

Dodatek č. 1
ke smlouvě o výpůjčce uzavřené dne 31. 10. 2023

Smluvní strany

Fakultní nemocnice Brno

Jihlavská 20

625 00 Brno

IČO: 65269705

DIČ: CZ65269705

Bankovní spojení: Česká národní banka, a.s. č.ú.: [REDACTED]

zastoupená: [REDACTED], ředitelem

FN Brno je státní příspěvková organizace, zřízená rozhodnutím Ministerstva zdravotnictví.

Nemá zákonnou povinnost zápisu do obchodního rejstříku, je zapsána do živnostenského rejstříku vedeného Živnostenským úřadem města Brna.

(dále jen vypůjčitel)

a

Kardio-Line spol. s r. o.

IČ: 46994769

DIČ: CZ46994769

se sídlem: Antonínská 5, Brno 602 00

zastoupena: [REDACTED], jednatel

bankovní spojení: KB Brno,

číslo účtu: [REDACTED]

zapsána v obchodním rejstříku vedeném Krajským soudem v Brně, oddíl C, vložka 8851

(dále jen půjčitel)

uzavírají níže uvedeného dne, měsíce a roku následující dodatek ke smlouvě o výpůjčce na bezplatné užívání přístroje pro spánkovou terapii Loewenstein Prisma LAB, klasifikační třída IIa na Všeobecné interní klinice:

I.

Smluvní strany se dohodly na následující změně:

Předmět výpůjčky bude nově připojován do datových sítí Vypůjčitele, proto se mění Příloha č. 1 a nově se doplňují Přílohy č. 2 a 3. Přílohy 1, 2 a 3 tvoří Přílohu tohoto dodatku.

II.

V ostatním zůstává smlouva nezměněna.

Dodatek nabývá platnosti dnem podpisu obou smluvních stran a účinnosti dnem jeho uveřejnění v registru smluv dle zákona č. 340/2015 Sb., zákon o registru smluv, ve znění pozdějších předpisů.

Vyhotovuje se ve dvou stejnopisech, po jednom pro každou smluvní stranu.

V Brně dne

Fakultní nemocnice Brno

Kardio-Line spol. s r. o.

PŘÍLOHA Č. 1

Specifikace Předmětu výpůjčky, případně Montáže

Přístroj pro spánkovou terapii/titraci Loewenstein, prismaLAB (vč. zvlhčovače, zdroje, patientského okruhu pro dospělé, 2 ks prachového filtru a brašny).

PŘÍLOHA Č. 2

Požadavky z oblasti informačních a komunikačních technologií na plnění smlouvy

Zboží a jeho příslušenství včetně veškerého software, který je součástí předmětu plnění (dále souhrnně jen „**Zařízení**“) musí splňovat následující požadavky zadavatele.

Je-li tato příloha připojena ke smlouvě o výpůjčce, pak kde je v této příloze uveden „Prodávající“, rozumí se tím Půjčitel, a kde je v této příloze uveden „Kupující“, rozumí se tím Vypůjčitel.

Blokové komunikační schéma:

Schéma komunikace PrismaLab a PC

Umístění technologie:

Brno-Bohunice 787
Spánkové centrum
Pokoje č. 1,2,3
Sesterna

Pokoj č.1: 1/3

PrismaLab
MAC: 48:91:53:00:23:af

Pokoj č.2: 1/9

PrismaLab
MAC: 48:91:53:00:27:9e

Pokoj č.3: 1/15

PrismaLab
MAC: 48:91:53:00:27:8b

SQL server

Aplikační
server

ROUTER

SWITCH

Služba prismaServer - port 2782

PC (PSG2)

PC (PSG3)

PC (PSG4)

PC (PSG5)

Kontaktní údaje správce technologie:



Od výrobce je doporučeno přiřadit IP adresy
DHCP serverem

Pokud manuálně – musí se přístroje
PrismaLab nacházet ve stejné síti a podsíti
jako PC



