Příloha č. 3 Zadávací dokumentace – Technická dokumentace zadavatele

Příloha č. 1 Kupní smlouvy – Technická dokumentace kupujícího

1 Technická specifikace zadavatele (kupujícího)

Obsah

Kupující požaduje dodávku jednotlivých komponent dle této technické dokumentace včetně příslušenství v níže uvedené minimální specifikaci.

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

Součástí dodávky níže uvedených technologií budou i dále uvedené služby.

Součástí dodávky bude dále dodávka dokumentace a nezbytné zaškolení administrátorů v prostředí kupujícího k běžnému provozu a ovládání dodaných technologií včetně specifik a konfigurace provedené v prostředí kupujícího.

Nabízené zboží musí být standardní, běžně dostupné a určené k produkčnímu použití.

Není dovoleno použití beta-verzí, kódu s custom úpravami či neoficiálních verzí.

Veškeré nabízené zboží musí být pokryto oficiálním supportem, přičemž požadavek na provedení bezplatného servisního zásahu musí být možné kdykoliv vznést přímo na výrobce zařízení.

Veškeré deklarované funkce a technické parametry nabízeného zboží musí být dostupné nejpozději dnem podání nabídky.

Deklarované funkce a technické parametry nabízeného zboží musí být ověřitelné prostřednictvím oficiálních datasheetů, release notes či manuálů vydaných výrobcem.

Užité pojmy níže:

- NBD – další pracovní den, tzn. například realizace opravy zařízení nejpozději další pracovní den od nahlášení
- x BD – x pracovních dnů, tzn. například realizace opravy zařízení nejpozději poslední pracovní den dané lhůty od nahlášení
- on-site – realizace například opravy zařízení v místě dodávky

Všechny aktivní prvky musí být z důvodu snadné údržby a jednotné servisní podpory od stejného výrobce. Musí být instalovány nové, nepoužité, licencované na koncového uživatele a musí na ně být poskytnuta záruka výrobce v požadované délce. Součástí této záruky výrobce musí být:

- zrychlená výměna hardwaru odeslání náhradního dílu NBD
- nárok na nový software po dobu životnosti
- přístup na support portál výrobce

Dodavatel se zaváže, že dodané síťové zařízení:

- pochází z autorizovaného prodejního kanálu výrobce
- má záruku výrobce
- splňuje podmínky servisní podpory výrobce

- obsahuje software výrobce s platnou licencí
- splňuje podmínky předpisů EU ohledně paralelního importu
- je reportováno zpět výrobci jako prodáno kupujícímu.

Dodavatel poskytne písemné potvrzení od zastoupení výrobce pro Českou republiku, že zařízení je z pohledu výrobce autorizované ve jménu kupujícího.

2 Návaznost na projekty nemocnic

Předmět plnění této technické specifikace plánuje kupující kofinancovat z několika projektů IROP jednotlivých nemocnic. Výčet projektů je uveden níže a dopad na fakturaci těchto projektů je uveden v kupní smlouvě.

Seznam projektů, které zajišťují kofinancování předmětu plnění této technické specifikace:

- Zvýšení kybernetické bezpečnosti Oblastní nemocnice Náchod a.s. v oblasti komunikačních sítí
- Zvýšení kybernetické bezpečnosti Oblastní nemocnice Trutnov a.s. v oblasti komunikačních sítí
- Zvýšení kybernetické bezpečnosti Oblastní nemocnice Jičín a.s. v oblasti komunikačních sítí
- Zvýšení kybernetické bezpečnosti Městské nemocnice, a.s. v oblasti komunikačních sítí

Z tohoto důvodu je potřeba odlišovat požadavek kupujícího na transparentní oddělení jednotlivých částí plnění tak, aby byla možná jednoduchá a transparentně přezkoumatelná fakturace plnění pro jednotlivé nemocnice, ale na druhou stranu samotné nemocnice a jejich zakladatel Zdravotnický holding Královéhradeckého kraje a.s. sledují klíčový cíl provozovat unifikovanou síťovou infrastrukturu, ve které si budou moci vzájemně vypomáhat, bude možné komplex sítě centrálně a jednotně řídit a její další rozvoj bude možné koordinovat společně.

Výsledné řešení tohoto plnění dále musí umožnit užití jednotných bloků IP adres napříč nemocnicemi v rámci konkrétních VLAN a další společně nastavená síťová pravidla, a tedy i spolupráci a výměnu dat jejich prostřednictvím.

Z tohoto důvodu je důležité, aby prodávající respektoval strukturu cenové tabulky, ve které je rozděleno plnění pro jednotlivé nemocnice, a současně aby ceny souvisejících prací, dodávek a služeb v podobě příslušenství zohlednil do cen těch položek, kterých se to bezprostředně týká a které budou součástí dodávky do jednotlivých nemocnic.

3 Místo plnění

Místem plnění jsou areály jednotlivých nemocnic na následujících adresách:

- **Oblastní nemocnice Náchod a.s.**
  - Purkyňova 446, 54701 Náchod
  - Bartoňova 951, 54701 Náchod
  - Jiráskova 506, 51601 Rychnov nad Kněžnou
  - Smetanova 91, 55001 Broumov – Nové Město
  - Národní 83, 55101 Jaroměř – Pražské Předměstí
  - T. G. Masaryka 367, 54901 Nové Město nad Metují, Česko
  - Pitkova 635, 517 73 Opočno
- **Oblastní nemocnice Trutnov a.s.**
  - Maxima Gorkého 77, 54101 Trutnov - Kryblice
  - Slezská 166, 54101 Trutnov – Vnitřní Město (budova finančního úřadu)
- **Oblastní nemocnice Jičín a.s.**

- Bolzanova 512, Valdické Předměstí, 506 01 Jičín
- Jana Maláta 493, 50401 Nový Bydžov

- **Městská nemocnice, a.s.**
  - Vrchlického 1504, 544 01 Dvůr Králové nad Labem
  - Rooseveltova 474, 54401 Dvůr Králové nad Labem

4 Počet a typ technologií

Počet a typ jednotlivých technologií, které jsou specifikovány níže, je definován v samostatné příloze zadávací dokumentace a kupní smlouvy v podobě cenové tabulky.

Cílem této tabulky je předcházet duplicitám v počtu uváděných typů kusů technologií, které navíc ještě musejí být rozděleny mezi jednotlivé projekty nemocnic.

V této technické specifikace je proto klíčovým požadavkem funkcionalita, související služby a případné příslušenství jednotlivých kusů plnění, když počet a jejich umístění co do konkrétní nemocnice a jejího areálu je uveden v cenové tabulce.

