj ako potenciálne ohrozenie ich zdravia a života formou kybernetického incidentu.

Z uvedených dôvodov bola v rámci ŠNOP spracovaná komplexná analýza rizík, ktorá obsahuje aj IT riziká a prijaté čiastkové opatrenia najmä pre oblasť ochrany osobných údajov. Systematicky sa však

problematika IB a KyB zatiaľ neriešila aj pre nedostatok finančných prostriedkov. Jednotlivé oblasti riadenia IB a KyB sú aktuálne riešené skôr ad-hoc, a úroveň ich vyspelosti je pre jednotlivé oblasti rôzna. Aktuálne nie je skoro vôbec pokrytá oblasť bezpečnostného monitoringu a následného systematického riešenia bezpečnostných incidentov.

1.2 Mapa IT štruktúry

Hardvérové vybavenie nemocnice predstavuje:

- min. 66 PC staníc vrátane notebookov (HPE ProDesk G5 az G6)
- min. 34 tlačiarní, HPE, OKI
- pripojenie na internet – RAINSIDE GARANT 50/550 Mbit/s - prívod optiky + HW Rainside

Palo Alto PA-440

- hlavný router, Inter VLAN routing, DHCP server, Layer7 filtering,
- Global Project (exmail.snop.sk) VPN
- licencie PAN-PA-440-BND-PRO, PAN-SVC-BKLN-440, PAN-PWR-CORD-EU

Mikrotik RB1100x4 Dude - Inter VLAN routing

- Záložný router, Inter VLAN routing, DHCP server, Layer3 filtering,
- DHCP server, OpenVPN,
- CAPsMAN controler pre WIFI na všetkých poschodiach - 34 CaPs,
- Pri výpadku PA-440, má rovnakú konfiguráciu LAYER3

2x Server HPE ProLiant DL360 Gen10

- (Server 2019 Standard) ako MS HyperV HA CLUSTER
- 2xXEON 4208 (8 cores) spolu 16 cores na jeden server, 256GB RAM, SSD RAID1 460GB
- Pripojene na diskové pole MSA2050 pomocou SAS
- Microsoft Failover Cluster – Hyper-V

MSA2050 (7TB - RAID6 SAS, 1.5TB - RAID5 SSD) Virtual Machine HA:

- DC01 - Windows 2019 Standard
- FileServer - Windows 2019 Standard
- Winamb - Windows 2019 Standard
- Pohoda - Windows 2019 Standard (MsSQL Express)
- ATTIS4 - Windows 2019 Standard (MsSQL Express)
- QlickSense - Windows 2019 Standard (IIS)
- Synapse - Windows 2016 Standard (Oracle)
- Eset Protect
- Dochadzka SQL - W10pro
- Linux Mail

1x ProLiant DL380p Gen8

Server 2019 Standar HyperV host

- 2x XEON E-2560 (8 cores) spolu 16 cores, 128GB Ram
- 1TB SSD Raid1, 1TB RAID5 SAS HyperV
- Virtual Machine:
  - DC02 - Windows 2019 Standard
  - W10pro - RDP
  - Zabbix Linux - monitroing všetkých prekov IT okrem PC/NB
  - LibreNMS Linux - monitoring SNMP pre sieťové zariadenia
  - Linux

SWITCHE

3x Aruba HP J9775A 2530-48G	do **31.10.2026 podpora**
2x HP J9776A 2530-24G Switch	do **31.10.2026 podpora**
2x HP J9773A 2530-24G-PoEP	do **31.10.2026 podpora**
1x CBS220-16P-2G-Cisco-16p	do **31.07.2027 podpora**
1x CBS220-16T-2G-SwitchB2428E	do **31.07.2027 podpora**

- Zálohovanie HyperVHornetSecurity + HornetSecurity Offiste Backup
- VPN štátna pokladnica (samostatný ADSL modem)
- Ostatné bezpečnostné prvky

Nemocnica disponuje dvomi serverovňami, na 2. NP a 3. NP budovy nemocnice. Prístup do priestorov je umožnený schodiskom alebo výťahom; miestnosti sú klimatizované pravidelne servisovanými klimatizačnými jednotkami a teplota v serverovni je monitorovaná teplotnými senzormi; odchýlenie od nastavených hodnôt je notifikované zodpovedným osobám s povereným vstupom do priestorov. Hardvérové vybavenie servera je umiestnené v rekových skriniach v priestoroch serverovní.