Obousměrná komunikace PrismaLab s PC

Vyhledávání přístrojů přes port UDP 51337,
odpověď UDP 51338

Vlastní komunikace probíhá přes TCP 51337

Zdrojová adresa	Cílová adresa	Transportní protokol	Zdrojový port	Cílový port	Aplikační protokol
PrismaLab	PC	TCP/UDP		51337/51338	
PC	PrismaLab	TCP/UDP		51337/51338	
PrismaLab	Aplik. server	TCP		2782	WCF
PC	Aplik. server	TCP		2782	WCF
Aplik. server	SQL server	TCP		1433	Db engine
Aplik. server	SQL server	TCP/UDP		1434	Db browser
Aplik. server	SQL server	TCP		80	SSRS via http
Aplik. server	SQL server	TCP		443	SSRS via https
Aplik. server	SQL server	TCP		2383	SSAS
Aplik. server	SQL server	TCP		2382	Redirector SSAS
Aplik. server	SQL server	TCP		135	Management tools
Aplik. server	SQL server	TCP		4022	SQL Service Broker

Toto blokové komunikační schéma zpracované na základě přílohy č. 3 dále jen „**blokové komunikační schéma**“.

Další práva a povinnosti smluvních stran týkající se oblasti informačních a komunikačních technologií:

Prodávající je povinen plnit veškeré povinnosti vyplývající z této přílohy, která je nedílnou součástí smlouvy. Pokud z povahy povinností uvedených v této příloze smlouvy vyplývá, že je Proávající povinen je plnit opakovaně či průběžně, je Proávající povinen tak činit po celou záruční dobu, jak je v této smlouvě sjednána. Pokud jsou smluvní strany v této smlouvě označeny jinak než Kupující a Proávající, použijí se dále uvedená ujednání dle významu použitého označení smluvních stran.

Není-li v této smlouvě sjednáno jinak, je Proávající povinen svolat v součinnosti s Kupujícím technickou schůzku se zástupci Kupujícího, a to na pracovišti Kupujícího a tak, aby se tato technická schůzka konala do 14 dnů od nabytí účinnosti smlouvy. Kupující je na této technické schůzce oprávněn Proávajícímu udělovat pokyny pro plnění smlouvy a technické podmínky zapojení, provozování a umístění Zařízení, případně implementace, integrace a konfigurace software, pokud je součástí Zařízení, a to v rozsahu neuvedeném v této smlouvě a v příslušné zadávací dokumentaci. Tyto pokyny a podmínky jsou pro Proávajícího závazné.

Kupující je oprávněn za účelem provádění kybernetických bezpečnostních opatření omezovat připojení Zařízení do datové sítě Kupujícího, a to v rozsahu, ve kterém to není pro provoz Zařízení nezbytné a ve kterém to není v rozporu se zadávací dokumentací. Proávající je povinen při plnění této smlouvy dodržet podmínky vyplývající z blokového komunikačního schéma.

Pokud Zboží nebude využívat antivirové ochrany Kupujícího (Microsoft Defender), je Proávající povinen za účelem zajištění kybernetické a informační bezpečnosti Zboží zajišťovat aktuálnost antivirové ochrany Zboží. Proávající je povinen za tímto účelem zajišťovat aktualizaci antivirové ochrany Zboží, přičemž Kupující negarantuje průchod jiných antivirových systémů na jejich aktualizací servery a neumožnění tohoto průchodu nelze považovat za nedostatek součinnosti Kupujícího. O provedených aktualizacích antivirové ochrany je Proávající povinen vést písemný provozní deník uložený u Kupujícího, ve kterém bude ve lhůtě bez zbytečného odkladu zaznamenávat informace o vydaných aktualizacích antivirové ochrany, o provedených aktualizacích antivirové ochrany (tj. implementovaných do Zboží) včetně informace, kdy byla aktualizace antivirové ochrany Zboží provedena. Do tohoto provozního deníku je Proávající povinen dále ve lhůtě bez zbytečného odkladu uvádět, kdo aktualizaci antivirové ochrany provedl, jestliže byla provedena jinak, než automaticky dálkovým přístupem Zboží na server výrobce antivirové ochrany. Tento provozní deník může být veden elektronicky, jestliže trvale přístupný Kupujícímu a bude splňovat podmínky presumpce spolehlivosti stanovené § 562 odst. 2 občanského zákoníku.