Instalační a další související práce spojené s dodávkou a nasazením jednotlivých technologií prodávající zohlední v ceně jednotlivých zařízení.

Příslušenství - Příslušenství pro jednotlivé technologie v počtu a typu transceiverů a dále kabelů pro propojení technologií v rámci jednotlivých racků a technologických místností je co do počtu a typu specifikováno rovněž v cenové tabulce.

5 Autentizační platforma (AAA)

Požadujeme centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti a guest přístup, definující pravidla přístupu k síti v závislosti na kontextu připojení (uživatel, typ zařízení, stav zařízení, místo připojení apod.). Ve spolupráci s aktivními prvky (LAN přepínači, bezdrátovými AP nebo VPN branami) poskytne tato autentizační platforma (AAA) ochranu před neoprávněným přístupem k pevné LAN síti, bezdrátové wifi síti (metodou 802.1x) a pro VPN přístup.

AAA bude řídit bezpečný přístup uživatelů a zařízení ke sdíleným síťovým zdrojům a bude mít vazbu na stávající řešení perimetru sítě na platformě FortiGate. Systém bude na základě sdílených informací umožňovat pozorovat infikovaná koncová zařízení, omezit jim přístup, nebo napomoci v remediačním procesu.

Systém musí být plně kompatibilní s dodávanými přepínači a bezdrátovými přístupovými body.

V ON Náchod je již provozován Policy Manager Aruba ClearPass pro 1500 současně autentizovaných zařízení (802.1x). Tento systém bude licenčně rozšířen tak, aby pokrýval celou nemocnici tzn. na 5000 současně autentizovaných zařízení. Součástí dodávky bude i upgrade systému ClearPass na aktuální verzi. Zadavatel však připouští nahrazení stávajícího systému Aruba ClearPass v ON Náchod tak, aby nově dodávaný systém plně nahradil stávající a plně pokrýval 5000 současně autentizovaných zařízení.

Současně je v ON Náchod provozována bezdrátová WiFi síť řízená dvojicí kontrolérů Aruba 7210 v HA zapojení. Tato síť bude rozšířena o kompatibilní bezdrátové přístupové body. Součástí dodávky bude upgrade SW Aruba Mobility Controller na aktuální verzi.

Zadavatel připouští nahrazení stávajícího řešení bezdrátové sítě založené na HA dvojici HW kontrolérů Aruba 7210. Současně s náhradou kontrolérů musí dodavatel nahradit 200 ks stávajících bezdrátových přístupových bodů včetně příslušných licencí.

V nemocnicích Jičín, Trutnov a Dvůr Králové jsou vybudována datová centra s využitím HA zapojení přepínačů Aruba 8325 a Aruba 6300. Datové centrum v Náchodě je napojeno přes prvky Aruba 8325 TOR v budovách A a K na CORE prvky Aruba 8320. Dále je v nových budovách J a K provozováno 87 ks access přepínačů HPE Aruba série 2930.

Požadavek na funkcionalitu	**Minimální požadavky**
Celková kapacita řešení současně autentizovaných (pomocí 802.1x) zařízení v **ON Trutnov**	3500
Celková kapacita řešení současně autentizovaných (pomocí 802.1x) zařízení v **ON Jičín**	3000
Celková kapacita řešení současně autentizovaných (pomocí 802.1x) zařízení v **N Dvůr Králové n. L.**	500
Požadavek na funkcionalitu – společné parametry	**Minimální požadavky**
Autentizační platforma (AAA) pro řízení přístupu uživatelů a zařízení do LAN a WiFi.	ANO
Virtuální appliance pro on-premise prostředí VMware	ANO
Virtuální appliance bez nutnosti dodatečných licencí např. pro OS nebo databáze.	ANO
Podpora řešení vysoké dostupnosti tak, aby v případě výpadku primárního AAA serveru převzal jeho roli sekundární server	ANO
Možnost vytváření clusteru více virtuálních appliance.	ANO
Cluster musí poskytovat vysokou dostupnost pro všechny funkcionality řešení a zároveň možnost navýšení počtu podporovaných uživatelů přidáním další instance.	ANO
Požadované metody autentizace uživatelů a zařízení	PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace
Podpora RADIUS pro autentizaci, autorizaci, zaznamenávání a proxy funkci pro externí RADIUS	ANO
Podpora RadSec (RADIUS over TLS)	ANO

Podpora RADIUS CoA dle RFC3576	ANO
Podpora autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, osobní profil či skupina v MS Active Directory	ANO
Možnost autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. za účelem omezení celkového času online či objemu přenesených dat za delší časové období	ANO
Možnost TACACS+ autentizace správců síťových zařízení	ANO
Řízení konfiguračních nebo přehledových příkazů na prvcích infrastruktury podle role administrátora	ANO
Možnost definice sad příkazů a jejich přiřazení podle role administrátora	ANO
Možnost integrace vícefaktorové autentizace pro řízení přístupu k prvkům sítě	ANO
Okamžité informace o prováděných příkazech na síťových zařízeních	ANO
Další požadované autentizační a autorizační zdroje a metody	LDAP, MS AD, Token, MAC, generická SQL databáze, Kerberos, HTTPS web autentizace, SSO (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta)
Ověření uživatelů heslem nebo certifikátem	ANO
Interní databáze pro uživatele i koncová zařízení	ANO
Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle: - uživatele (role, skupiny), - stavu a typu koncového zařízení (viz výše), - místa připojení, - historie připojení	ANO
Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě	ANO
Zaznamenávání aktivity uživatelů a zařízení připojených k síti	ANO
Snadné vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod.	ANO
Samoobslužný portál pro uživatele	ANO
Registrace zařízení pomocí MAC adresy pro non-IT uživatele – omezená funkce administračního rozhraní, se zařazením zařízení do skupiny s definovanou politikou přístupu.	ANO