Softvérové vybavenie nemocnice:

- brána firewall a ochrana pred neoprávneným vstupom PA-440 od spoločnosti Palo Alto Networks, ktorý v reálnom čase monitoruje a vyhodnocuje prípadné zraniteľnosti, komunikáciu na IoC adresy a riadi sieťové toky,
- z pohľadu bezpečnostného monitoringu na účely zberu logov a ich vyhodnocovania používa nemocnica aplikáciu ManageEngine ADAudit Plus, ktorá vyhodnocuje základné typy škodlivých udalostí a pre vybrané udalosti (napr. prihlásenie, odhlásenie, prístup k súborom, zmena oprávnení, smeny na úrovni používateľov, skupín, GPO, korelácie udalostí ako vyhodnotenie prístupov na základe času, viacnásobné prihlásenie pod tým istým kontom na rôznych PC v rovnakom čase atď.) zasiela administrátorovi IT mailové notifikácie
- prevádzka a správa týchto zariadení je zabezpečená v režime 8x5
- monitorovací nástroj LibreNMS (SNMP monitoring SWITCHOV a FW)
- Eset Protect – Aktualizácie Endpoint, monitoring udalostí IDS/HIPS zo všetkých WINDOWS OS

1.3 Mapa IMS

Integrovaný manažérsky systém kvality (ďalej IMS) je certifikovaný podľa ISO 9001:2015, ISO14001:2015 a ISO 45001:2018 a v rámci podporných procesov je proces 3. INF Ochrana osobných údajov a zabezpečenie IT, súčasťou ktorého je bezpečnostná dokumentácia

Bezpečnostná dokumentácia

ŠNOP aktuálne disponuje dokumentáciou v zmysle zavedeného IMS, ktorá čiastočne pokrýva aj rôzne oblasti riadenia IB a KyB. Túto dokumentáciu je potrebné rozšíriť, zaktualizovať, prípadne vytvoriť nové dokumenty pre oblasti riadenia IB a KyB, ktoré ešte nie sú pokryté vôbec (napr. BCP a DRP plány, min. pre najkritickejšie systémy).

2. Špecifikácia predmetu plnenia

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

Objednávateľ požaduje, aby realizáciu plnenia Zhotoviteľ zabezpečoval prostredníctvom osôb, ktoré sú technicky a odborne spôsobilé na jeho realizáciu.

3. Formy spolupráce a súčinnosti

Miestom realizácie predmetu plnenia je sídlo Objednávateľa.

V prípade technologických opatrení Objednávateľ požaduje konkrétny technologický návrh na základe technickej špecifikácie a parametrov informačnej siete Objednávateľa. Zhotoviteľ vytvorí dokument s presným technickým popisom riešenia a špecifikáciami hardvéru resp. softvéru.

Vedeniu ŠNOP budú na schválenie predložené vypracované smernice, a najmä spôsob riadenia (mitigácie) identifikovaných rizík z aktualizovanej AR/BIA, čo zabezpečí formálne zadefinovanie procesov pre oblasť riadenia IB a KyB.

Z pohľadu technických opatrení budú do praxe zavedené bezpečnostné informačné systémy, aplikácie a riešenia, ktoré prispejú najmä k včasnej identifikácií bezpečnostných incidentov, ich efektívnemu a rýchlemu riešeniu a k celkovému zvýšeniu úrovne IB a KyB v rámci ŠNOP.

Ak je súčasťou predmetu plnenia aj tovar, resp. v tých častiach plnenia, kde je predmetom plnenia aj tovar, tovarová časť predmetu plnenia musí byť:

- dodaná ako nová a nepoužitá, pričom za novú sa považuje, ak rok dodania je totožný s rokom výroby predmetu plnenia, alebo ak rok výroby predmetu plnenia je o jeden rok nižší ako je rok dodania predmetu plnenia;
- certifikovaná v súlade s platnou legislatívou EÚ a SR;
- súčasťou ceny aj doprava do miesta dodania určeného Objednávateľom;
- súčasťou predmetu plnenia aj montáž dodaného tovaru, dodanie kompletnej dokumentácie dodaného riešenia, otestovanie dodaného a nainštalovaného predmetu plnenia pred uvedením do ostrej prevádzky a zaškolenie budúcej obsluhy (zamestnancov Objednávateľa) na prácu s nainštalovaným predmetom plnenia v mieste sídla Objednávateľa;
- súčasťou predmetu plnenia aj dodanie záručných listov a návodov na obsluhu v slovenskom jazyku alebo v českom jazyku, zápisníc a osvedčení o vykonaných skúškach, certifikáty a atesty, správy o vykonaných odborných skúškach a odborných prehliadkach a skúškach, prevádzkové poriadky, doklady o zaškolení obsluhy Objednávateľa a ostatné doklady súvisiace s predmetom plnenia, ak si to povaha plnenia vyžaduje.

Projekt je realizovaný s cieľom rozšíriť spôsobilosti v oblasti informačnej a kybernetickej bezpečnosti v rámci ŠNOP a zabezpečiť súlad so zákonom o ITVS a zákonom o KyB. Financovanie aktivít predmetu plnenia bude realizované formou projektu podporeného z dopytovej výzvy „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v zdravotníckych zariadeniach".