Jestliže je součástí předmětu smlouvy dodávka počítačů nebo poskytnutí software, které nejsou registrovány současně se Zařízením jakožto zdravotnický prostředek dle zákona č. 89/2021 Sb., a tento software je určen pro operační systém Microsoft Windows, musí takové počítače a takový software splňovat následující požadavky Kupujícího:

- Instalaci operačního systému (dále též jen „OS“) a software (dále též jen „SW“) provede Kupující. Kupující zavede OS do domény fnbrno.cz, tj. Zařízení musí umožňovat toto zavedení.
- Instalace serverové i klientské části SW je povolena pouze do %ProgramFiles% a %ProgramFiles(x86)%. Klientská část SW bude uživatelům poskytována přes DFS ze síťového úložiště, nebo bude virtualizována technologií VMware ThinApp.

- Zařízení ani SW nesmí vytvářet složky a soubory v kořenovém adresáři systémového oddílu.
- SW nesmí pro svůj provoz vyžadovat jiná oprávnění k OS, než která má v defaultním nastavení nastavena skupina Users.
- Zařízení ani SW nesmí jakýmkoliv způsobem manipulovat s oprávněním jednotlivých položek registru OS.
- Veškeré požadované (dokumentované) funkcionality SW musí pracovat s aktivovaným a standardně nastaveným firewallem v OS Windows.
- Na počítači musí být možné instalovat a používat antivirový systém zadavatele (Microsoft Defender).
- Veškeré požadované (dokumentované) funkcionality SW musí pracovat s aktivovaným řízením uživatelských účtů (User Account Control, UAC).
- Povoleny budou pouze následující komponenty a SW nesmí žádné další vyžadovat: Microsoft .Net Framework a NET Core – pouze aktuální verze s garantovanou podporou výrobce minimálně 2 roky Oracle Java – pouze aktuální verze s označením Long-Term-Support (LTS) a garantovanou podporou výrobce minimálně 2 roky.
- Součástí dodávky počítače musí být licence OS v rozsahu nezbytném pro provoz počítače, Zařízení a SW.
- Pokud je pro provoz SW nezbytný HW klíč, musí být takový HW klíč součástí dodávky a musí podporovat provoz SW na virtualizační platformě Vmware.
- Přístup do SW musí být možné zabezpečit pomocí LDAPs (serveru) / SSO (klient).
- Všechny bezpečnostní aktualizace (operační systémy, aplikace a další instalované SW komponenty) musí být možné instalovat kdykoli; umožňuje-li výrobce software automatickou aktualizaci, musí být povolena a přednastavena.
- Při plnění smlouvy je zakázáno, resp. Kupující nepřipouští:
 - přímý přístup z vnějšku FN Brno do vnitřní datové sítě FN Brno;
 - provádět instalaci dodavatelských ROOT certifikátů (PC, USER);
 - provádět změnu oprávnění složek na koncových stanicích;
 - provádět změnu oprávnění záznamů v registru (PC, USER);
 - využívat soubor lmhosts;
 - provádět uživatelskou instalaci počítačových programů; povoleny jsou pouze instalace „AllUsers“;
 - připojovat se nebo odesílat data přes telefonní (FAX) linku;
 - využívat pro provoz SW a jiných počítačových programů nepodporované operační systémy, příp. systémy, kterým končí podpora výrobce dříve než za 2 roky ode dne jejich instalace; a
 - instalovat ani používat:
 - makra systému MS Office;
 - Flash player;
 - Active X; ani
- Microsoft Silverlight.

Jestliže je součástí předmětu smlouvy dodávka počítačů nebo poskytnutí software, které nejsou registrovány současně se Zařízením jakožto zdravotnický prostředek dle zákona č. 89/2021 Sb., a tento software je určen pro operační systém Linux, musí takové počítače a takový software splňovat následující požadavky Kupujícího:

- Instalace OS a SW provede zadavatel. Zadavatel OS zavede do domény fnbrno.cz.
- OS pro serverovou část je CentOS/RedHat Linux.
- Instalace serverové části softwaru je povolena pouze do adresáře /opt (včetně logů, konfigurace, atd.).
- Klienti jsou vždy na platformě Windows. Uživatelská/klientská část softwaru proto musí být řešena buď jako webová, nebo být uživatelům poskytována ze síťového úložiště (viz požadavky pro případ OS Windows).
- Správa SW musí být oddělená od správy OS.