Podpora REST API pro většinu základních úkonů AAA platformy	ANO
Zpracovávání syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Minimálně v rozsahu přijmutí bezpečnostního hlášení z firewallu a izolace konkrétního klienta na základě tohoto hlášení.	ANO
Sběr dodatečných informací o připojených zařízeních ("profiling") jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace musí být možné využít pro doplňkové ověření přístupu zařízení do sítě.	ANO
Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle: - uživatele (role, skupiny), - stavu a typu koncového zařízení (viz výše), - místa připojení, - historie připojení	ANO
Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě	ANO
LAN a WLAN Guest portál. Portál musí podporovat možnost přihlašování přes účty minimálně těchto sociálních sítí – Linkedln, Facebook, Twitter. Portál musí umožňovat bohatou grafickou úpravu včetně možnosti přidávání videí a dalšího dynamického obsahu. Možnost samoobslužné registrace hosta do sítě pomocí SMS, email ověřením nebo na elektronickou notifikaci a schválení pověřených pracovníků.	ANO
Centralizovaná správa s grafickým rozhraním	ANO
Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému	ANO
Zjednodušení správy vytvářením skupin uživatelů, koncových a síťových zařízení	ANO
Zaznamenávání událostí na externí syslog server	ANO
Podpora SNMPv3	ANO
NTP pro synchronizaci času	ANO
Certifikace Common Criteria a FIPS 140-2	ANO
Automatické zakázání non-FIPS autentizačních protokolů (např. PAP/ASCII, CHAP, and MS-CHAPv1) při aktivaci FIPS módu	ANO
Systém musí podporovat funkce na poptávaném bezdrátovém řešení a přepínačích	ANO
Jakékoliv funkční rozšíření systému musí být vždy v rámci stejné virtuální appliance jako je AAA systém.	ANO
Technická podpora na 5 let garantovaná přímo výrobcem technologie v režimu NBD. Možnost otevírat servisní požadavky přímo u výrobce.	ANO

6 Přepínač typ 1

Požadavek na funkcionalitu	Minimální požadavky
Typ přepínače	L3 switch
Montáž do racku, velikost max. 1U	ANO
Podpora virtualizace – možnost sloučit alespoň dva fyzické přepínače do jednoho logického celku – virtuálního switche	ANO
Podpora upgrade software za provozu (ISSU nebo ekvivalentní)	ANO
OoB management formou portu RJ45 s podporou ethernetu	ANO
Interní hot-swap AC napájecí zdroj	2x
Redundantní hot-swap ventilátory	ANO
Směr proudění vzduchu zařízením: zepředu-dozadu	ANO
Minimální počet 1/10/25Gbps portů s volitelným fyzickým rozhraním	32
Minimální počet 40/100Gbps portů s volitelným fyzickým rozhraním	4
Wirespeed (neblokující) na všech portech	ANO
Minimální propustnost přepínače	2,4 Tbps
Minimální paketový výkon přepínače	1 Bpps
Min. počet IPv4 unicast směrovacích záznamů	212 000
Min. počet IPv6 unicast směrovacích záznamů	212 000
Minimální počet záznamů v tabulce MAC adres	82 000
IEEE 802.3-2005	ANO
Podpora seskupení portů Muli-chassis LAG (IEEE 802.3ad) mezi různými prvky	ANO
IEEE 802.3ad přes více šasi (funkční ekvivalent Multichassis Etherchannel)	ANO
Podpora jumbo rámců včetně velikosti 9198 Byte	ANO
IEEE 802.1D	ANO
Minimální počet aktivních VLAN podle IEEE 802.1Q	4 000
Tunelování 802.1Q v 802.1Q	ANO
IEEE 802.1X – Port Based Network Access Control	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)	ANO
802.1x autentizace přepínače vůči nadřazenému přepínači	ANO
Podpora linkové agregace IEEE 802.1AX	ANO
Podpora RADIUS CoA	ANO
Podpora Radius over TLS (RadSec)	ANO

IEEE 802.1s – Multiple Spanning Trees	ANO
IEEE 802.1w – Rapid Tree Spanning Protocol	ANO
IEEE 802.1p	ANO
Protokol pro definici a správu VLAN sítí: MVRP nebo VTP	ANO
Detekce protilehlého zařízení: CDP nebo LLDP	ANO
Detekce jednosměrnosti optické linky: UDLD nebo DLDP	ANO
STP root guard a STP loop guard nebo ekvivalentní	ANO
Možnost autorecovery po chybovém stavu (root guard, loop guard)	ANO
Multicast/broadcast storm control – hardwarové omezení poměru unicast/multicast rámců na portu	ANO
Router Redundancy protokol pro IPv4 a IPv6 (např. VRRP nebo HSRP)	ANO
DHCP server a relay pro IPv4 a IPv6 včetně podpory VRF	ANO
IP alias (více IP sítí na jednom rozhraní)	ANO
IPv6 ACL a IPv6 QoS	ANO
IPv6 services (DNS, Telnet, SSH, Syslog, ICMP, DHCP)	ANO
IPv6 Multicast (MLDv1 & v2)	ANO
IPv6 MLDv2 snooping	ANO
HTTP, SNMP přes IPv6	ANO
RADIUS, TACACS+ pomocí IPv4 a IPv6	ANO
Dynamické směrování: RIPv2, OSPFv2,BGPv4, OSPFv3 a MP BGP	ANO
Podpora service insertion včetně technologie VXLAN	ANO
Dynamické směrovací protokoly podporují autentizaci	ANO
Policy-based routing podle ACL	ANO
Podpora minimálně 256 logických virtuálních směrovacích instancí (VRF)	ANO
Protokoly a služby ve VRF (RADIUS, TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)	ANO
Multicast: PIM-DM, PIM-SM, IPv6 PIM-SM, PIM-SSM, IPv6 PIM-SSM, MSDP	ANO
IGMPv2, IGMPv3	ANO
IGMPv3 snooping	ANO
ACL na rozhraní IN/OUT (včetně virtuálních – VLAN, 802.3ad)	ANO
ACL pro IP	ANO
ACL pro ethernetové rámce	ANO
Možnost definovat povolené MAC adresy na portu	ANO
Možnost definovat maximální počet MAC adres na portu	ANO

Zabezpečení a analýza DHCP protokolu (např. DHCP snoopingu nebo funkčně ekvivalentní)	ANO
Podpora ochrany podvrženého mapování IP/MAC adresy (např. IP Source Guard/IPSG nebo funkčně ekvivalentní)	ANO
Ochrana centrálního procesoru (control plane) před útoky typu DoS	ANO
CLI rozhraní	ANO
Python scripting – lokální interpret jazyka v přepínači	ANO
Linux shell	ANO
Konfigurace zařízení v člověku čitelné textové formě	ANO
SSHv2	ANO
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ANO
SNMPv2 a SNMPv3	ANO
Podpora synchronizace času protokolem NTPv3 (klient i server)	ANO
Monitorování aplikačních toků prostřednictvím technologie NetFlow nebo IPFIX	ANO
Interní uložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení: min. 30 GB	ANO
AAA ověřování uživatelů (autentizace, autorizace, accounting) - TACACS+, RADIUS – minimálně 3 servery	ANO
Zrcadlení portů (např. SPAN nebo ekvivalentní)	ANO
Vzdálený port mirroring (ERSPAN)	ANO
Syslog – minimálně 3 servery	ANO
Syslog SNMP trap	ANO
Uživatelsky modifikovatelné automatické reakce/obsluhy událostí při provozu přepínače (např. pomocí EEM skriptů nebo ekvivalentní)	ANO
Nástroje měření odezev sítě (např. IP SLA nebo ekvivalentní)	ANO
Možnost automatické nebo manuální zálohy konfigurace z externího zdroje	ANO
NTP klient i server	ANO
DHCP server	ANO
Ochrana proti nahrání modifikovaného SW do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu OS zařízení prostřednictvím TPM čipu	ANO
Doživotní záruka výrobce, tzn. min. 5 let od ukončení prodeje, včetně vestavěných zdrojů a ventilátorů a nároku na běžně dostupné nové verze SW.	ANO