Implementáciou bezpečnostných opatrení a následným ukončením realizácie predmetu plnenia bude Objednávateľ spĺňať legislatívne požiadavky vyplývajúce z informačnej a kybernetickej bezpečnosti a legislatívy k ITVS. Zároveň bude Objednávateľ pripravený na úspešný audit v kybernetickej bezpečnosti.

4. Záruka a záručná doba

Záručná doba na poskytnuté služby

- Všetky skutočnosti, ktoré budú počas realizácie predmetu plnenia vyhodnotené ako nezhody a neboli identifikované vykonaním rozdielovej analýzy sú predmetom záruky a Zhotoviteľ je povinný navrhnúť opatrenia na ich odstránenie.
- Záručná doba končí úspešným auditom kybernetickej bezpečnosti, alebo neúspešným auditom, ak všetky nezhody zistené počas auditu boli identifikované v rozdielovej analýze. Objednávateľ

vykoná audit kybernetickej bezpečnosti do 6 mesiacov od ukončenia plnenia podľa tejto zmluvy. Ak audit v tejto dobe nebude vykonaný, záručná doba bude ukončená.

Záruka a záručná doba a podpora softvérového vybavenia predmetu plnenia

- Softvérové licencie z predmetu plnenia požaduje Objednávateľ s podporou min. 36 mesiacov.

Záruka a záručná doba hardvérového vybavenia predmetu plnenia

- Záruka pre hardvérové vybavenie z predmetu plnenia min. 36 mesiacov .

5. Harmonogram požiadaviek podľa hlavných aktivít projektu

Trvanie činnosti	Obsah činnosti	Termín realizácie (počet prac. dní)
Začiatok projektu	Začiatok projektu	T1 = T0a + 5
Fáza 1 cca 2 mesiace	Analýza a dizajn (predpokladaný rozsah v zmysle projektu - 38 človekodní) Činnosť zahŕňa odovzdanie produktov (výstupov) 1.1 – 1.4. v zmysle bodu 2 Špecifikácia predmetu zákazky Nákup technických prostriedkov, programových prostriedkov a služieb Činnosť zahŕňa odovzdanie produktov 1.9., 1.11, 1.12, 1.14. a 1.15. v zmysle bodu 2 Špecifikácia predmetu zákazky	T2 = T1 + 35
Fáza 2 cca 2 mesiace	Implementácia a testovanie (predpokladaný rozsah v zmysle projektu - 13 človekodní) Činnosť zahŕňa poskytovanie služieb podľa bodu 1.5 – 1.6. v zmysle bodu 2 Špecifikácia predmetu zákazky Implementácia a testovanie (predpokladaný rozsah v zmysle projektu - 96 človekodní) Činnosť zahŕňa poskytovanie služieb podľa bodu 1.7, 1.8, 1.10 v zmysle o bodu 2 Špecifikácia predmetu zákazky	T3 = T2 + 38
Fáza 3 cca 1 mesiac	Nasadenie (predpokladaný rozsah v zmysle projektu - 3 človekodní) Činnosť zahŕňa poskytovanie služieb podľa bodu 1.5 – 1.6. v zmysle bodu 2 Špecifikácia predmetu zákazky Nasadenie (predpokladaný rozsah v zmysle projektu - 10 človekodní) Činnosť zahŕňa poskytovanie služieb podľa bodu 1.13 v zmysle bodu 2 Špecifikácia predmetu zákazky	T3 = T2 + 16

T0 – dátum vstupu do platnosti zmluvy o dielo. Dni použité pre výpočet termínov sú pracovné dni.

V prípade, že bude možné realizovať plnenie jednotlivých etáp v skorších termínoch, na ktorých sa Zmluvné strany dohodnú, nebude potrebné takto upravené termíny predložiť na schválenie. Harmonogram činností musí byť ukončený a odovzdaný najneskôr do 30.09.2023.

Zoznam skratiek

2FA	Dvojfaktorová autorizácia
AR	Analýza rizík
BCM	Business Continuity Management (Oblasť riadenia kontinuity procesov)
BCP	Business Continuity Plan
BIA	Analýza dopadu
DRP	Disaster Recovery Plan
FW	Firewall
HW	Hardvér
IB	Informačná bezpečnosť
IDS/IPS	Intrusion detection systems / Intrusion prevention systems
IMS	Integrovaný manažérsky systém na báze ISO 9001:2015, ISO14001:2015 a ISO 45001:2018
IT	Informačné technológie
ITVS	Informačné technológie verejnej správy
IS	Informačný systém
KYB	Kybernetická bezpečnosť
LMS	Log manažment systém
NBD	
NBÚ	Národný bezpečnostný úrad
NIS	Nemocničný informačný systém
OS	Operačný systém
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SIEM	Security Incident and Event Management
SOC	Security Operation Centre
SW	Softvér
ŠNOP	Špecializovaná nemocnica pre ortopedickú protetiku Bratislava, n.o.