- SW musí umožňovat zálohování nástrojem Veeam a vytvářet pomocí tohoto nástroje konzistentní zálohy.
- Pokud je pro provoz SW nezbytný HW klíč, musí být takový HW klíč součástí dodávky a musí podporovat provoz SW na virtualizační platformě Vmware.
- Přístup do SW musí být možné zabezpečit pomocí LDAPs (serveru) / SSO (klient).

Požadavky vyplývající z právní úpravy ochrany osobních údajů:

- Zařízení, je-li součástí předmětu veřejné zakázky software, pak i software, musí umožňovat:
 - dodržování zásad zpracování osobních údajů dle nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „**GDPR**“);
 - výkon práv subjektů osobních údajů upravených v GDPR;
 - provádět zabezpečení osobních údajů proti narušení jejich důvěrnosti.
- Zařízení, je-li součástí předmětu veřejné zakázky software, pak i software, musí:
 - zpracovávat osobní údaje pouze v rozsahu nezbytném pro dosažení účelu tohoto zpracování;
 - zajišťovat zabezpečení osobních údajů proti narušení jejich integrity a dostupnosti;
 - podporovat pseudonymizaci osobních údajů.

Požadavky na vzdálený přístup:

- při poskytování plnění vzdáleným přístupem Kupující umožňuje Prodávajícímu vzdálený přístup pouze prostřednictvím klienta VPN, přičemž Kupující si vyhrazuje právo v průběhu plnění smlouvy klienta VPN změnit na jiného klienta VPN s ohledem na aktuální technologický vývoj;
- pokud Kupující požaduje provádění nepřetržitého vzdáleného dohledu (monitoring) nad Zařízením či jeho součástmi nebo pokud je tento monitoring nezbytný pro provoz Zařízení, může Zařízení využívat pouze odchozí komunikaci směrem z prostředí Kupujícího a zajištění prostupnosti na Firewallu Kupujícího; není-li možné využít pro monitoring pouze odchozí komunikaci, musí Prodávající poskytovat plnění tak, aby monitoring probíhal výhradně prostřednictvím IPSEC tunelu dle blokového komunikačního schéma.

Prodávající je povinen ve lhůtě sjednané pro dodání Zboží v nezbytných podrobnostech zpracovat následující dokumenty, jejichž zpracování podléhá akceptaci Kupujícího:

- zálohovací plán, jehož účelem je v nezbytných podrobnostech popsat proces zálohování Zboží, zejména dat zpracovávaných prostřednictvím Zboží a Software s využitím systému Kupujícího Veeam, a to tak, aby Kupující mohl v součinnosti s Prodávajícím kdykoli (zejména v případě havárie) provést kompletní obnovu v rozsahu těchto záloh (dále jen „**Zálohovací plán**“), přičemž součástí Zálohovacího plánu musí být rovněž specifikace četnosti zálohování a způsobů a míst ukládání záloh, jakož i specifikace požadavků na kapacitu úložiště pro ukládání záloh;
- popis řešení archivace a skartace dat zpracovávaných prostřednictvím Zboží a Software dle platné právní úpravy (dále jen „**Řešení archivace a skartace dat**“);
- migrační plán, jehož účelem je v nezbytných podrobnostech popsat proces převodu dat zpracovávaných prostřednictvím Zboží a Software do jiných systémů, které mají obdobné účelové určení tak, aby Kupující mohl tato data prostřednictvím těchto jiných systémů bez omezení dále zpracovávat (dále jen „**Migrační plán**“).

Požadavky zadavatele na komunikaci s PACS

V případě, že Zařízení má dle této smlouvy komunikovat s PACS Kupujícího, platí následující požadavky Kupujícího:

- Prodávající je dle pokynů Kupujícího v rámci dodávky Zařízení povinen provést nastavení workflow Zařízení, tj. připojení k digitálním archivům Kupujícího, včetně případně nastavení worklistu a odzkoušení bezproblémového provozu dle požadavků Kupujícího;
- Zařízení musí splňovat požadavky na mandatorní DICOM tags pro snímky dle tabulky zpracovávané na základě přílohy č. 3 této smlouvy.