7 Přepínač typ 2

Požadavek na funkcionalitu	Minimální požadavky
Typ přepínače	L2/L3 switch
Montáž do racku, velikost max. 1U	ANO
OoB management formou portu RJ45 s podporou ethernetu	ANO
Interní AC zdroj	ANO
Minimální počet 10/100/1000Mbps metalických portů	48
Minimální počet 10Gbps SFP+ portů s volitelným fyzickým rozhraním	4
Minimální propustnost přepínače	176 Gbps
Minimální paketový výkon přepínače	130 Mpps
Minimální kapacita sběrnice stohu	8MB
Podpora PoE+ dle standardu	802.3at
Dostupný výkon pro PoE+ napájení	370W
Schopnost poskytovat PoE napájení připojeným zařízením i během restartu přepínače	ANO
Podporovaný počet přepínačů ve stohu	8
Minimální kapacita sběrnice stohu	80 Gbps
Redundance řídícího prvku v rámci stohu	ANO
Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)	ANO
Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG)	ANO
Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF	ANO
Minimální počet záznamů v tabulce MAC adres	32 000
Min. počet IPv4 unicast směrovacích záznamů	2 000
Min. počet konfigurovatelných security ACL	5 000
Počet LACP skupin/linek ve skupině	32/8
Podpora VLAN podle IEEE 802.1Q, počet aktivních VLAN	2 000
Private VLAN	ANO
Tunelování 802.1Q v 802.1Q	ANO
IEEE 802.1x	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)	ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO
802.1x autentizace přepínače vůči nadřazenému přepínači	ANO

Podpora RADIUS CoA	ANO
Podpora Radius over TLS (RadSec)	ANO
Podpora instance spanning-tree protokolu per VLAN – alespoň 128 instancí	ANO
IEEE 802.1w – Rapid Spanning Tree Protocol	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO
Podpora "jumbo rámců" včetně velikosti 9198 Byte	ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO
Podpora L3 routed port	ANO
OSPFv2 a OSPFv3	ANO
Podpora service insertion včetně technologie VXLAN	ANO
Multicast: PIM-DM, PIM-SM, IPv6 PIM-SM, PIM-SSM, IPv6 PIM-SSM	ANO
Podpora logických virtuálních směrovacích instancí (VRF) v rámci téhož L3 přepínače	ANO
First Hop Redundancy Protokol (např. VRRP nebo HSRP)	ANO
IGMPv2, IGMPv3	ANO
IGMP snooping a MLD snooping	ANO
DHCP server a relay pro IPv4 a IPv6	ANO
Minimální počet HW QoS front	8
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	ANO
IPv6 services (Telnet, SSH, Syslog, DHCP)	ANO
IPv6 QoS	ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO
IPv6 Port ACL, VLAN ACL	ANO
Možnost definovat povolené MAC adresy na portu	ANO
Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU	ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO
Podpora TPM nebo HW trusted modulu	ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO
Monitorování aplikačních toků prostřednictvím technologie NetFlow nebo sFlow	ANO
Podpora NTPv3	ANO

Konfigurace zařízení v člověku čitelné textové formě	ANO
SSHv2 a HTTPS pro IPv4 a IPv6	ANO
Podpora SNMPv2c a SNMPv3	ANO
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO
Port mirroring, alespoň 4 různé obousměrné session	SPAN, ERSPAN
API rozhraní pro konfiguraci pomocí NETCONF nebo RESTCONF za použití YANG/JSON data modelů.	ANO
Python scripting – lokální interpret jazyka v přepínači	ANO
Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů	ANO
Ochrana proti nahrání modifikovaného SW do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu OS zařízení prostřednictvím TPM čipu	ANO
Doživotní záruka výrobce, tzn. min. 5 let od ukončení prodeje, včetně vestavěných zdrojů a ventilátorů a nároku na běžně dostupné nové verze SW.	ANO

8 Přepínač typ 3

Požadavek na funkcionalitu	**Minimální požadavky**
Typ přepínače	L3 switch
Montáž do racku, velikost max. 1U	ANO
Podpora virtualizace – možnost sloučit alespoň dva fyzické přepínače do jednoho logického celku – virtuálního switche	ANO
Minimální počet 10Gbps SFP+ portů s volitelným fyzickým rozhraním	24
Minimální počet 40/100Gbps nebo 25/50Gbps portů s volitelným fyzickým rozhraním	4
Interní hot-swap AC napájecí zdroj	2x
Vyměnitelné ventilátory – hot swap	ANO
Minimální propustnost přepínače	880 Gbps
Minimální paketový výkon přepínače	650 Mpps
Min. počet IPv4 unicast směrovacích záznamů	60 000
Min. počet IPv6 unicast směrovacích záznamů	60 000
Minimální počet záznamů v tabulce MAC adres	32 000
Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG)	ANO
IEEE 802.3ad přes více šasi (funkční ekvivalent Multichassis Etherchannel)	ANO