Lhůty a sankce

Veškeré povinnosti Prodávajícího sjednané v této příloze smlouvy je Prodávající povinen splnit ve lhůtě bez zbytečného odkladu.

Pro případ porušení povinností Prodávajícího dle tohoto dodatku se sjednávají následující smluvní pokuty a sankce:

- pokud Prodávající poruší některou svou povinnost uvedenou v této příloze, je povinen uhradit Kupujícímu smluvní pokutu ve výši 10000,- Kč (slovy: desettisíc korun českých), a to za každý takový případ;
- pokud Prodávající neposkytne součinnost ve lhůtě bez zbytečného odkladu, je povinen uhradit Kupujícímu smluvní pokutu ve výši 10000,- Kč (slovy: desettisíc korun českých), a to za každý takový případ a po doručení každé písemné výzvy Kupujícího k poskytnutí takové součinnosti.

V případě, že Zařízení nesplňuje některé z požadavků uvedených v této příloze nebo neumožňuje splnění pokynů udělených Prodávajícímu na základě ujednání uvedených v této příloze, jedná se o podstatné porušení smlouvy, pro které je Kupující oprávněn odstoupit od smlouvy.

PŘÍLOHA Č. 3

Požadavky z oblasti informačních a komunikačních technologií na Předmět výpůjčky

Je-li tato příloha připojena k výzvě k podání nabídky na veřejnou zakázku malého rozsahu zadávanou mimo zadávací řízení, rozumí se v této příloze namísto účastníka zadávacího řízení uchazeč o takovou veřejnou zakázku. Je-li tato příloha součástí podmínek Fakultní nemocnice Brno pro uzavření smlouvy o výpůjčce, rozumí se v této příloze namísto účastníka zadávacího řízení oslovený budoucí půjčitel a namísto zadavatele případný budoucí vypůjčitel. Je-li tato příloha připojena ke smlouvě o výpůjčce, rozumí se v této příloze namísto účastníka zadávacího řízení půjčitel, namísto zadavatele vypůjčitel a pod pojmem Zboží se rozumí Předmět výpůjčky.

Zboží a jeho příslušenství včetně veškerého software, který je součástí nabízeného řešení (dále souhrnně jen „Zařízení“), musí splňovat následující požadavky zadavatele.

Je-li tato příloha připojena k výzvě k podání nabídky na veřejnou zakázku malého rozsahu zadávanou mimo zadávací řízení, rozumí se v této příloze namísto účastníka zadávacího řízení uchazeč o takovou veřejnou zakázku. Je-li tato příloha součástí podmínek Fakultní nemocnice Brno pro uzavření smlouvy o výpůjčce, rozumí se v této příloze namísto účastníka zadávacího řízení oslovený budoucí půjčitel a namísto zadavatele případný budoucí vypůjčitel.

Pokud Zařízení UMOŽŇUJE připojení do datové sítě:

- zadavatel požaduje, aby účastník zadávacího řízení jako součást své nabídky zpracoval blokové komunikační schéma Zařízení dle pokynů na konci těchto požadavků;
- zadavatel požaduje, aby účastník zadávacího řízení jako součást své nabídky zpracoval samostatné blokové komunikační schéma (dle pokynů na konci těchto požadavků) rovněž pro aplikační software, který je součástí předmětu veřejné zakázky.

Pokud Zařízení UMOŽŇUJE připojení do datové sítě, vyhrazuje si zadavatel právo za účelem provádění kybernetických bezpečnostních opatření omezovat připojení Zařízení do datové sítě zadavatele, a to v rozsahu, ve kterém to není pro provoz Zařízení nezbytné a ve kterém to není v rozporu se zadávací dokumentací.

Pokud Zařízení NEUMOŽŇUJE připojení do datové sítě:

- zadavatel požaduje zamezení používání USB portu Zařízení uživatelem, a to pomocí ochrany heslem.

Pokud Zařízení UMOŽŇUJE připojení do datové sítě drátovým připojením, musí splňovat následující požadavky zadavatele:

- Připojení k síti typu Fast Ethernet nebo Gigabit Ethernet
- Rozhraní - konektor RJ-45, propojovací kabel UTP min. cat. 5e mezi zařízením a přípojkou datové sítě v potřebné délce.
- Nevyplyvá-li za zadávací dokumentace, že Zařízení nebude zahrnuto do domény zadavatele, platí následující požadavky zadavatele:
 - Autentizace IEEE 802.1x (EAP-TLS a PEAPv0).
 - Podporované certifikáty - podpora délky klíče 2048 a 4096 bitů, podpora hashovací funkce SHA-256 a SHA-512.
 - Generování klíčů a vystavování odpovídajících certifikátů zajišťuje zadavatel (útvár Centra informatiky).
 - Zařízení musí ověřovat důvěryhodnost certifikátu serveru.

- Zařízení nesmí být provozováno v režimu bridge.
- Protokol - síťový provoz výhradně prostřednictvím IPv4.
- Podpora beztrždního adresování (dle RFC 4632).
- Zařízení musí odpovídat na požadavek o odezvu ICMPv4 (ping) ze sítí, které určí zadavatel.
- Povinné nastavení síťové adresy na DHCP (adresa IP musí být fixována na adresu MAC) prostředky zadavatele dle RFC 2131 a 2132, parametry a volby DHCP je oprávněn určit zadavatel.

Pokud Zařízení UMOŽŇUJE připojení do datové sítě bezdrátovým WiFi připojením, musí splňovat následující požadavky zadavatele:

- Podporovaná frekvenční pásma jsou 2,4 GHz (podpora evropského pásma, kanály 1-13) a 5 GHz (kanály 32-140).
- Podporované přenosové normy jsou 802.11 g/n (2,4 GHz) a 802.11 a/n/ac (5 GHz).
- Podporované šifrování WPA2 (AES), podporovaná délka PSK klíče je min. 16 tisknutelných ASCII znaků.
- Autentizace IEEE 802.1x (EAP-TLS a PEAPv0). Podporované certifikáty - podpora délky klíče 2048 a 4096 bitů, podpora hashovací funkce SHA-256 a SHA-512. Generování klíčů a vystavování odpovídajících certifikátů zajišťuje zadavatel (útvár Centra informatiky). Instalaci prvotního i dalších certifikátů zajišťuje uchazeč. Platnost certifikátu musí činit max. 2 roky. Zařízení musí ověřovat důvěryhodnost certifikátu serveru.
- Wi-Fi Zařízení nesmí být provozováno v režimu bridge.
- MAC adresa Zařízení musí odpovídat MAC adrese koncového bezdrátového interface.
- Wi-Fi Zařízení musí být schopné provozu v prostředí s automatickým přeladováním RF kanálů a optimalizací vysílacího výkonu.
- Protokol - síťový provoz výhradně prostřednictvím IPv4.
- Podpora beztrždního adresování (dle RFC 4632).
- Zařízení musí odpovídat na požadavek o odezvu ICMPv4 (ping) ze sítí, které určí zadavatel.
- Povinné nastavení síťové adresy na DHCP (adresa IP musí být fixována na adresu MAC prostředky zadavatele dle RFC 2131 a 2132, parametry a volby DHCP určuje zadavatel).
- Ochrana pomocí WPA2 klíče, privátního klíče (certifikátu) a přístupových údajů před neautorizovaným přístupem (např. vyčleněním těchto funkcionalit do servisního nastavení přístroje, které je chráněno heslem).

Pokud Zařízení mezi svými komponentami komunikuje bezdrátově, musí taková komunikace splňovat následující požadavky zadavatele:

- musí být provozována v souladu s právními předpisy a rozhodnutím odpovědných orgánů státní správy, musí být zcela nezávislá na stávající již provozované bezdrátové technologii Zadavatele a nesmí ji, jakkoliv ovlivňovat, tj. zejména nesmí využívat stejná frekvenční pásma jako stávající bezdrátová infrastruktura zadavatele a může využívat pouze taková frekvenční pásma a takové způsoby komunikace, které nezpůsobí žádnou interferenci s komunikací ve stávající bezdrátové infrastruktuře zadavatele a žádným způsobem ani potenciálně neovlivní stávající bezdrátovou infrastrukturu zadavatele;
- stávající bezdrátová infrastruktura zadavatele je provozována ve frekvenčním pásmu 2,4 GHz (podpora evropského pásma - kanály 1-13) a 5 GHz (kanály 32-140) s podporovanými přenosovými normami 802.11 g/n (2,4 GHz) a 802.11 a/n/ac (5 GHz);
- nesmí jakkoliv ovlivňovat komunikaci dle standardu WiFi 6E (6GHz) v pásmu 5925 - 6425 MHz (první odrážka se v tomto případě použije obdobně);

- nesmí porušovat regulaci ETSI.

Protokoly nepodporované v prostředí zadavatele:

- Zadavatel nepřipouští komunikaci Zařízení s jinými zařízeními zadavatele následujícími protokoly: FTP, Telnet, SMTP, TFTP, Gopher, POP2, POP3, IMAP, IPX, SMB (SAMBA), NFS v3 a starší (NFS verze 4 je povolen), NCP, RPC, UUCP, RTSP, VNC, IRC, LDAP (povolen je pouze LDAPS), NETBIOS.

Požadavky na antivirovou ochranu:

- Zadavatel požaduje antivirovou ochranu Zařízení jedním z dále uvedených způsobů, ledaže antivirovou ochranu Zařízení nelze s ohledem na jeho povahu využívat. Účastník zadávacího řízení v nabídce uvede, která z následujících variant řešení antivirové ochrany bude u Zařízení zajištěna:
 - Zadavatel umožňuje využití antivirového systému zadavatele, u kterého je zadavatelem zajišťována pravidelná aktualizace.
 - Při použití jiné antivirové ochrany, než je antivirový systém zadavatele, je dodavatel povinen zajišťovat vlastní postup aktualizace, protože **zadavatel nezajišťuje průchod jiných antivirových systémů na jejich aktualizací servery**. Dodavatel je přitom povinen dodržovat veškeré výše a níže uvedené podmínky pro připojení Zařízení do datové sítě zadavatele. O provedených aktualizacích antivirové ochrany je dodavatel povinen vést písemný provozní deník, ve kterém bude zaznamenávat informace o vydaných aktualizacích antivirové ochrany, o provedených aktualizacích antivirové ochrany (tj. implementovaných do Zařízení) včetně informace, kdy byla aktualizace antivirové ochrany Zařízení provedena. Do tohoto provozního deníku dodavatel bude uvádět rovněž, kdo aktualizaci antivirové ochrany provedl, jestliže byla provedena jinak, než automaticky dálkovým přístupem Zařízení na server výrobce antivirové ochrany. Provozní deník může být veden elektronicky, jestliže bude splňovat podmínky presumpce spolehlivosti stanovené § 562 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
- Jestliže antivirovou ochranu Zařízení jedním z výše uvedených způsobů nelze s ohledem na povahu Zařízení zajistit, uvede účastník zadávacího řízení do nabídky zdůvodnění, které musí být objektivní, tj. musí vyplývat z právních předpisů nebo z jiných skutečností nezávislých na účastníkovi zadávacího řízení.

Jestliže je součástí předmětu veřejné zakázky:

- **dodávka počítačů, fyzických serverů, virtuálních appliance nebo poskytnutí software, které nejsou registrovány současně se Zařízením jakožto zdravotnický prostředek dle zákona č. 89/2021 Sb. ani jako diagnostické prostředky in vitro dle zákona č. 268/2014 Sb., a tento software je určen pro operační systém Microsoft Windows, nebo**
- **dodávka software, který je registrován jakožto zdravotnický prostředek dle zákona č. 89/2021 Sb. nebo jako diagnostické prostředky in vitro dle zákona č. 268/2014 Sb., a tento software je určen pro operační systém Microsoft Windows a má být instalován na počítači, fyzickém serveru nebo virtuálním serveru Kupujícího, pak**
takové počítače, servery, appliance a takový software musí splňovat následující požadavky zadavatele:
 - Instalaci operačního systému (dále též jen „OS“) a software (dále též jen „SW“) provede zadavatel. Zadavatel zavede OS do domény fnbrno.cz, tj. předmět veřejné zakázky musí umožňovat toto zavedení.