Podpora "jumbo rámců" včetně velikosti 9198 Byte	ANO
IEEE 802.1D	ANO
Minimální počet aktivních VLAN podle IEEE 802.1Q	4 000
Tunelování 802.1Q v 802.1Q	ANO
IEEE 802.1x	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)	ANO
802.1x autentizace přepínače vůči nadřazenému přepínači	ANO
Podpora RADIUS CoA	ANO
Podpora Radius over TLS (RadSec)	ANO
IEEE 802.1s – Multiple Spanning Trees	ANO
IEEE 802.1w – Rapid Spanning Tree Protocol	ANO
IEEE 802.1p	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO
Detekce jednosměrnosti optické linky: UDLD nebo DLDP	ANO
STP root guard a STP loop guard nebo ekvivalentní	ANO
Možnost autorecovery po chybovém stavu (root guard, loop guard)	ANO
Multicast/broadcast storm control – hardwarové omezení poměru unicast/multicast rámců na portu	ANO
Router Redundancy protokol pro IPv4 a IPv6 (např. VRRP nebo HSRP)	ANO
DHCP server a relay pro IPv4 a IPv6 včetně podpory VRF	ANO
IP alias (více IP sítí na jednom rozhraní)	ANO
IPv6 ACL a IPv6 QoS	ANO
IPv6 services (DNS, Telnet, SSH, Syslog, ICMP, DHCP)	ANO
IPv6 Multicast (MLDv1 & v2)	ANO
IPv6 MLDv2 snooping	ANO
HTTP, SNMP přes IPv6	ANO
RADIUS, TACACS+ pomocí IPv4 a IPv6	ANO
Dynamické směrování: RIPv2, OSPFv2, BGPv4, OSPFv3 a MP BGP	ANO
Podpora service insertion včetně technologie VXLAN	ANO
Policy-based routing podle ACL	ANO
Podpora minimálně 256 logických virtuálních směrovacích instancí (VRF)	ANO

Protokoly a služby ve VRF (RADIUS, TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)	ANO
Multicast: PIM-DM, PIM-SM, IPv6 PIM-SM, PIM-SSM, IPv6 PIM-SSM, MSDP	ANO
IGMPv2, IGMPv3	ANO
IGMPv3 snooping	ANO
ACL na rozhraní IN/OUT (včetně virtuálních – VLAN, 802.3ad)	ANO
ACL pro IP	ANO
ACL pro ethernetové rámce	ANO
Možnost definovat povolené MAC adresy na portu	ANO
Možnost definovat maximální počet MAC adres na portu	ANO
Zabezpečení a analýza DHCP protokolu (např. DHCP snoopingu nebo funkčně ekvivalentní)	ANO
Podpora ochrany podvrženého mapování IP/MAC adresy (např. IP Source Guard/IPSG nebo funkčně ekvivalentní)	ANO
Ochrana centrálního procesoru (control plane) před útoky typu DoS	ANO
CLI rozhraní	ANO
Python scripting – lokální interpret jazyka v přepínači	ANO
Linux shell	ANO
Konfigurace zařízení v člověku čitelné textové formě	ANO
SSHv2	ANO
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ANO
SNMPv2 a SNMPv3	ANO
Podpora synchronizace času protokolem NTPv3 (klient i server)	ANO
Monitorování aplikačních toků prostřednictvím technologie NetFlow nebo IPFIX	ANO
Interní uložiště dat: min. 30 GB	ANO
AAA ověřování uživatelů (autentizace, autorizace, accounting) - TACACS+, RADIUS	ANO
Zrcadlení portů (např. SPAN nebo ekvivalentní)	ANO
Vzdálený port mirroring (ERSPAN)	ANO
Syslog – minimálně 3 servery	ANO
Uživatelsky modifikovatelné automatické reakce/obsluhy událostí při provozu přepínače (např. pomocí EEM skriptů nebo ekvivalentní)	ANO
Nástroje měření odezev sítě (např. IP SLA nebo ekvivalentní)	ANO
Možnost automatické nebo manuální zálohy konfigurace z externího zdroje	ANO
DHCP server	ANO

Ochrana proti nahrání modifikovaného SW do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu OS zařízení prostřednictvím TPM čipu	ANO
Doživotní záruka výrobce, tzn. min. 5 let od ukončení prodeje, včetně vestavěných zdrojů a ventilátorů a nároku na běžně dostupné nové verze SW.	ANO

9 Kontrolér bezdrátové sítě - dva typy

Požadavek na funkcionalitu - typ 1	**Minimální požadavky**
On-premise appliance, nepřipouští se cloud řešení	ANO
Specializovaná hardware appliance – nepřipouští se virtualizovaný kontrolér	ANO
Hardware i software podporovaný jedním výrobcem	ANO
Minimální propustnost dodaného zařízení pro data	20 Gbps
Minimální počet 10Gb SFP+ portů s volitelným fyzickým rozhraním	4x
Počet podporovaných AP bez nutnosti přidávání hardware	500
Možnost licenčního rozšíření až na 2000 AP v rámci jedné appliance kontroléru	2 000
Počet současně připojených wifi klientů	16 000
Možnost licenčního rozšíření až na 32 000 současně připojených klientů	32 000
Požadavek na funkcionalitu – typ 2	**Minimální požadavky**
On-premise appliance, nepřipouští se cloud řešení	ANO
Specializovaná hardware nebo virtuální appliance – v případě virtuální appliance je součástí dodávky 1U rack server s výkonnostními parametry doporučenými výrobcem	ANO
Podporované hypervisory: VMware ESX, Hyper-V, KVM	ANO
Hardware i software podporovaný jedním výrobcem	ANO
Minimální propustnost dodaného zařízení pro data	6 Gbps
Minimální počet 10Gb SFP+ portů s volitelným fyzickým rozhraním	2x
Minimální počet 1Gb RJ45 portů	2x
Počet podporovaných AP bez nutnosti přidávání hardware	250
Možnost licenčního rozšíření až na 500 AP v rámci jedné appliance kontroléru	ANO
Počet současně připojených wifi klientů	4000
Možnost licenčního rozšíření až na 6000 současně připojených klientů	ANO
Požadavek na funkcionalitu – společné parametry	**Minimální požadavky**
Podpora redundance na úrovni kontrolérů a jejich portů	ANO
Lokální síť – možnost tunelování uživatelských dat z AP až na kontrolér, možnost šifrování těchto uživatelských dat bez výrazného vlivu na propustnost	ANO

Mesh síť – podpora mesh sítí, současné připojení normálních a mesh AP k jednomu kontroléru	ANO
Vzdálené lokality – možnost lokálního bridgování uživatelských dat per SSID přímo na příslušném AP	ANO
Šifrovaná řídící komunikace AP-kontrolér	ANO
Podpora 802.11i, respektive jeho implementace WPA2 včetně enterprise variant autentizace/šifrování	ANO
Podpora WPA3 – WPA3 Enterprise, WPA3 SAE, WPA3 OWE	ANO
PSK autentizace vč. možnosti různých PSK klíčů pro různé klienty v rámci jednoho SSID	ANO
Podpora standardu „802.11w“ pro ochranu řídících rámců na AP a klientovi	ANO
Podpora standardu „802.11u“ pro výběr SSID a autentizaci klienta	ANO
Integrované řešení návštěvnického přístupu s možností webové autentizace (včetně nativních IPv6 klientů), bezpečné oddělení od zaměstnaneckého provozu	ANO
Podpora řešení návštěvnického přístupu pro klienty bezdrátové i drátové sítě	ANO
Možnost omezit počet klientů per SSID	ANO
Lokální profilování zařízení – per uživatel a per zařízení	ANO
Integrovaný IDS systém pro detekci cizích AP (Rogue AP) a klientů v AdHoc režimu, možnost vynuceného odpojení klientů od cizích AP	ANO
Podpora Flexible NetFlow a exportu záznamů (dle RFC 3954) nebo IPFIX o datových tocích uživatelů (vč. zdrojové a cílové IP adresy, portů, WLAN ID, počtu paketů a objemu přenesených dat) směrem k externímu kolektoru	ANO
Podpora standardu „802.11r“ pro rychlý roaming klientů mezi AP	ANO
Podpora standardu „802.11k“ pro optimalizaci roamingu	ANO
Podpora standardu „802.11v“ pro optimalizaci připojení klienta	ANO
Podpora 802.11e/WMM	ANO
Diferenciace úrovní QoS pro různé služby a skupiny uživatelů (zaměstnance a návštěvníky), možnost obousměrného omezení propustnosti per klient.	ANO
Mechanismy řízení přístupu (Call Admission Control) pro hlasový i video provoz. Konfigurovatelné parametry max. zátěže a šířky pásma.	ANO
Podpora Video-streamingu se spolehlivým multicastem	ANO
Optimalizace multicast provozu v bezdrátové síti (IGMP snooping)	ANO
Aplikační inspekce přenášeného provozu (DPI na 7. vrstvě ISO/OSI na základě aplikačních signatur) umožňující rozpoznání jednotlivých aplikací, grafické zobrazení statistik a možnost řízení QoS per rozpoznaná aplikace	ANO
Automatizovaná centrální správa frekvenčního pásma	ANO

Monitoring rádiového spektra vč. 20/40/80 MHz kanálů, možnost okamžité automatické centralizovaně řízené reakce (změna kanálu nebo jeho šířky, změna vysílacího výkonu), grafické vyobrazení informací o kvalitě signálu	ANO
Automatické zvýšení vysílacího výkonu okolních AP při výpadku AP („self healing“)	ANO
Možnost detekce rušivých signálů (interference) a identifikace zdrojů interference na základě signatur	ANO
Mesh síť – automatický výběr vhodného kanálu pro backhaul, automatické sestavení optimálního mesh stromu, monitorování všech kanálů na pozadí s rychlou konvergencí v případě výpadku primárního nadřazeného AP	ANO
Troubleshooting radiového signálu a automatické řešení problému rušivého signálu	ANO
Možnost definovat různé konfigurační profily a ty následně přiřadit vybraným AP (např. dle umístění AP, bezpečnostních pravidel atd.).	ANO
Možnost vytvořit různé rádiové profily (nastavení kanálů, rychlostí) a ty následně přiřadit vybraným AP.	ANO
Podpora IPv6 – management kontroléru (vč. Syslog, radius)	ANO
Podpora IPv6 – komunikace AP-kontrolér	ANO
Podpora IPv6 – Guest Access i pro nativní klienty vč. webové autentizace pro IPv6 klienty	ANO
Podpora IPv6 – IPv6 multicast, MLD snooping	ANO
Podpora IPv6 – bezpečnost (RA Guard, ACL)	ANO
Podpora IPv6 – ND cache na kontroléru, optimalizace přenosu ND zpráv	ANO
Centrální administrace správců s granularitou přístupových práv	ANO
Podpora správy přes serial CLI nebo přes IP pomocí SSH/telnet a https web GUI, SNMP	ANO
Podpora API rozhraní pro plnou konfiguraci kontroléru pomocí NETCONF nebo RESTCONF za použití YANG/JSON data modelů. Podpora exportu provozních dat z kontroléru.	ANO
Možnosti využití API pro automatizovanou správu	ANO
Podpora lokalizačních dat připojených klientů pomocí RTLS	ANO
SNMPv2c, SNMPv3	ANO
Plná kompatibilita s nabízenými přístupovými body	ANO
Záruka a podpora výrobce včetně nároku na verze SW na 5 let	ANO

10 Bezdrátový přístupový bod (AP)

Požadavek na funkcionalitu	**Minimální požadavky**
Třída zařízení: indoor přístupový bod (AP)	ANO
Integrované antény pro obě pásma 2.4 a 5Ghz	ANO
Uzavřená konstrukce bez ventilátorů	ANO

Podpora bezdrátových standardů	802.11a/b/g/n, 802.11ac wave2, 802.11ax
Plnohodnotná certifikace Wi-Fi Aliance	IEEE 802.11a/b/g/n/ac
Plnohodnotná certifikace Wi-Fi Aliance	WPA3-CNSA, WPA3-SAE, WPA3-OWE
Pracovní režim AP řízené kontrolérem (lightweight)	ANO
Minimální počet portů ethernet LAN	1x 100/1000/2500Mbit/s RJ45
Podpora muligigabit ethernet 2.5 Gbps IEEE 802.3bz	ANO
Možnost 802.3af/at PoE napájení z přepínače nebo injectoru – plná funkce při použití 802.3at, v případě 802.3af běží přístupový bod minimálně v režimu 1x1 MIMO pro obě rádiová pásma bez sníženého vysílacího výkonu	ANO
Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz	ANO
MIMO a počet nezávislých streamů na 2,4GHz rádio:	2x2:2
MIMO a počet nezávislých streamů na 5GHz rádio:	4x4:4
Podpora šířky kanálu 160 MHz	ANO
Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP	ANO
Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11 n/ac/ax klientům (Tx Beam Forming)	ANO
Podpora mechanismu pro přepojení klientů z 2,4GHz do 5GHz pásma	ANO
AP obsahuje X.509 certifikát s lokální platností pro nasazeni PKI	ANO
Podpora autentizace AP do LAN sítě pomocí 802.1x, AP obsahují 802.1x supplikant	ANO
Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark)	ANO
Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 pomocí Telnet nebo SSH	ANO
AP obsahuje Integrované Bluetooth 5.0 Low Energy (BLE) rádio a integrované Zigbee 802.15.4 rádio	ANO
USB port 2.0 - možnost napájení pro vložené zařízení alespoň 4W	ANO
Minimální počet inzerovaných SSID (BSSID) na radio	8
SNMPv2/v3	ANO
Současná funkčnost AP pro přenos dat, analýzu spektra a detekci bezpečnostních incidentů	ANO
HW i SW podpora FTM – 802.11mc	ANO
Rozsah provozních teplot 0° až +50°C bez nutnosti redukce výkonu nebo omezení funkcí	ANO
Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanizmy pro ochranu SW a HW proti útokům	ANO

Součástí AP je příslušenství pro montáž na zeď nebo strop	ANO
AP je fyzicky zabezpečitelné/uzamknutelné k okolním pevným částem pomocí Kensington lock	ANO
Doživotní záruka výrobce, tzn. min. 5 let od ukončení prodeje.	ANO

11 Požadované implementační služby

11.1 Základní instalační služby

V rámci dodávky předmětu plnění kupující požaduje následující systémové práce:

- Instalace a konfigurace SW appliance
- Konfigurace autentizačních politik 802.1x a MAC auth
- Vazba autentizačních platforem na Active Directory
- Integrace se stávajícími firewally nemocnic FortiGate, jedná se o stávající technologii provozovanou nemocnicemi
- Profilování zařízení
- Demontáž stávajících switchů v pozicích při osazování prvků nových
- Montáž prvků do racku, propojení, sestohování, montáž prvku musí být provedena tak, aby po jeho uvedení do provozu nebyl narušen provoz a dostupnost aplikačních služeb, které jsou poskytovány stávající technologií a její konfigurací; součinnost pro instalaci jednotlivých prvků musí být předem odsouhlasena
- Montáž bezdrátových přístupových bodů, kdy připravenost na úrovni UTP kabelu v místě umístění bezdrátového přístupového bodu zajistí kupující
- Aktualizace firmware, nastavení lokálních účtů apod.
- Základní konfigurace zařízení na úrovni min. IP adresy, NTP, SNMP, logování
- L3 konfigurace, migrace stávajících politik, ACL
- L2 konfigurace, přiřazení VLAN, STP, LACP
- Konfigurace SSID, bezpečnostní politiky, mapování VLAN, autentizace
- Konfigurace QoS
- Integrace do stávajících dohledových systémů (min. HP iMC a Zabbix)
- Otestování, testy redundance
- Zaškolení administrátorů

Realizací předmětu plnění dle této specifikace kupující sleduje potřebu implementace opatření v oblasti kybernetické bezpečnosti z projektu IROP, z nějž plánuje toto plnění kofinancovat. Z tohoto důvodu v rámci plnění musí být výslovně zajištěno následující

- kontrola uživatelů a jejich zařízení přistupujících k síťovým zdrojům
- „viditelnost“ koncových zařízení v síti
- zamezení napadení sítě zevnitř neznámým útočníkem
- implementaci protokolu 802.1X (LocalDB, MS AD)
- MAC autentizaci a profilaci zařízení (LAN, WLAN)

- bezpečný přístup pro hosty
- automatizace nasazení bezpečnostních politik znamená snížení operativy
- reportování anomálií a pokusů o vniknutí do sítě
- integrace s řešením NGFW znamená zamezení šíření napadení systému, či jejímu omezení
- notifikace uživatele o případném bezpečnostním incidentu

11.2 Sjednocení konfigurace sítě, politik a VLAN

V rámci realizace plnění kupující požaduje **zpracování analýzy VLAN a síťových politik** v nemocnici, jejich zdokumentování a sestavení nového návrhu, který bude nasazen společně s novými prvky v rámci plnění této technické specifikace.

Analýza VLAN a síťových politik bude provedena nejen na úrovni nemocnice, ale bude zohledňovat požadavky na strukturu a způsob fungování síťového prostředí Zdravotnického holdingu Královéhradeckého kraje a.s., který je zakladatelem nemocnice. To znamená, že prodávající provede analýzu ve všech nemocnicích, do kterých v rámci plnění této technické specifikace na základě samostatných smluv bude dodávat technologie, tuto analýzu písemně sestaví, určí v ní průsečíky a dobrou praxi v jednotlivých nemocnicích a provede vyhodnocení stávajícího stavu.

Na základě takového vyhodnocení, provede prodávající **návrh sjednocení VLAN a síťových politik napříč nemocnicemi Zdravotnického holdingu Královéhradeckého kraje a.s.**, a takový návrh v podobě rozdělení na jednotlivé nemocnice a dopady do jejich konfigurací a síťových služeb předloží k projednání kupujícímu.

Při návrhu musí maximálně prodávající respektovat potřeby nemocnice a dále zohlednit skutečnosti, na kterých se takové potřeby zakládají, tedy zejména návaznost provozovaných informačních systémů a technologií na stávající konfiguraci a s tím související potřeby nemocnic, provést případný přechod na nové konfigurace postupně, či navrhnout i přechodná a náhradní řešení.

Součástí návrhu musí být i následující:

- požadavky na rekonfiguraci stávajících prvků nemocnice mimo plnění této technické specifikace
- přesný instalační plán, včetně závazného **harmonogramu realizace plnění**

Termín - Zpracování analýzy a návrhu VLAN a síťových politik provede prodávající nejpozději do 4 týdnů od nabytí účinnosti této smlouvy.

Kupující prodávajícímu sdělí své připomínky k výstupu analýzy do 2 týdnů.

Prodávající se zavazuje všechny připomínky kupujícího zohlednit a finalizovat návrh sjednocení VLAN a síťových politik do jednoho týdne.

Zahájení implementačních a instalačních prací bude předcházet odsouhlasení výstupů analýzy a návrhu realizačních prací ze strany kupujícího (nemocnice). Bez výslovného souhlasu kupujícího nebude možné

zahájit uvedené práce a jejich zahájení v rozporu s tímto ustanovením ze strany prodávajícího bude považováno za podstatné porušení smlouvy.

Výsledný dokument analýzy VLAN a síťových politik, včetně návrhu a instalačního plánu (harmonogramu) bude po zapracování připomínek kupujícího ze strany prodávajícího protokolárně předán kupujícímu a bude závazný.

Po realizaci instalační služeb prodávající aktualizuje dokument návrhu sjednocení VLAN a síťových politik podle skutečného provedení a dále **jej doplní o architektonickou vizualizaci výsledné sítě**, včetně popisu jednotlivých prvků, jejich určení a adres a výsledný dokument předá kupujícímu.

11.3 Časový rámec pro realizaci instalačních služeb

S ohledem na skutečnost, že nemocnice nemohou přerušit svůj provoz, a dále na skutečnost, že v prostředí nemocnic je potřeba zachovávat zvýšenou míru čistoty a klidu, mohou fyzické instalační práce probíhat v pracovních dnech pouze v časech 15:00 až 05:00 hodin a o víkendech v časech 12:00 až 05:00 hodin, nebude-li v konkrétních případech dohodnuto jinak.

Konfigurační služby a služby realizované formou vzdáleného přístupu mohou být realizovány i mimo výše uvedenou dobu, za předpokladu, že budou založeny na schváleném harmonogramu.

Přípravné práce, které nebudou zasahovat do aktivního propojení sítě bude možné ze strany prodávajícího realizovat i mimo tyto časy na základě dohody s kupujícím.

S ohledem na povahu organizace kupujícího musí prodávající při realizaci konfiguračních pracích vzít v úvahu potřebu řádného provozu informačních systémů závislých na síťových službách, které budou v rámci realizace tohoto plnění rekonfigurovány a v návrhu harmonogramu a při realizaci prací toto musí prodávající zohlednit.

Tedy zejména svojí činností nepůsobil překážky v dostupnosti služeb prostřednictvím sítě i v jiných časech, než kdy budou dle harmonogramu odsouhlaseny práce na síťové infrastruktuře, které mohou vést k nedostupnosti prostřednictvím sítě poskytovaných služeb, které jsou součástí poskytování zdravotních služeb.

11.4 Zkušební provoz

V rámci realizovaného plnění je požadován zkušební provoz nově nasazených technologií jako celku.

Zkušební provoz je součástí plnění dle této technické specifikace a je i součástí plnění tak, že je potřeba jej zohlednit do harmonogramu prací ze strany prodávajícího.

Požadovaná délka zkušebního provozu jsou dva kalendářní měsíce.

Předmětem zkušebního provozu je ověření provedených dodávek a služeb, tedy zejména funkčnosti dodaných zařízení a správnosti provedené konfigurace.

Zahájení zkušebního provozu proto musí předcházet nasazení všech technologií a provedení všech souvisejících dodávek a služeb (zejména konfigurací).

Zahájení zkušebního provozu podléhá předložení potvrzení o instalaci a konfiguraci technologií ze strany prodávajícího a potvrzení možnosti zahájení zkušebního provozu ze strany kupujícího.

Délka zkušebního provozu je nastavena v takové délce, aby umožnila kupujícímu ověřit správnost provedené konfigurace a dále schopnosti dodaných zařízení plnit požadavky na ně stanovené. Délka zkušebního provozu byla stanovena tak, aby kupujícímu umožnila ověřit většinu procesů a situací v rámci uvažovaného užití předmětu plnění. Jedná se zejména o nepravidelné činnosti v prostředí nemocnice a dále o pravidelné činnosti nicméně s časovým horizontem, které mají zvýšené nároky na síťové prostředí a jeho konfiguraci, tedy předmět plnění dle této technické specifikace. Jedná se o komplexní zálohovací procesy, interní migrace dat a další typické činnosti v zařízení typu nemocnice a jejího IT prostředí.

11.5 Kybernetická bezpečnost

Předmět plnění dle této technické specifikace vstupuje do informačního prostředí jednotlivých nemocnic, které podléhá na rozličné úrovni dopadům následujících právních předpisů:

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
- Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)

Prodávající musí jednat řádně a v kontextu výše uvedených právních předpisů v oblasti kybernetické bezpečnosti a v případě potřeby si v rámci realizace plnění vyžádat od kupujícího doplňující informace tak, aby byl připraven reflektovat své jednání a proces realizace plnění v souladu s výše uvedenými předpisy a jejich případnou formou implementace v jednotlivých nemocnicích.

Mezi nemocnicemi je provozovatelem informačního systému základní služby Oblastní nemocnice Náchod a.s.

V rámci realizovaného plnění a dopadu výše uvedené legislativy bude prodávající zařazen mezi tzv. významné dodavatele.

Pro všechny nemocnice je však ze strany prodávajícího nezbytné dodržet výše uvedenou národní legislativu a dále v kontextu realizovaného plnění zohlednit směrnici NIS 2, jako závazný právní předpis EU určený k implementaci jednotlivými státy EU v rozsahu, který umožňuje přímou interpretaci a vztahuje se k realizovanému plnění.

11.6 Projektové řízení

S ohledem na rozsah projektu a dopad jeho zavedení do produkčního provozu na výkon činnosti kupujícího je v rámci dodávky předmětu plnění kupujícím požadováno aplikování základních principů projektového řízení ze strany prodávajícího.

Jedná se zejména řízení projektových prací v souladu s uzavřenou smlouvu s ohledem na věcné plnění dané smlouvou – rozsah, posloupnost a hloubku projektových prací, (tj. harmonogramu) – řízení postupu prací s ohledem na závazný harmonogram projektu – dodržování termínů harmonogramu, podchycení případných kolizí, zpoždění nebo vznikajících rizik a jejich reportování směrem ke kupujícímu, aktivní řešení výše uvedených nestandardních situací

Zápisy - Zpracování pravdivých, úplných a věcně jasných a vypovídajících zápisů z konzultačních schůzek a pracovních jednání (s cílem zaznamenání klíčových rozhodnutí, ujednání, navržených nebo dohodnutých termínů a způsobů řešení dílčích částí projektu atd.)

Kontrolní dny - Prezenční účast odpovědné osoby prodávajícího na kontrolních dnech v pravidelných min. měsíčních intervalech v sídle kupujícího, případně se souhlasem obou smluvních stran formou videokonference nebo telekonference. Termíny kontrolních dnů budou součástí harmonogramu.

U kontrolních dnů kupující požaduje, aby byly organizovány společně pro všechny nemocnice Zdravotnického holdingu Královéhradeckého kraje, a.s., ve kterých dochází k realizaci plnění prodávajícím dle této technické specifikace.

Reporting - Reporting plnění na úrovni pravidelných dvoutýdenních písemných zpráv směrem k odpovědné osobě kupujícího (seznam prací, které byly vykonány pro danou část projektu, stav těchto prací (ukončeno, odloženo, v realizaci); popis vzniklých problémů a způsob jejich řešení. Kupující si vyhrazuje právo vyžádat reporting projektu i mimo dvoutýdenní interval, na takovou žádost bude prodávající povinen reagovat vždy nejpozději písemnou zprávou do 4 pracovních dnů.

Řízení rizik plnění, hodnocení pravděpodobnosti jejich výskytu a míry dopadu, návrh řešení k jejich eliminaci.

Řízení změn na plnění, v případě požadavků na změnu v plnění provedení konzultací k ověření nutnosti změny plnění; zjištění dopadu požadovaných změn směrem ke koncepci celkového řešení, harmonogramu, dotačnímu titulu, vytížení lidských zdrojů atd. V případě odsouhlasení změn spolupráce při implementaci změn do plnění, komunikace s dalšími zapojenými osobami a specialisty za dotčené technologie a informační systémy.