- Instalace serverové i klientské části SW je povolena pouze do %ProgramFiles% a %ProgramFiles(x86)%. Klientská část SW bude uživatelům poskytována přes DFS ze síťového úložiště, nebo bude virtualizována technologií VMware ThinApp.
- Zařízení ani SW nesmí vytvářet složky a soubory v kořenovém adresáři systémového oddílu.
- SW nesmí pro svůj provoz vyžadovat jiná oprávnění k OS, než která má v defaultním nastavení nastavena skupina Users.
- Zařízení ani SW nesmí jakýmkoliv způsobem manipulovat s oprávněním jednotlivých položek registru OS.
- Veškeré požadované (dokumentované) funkcionality SW musí pracovat s aktivovaným a standardně nastaveným firewallem v OS Windows.
- Na počítači musí být možné instalovat a používat antivirový systém zadavatele. Zadavatel si vyhrazuje právo v průběhu plnění smlouvy antivirový systém s ohledem na aktuální technologický vývoj změnit.
- Veškeré požadované (dokumentované) funkcionality SW musí pracovat s aktivovaným řízením uživatelských účtů (User Account Control, UAC).
- Povoleny budou pouze následující komponenty a SW nesmí žádné další vyžadovat: Microsoft .Net Framework a NET Core – pouze aktuální verze s garantovanou podporou výrobce minimálně 2 roky Oracle Java – pouze aktuální verze s označením Long-Term-Support (LTS) a garantovanou podporou výrobce minimálně 2 roky.
- Součástí dodávky počítače musí být licence OS v rozsahu nezbytném pro provoz počítače, Zařízení a SW.
- Pokud je pro provoz SW nezbytný HW klíč, musí být takový HW klíč součástí dodávky a musí podporovat provoz SW na virtualizační platformě Vmware.
- Přístup do SW musí být možné zabezpečit pomocí LDAPs (serveru) / SSO (klient).
- Všechny bezpečnostní aktualizace (operační systémy, aplikace a další instalované SW komponenty) musí být možné instalovat kdykoli; umožňuje-li výrobce software automatickou aktualizaci, musí být povolena a přednastavena.
- Zadavatel nepřipouští:
 - přímý přístup z vnějšku FN Brno do vnitřní datové sítě FN Brno;
 - provádět instalaci dodavatelských ROOT certifikátů (PC, USER);
 - provádět změnu oprávnění složek na koncových stanicích;
 - provádět změnu oprávnění záznamů v registru (PC, USER);
 - využívat soubor lmhosts;
 - provádět uživatelskou instalaci počítačových programů; povoleny jsou pouze instalace „AllUsers“;
 - připojovat se nebo odesílat data přes telefonní (FAX) linku;
 - využívat pro provoz SW a jiných počítačových programů nepodporované operační systémy, příp. systémy, kterým končí podpora výrobce dříve než za 2 roky ode dne jejich instalace; a
 - instalovat ani používat:
 - makra systému MS Office;
 - Flash player;
 - Active X; ani
 - Microsoft Silverlight.

Jestliže je součástí předmětu veřejné zakázky:

- **dodávka počítačů, fyzických serverů, virtuálních appliance nebo poskytnutí software, které nejsou registrovány současně se Zařízením jakožto zdravotnický prostředek dle zákona č. 89/2021 Sb. ani jako diagnostické prostředky in vitro dle zákona č. 268/2014 Sb., a tento software je určen pro operační systém Linux, nebo**

- **dodávka software, který je registrován jakožto zdravotnický prostředek dle zákona č. 89/2021 Sb. nebo jako diagnostické prostředky in vitro dle zákona č. 268/2014 Sb., a tento software je určen pro operační systém Linux a má být instalován na počítači, fyzickém serveru nebo virtuálním serveru Kupujícího, pak**
takové počítače, servery, appliance a takový software musí splňovat následující požadavky zadavatele:
 - Instalace OS a SW provede zadavatel. Zadavatel OS zavede do domény fnbrno.cz.
 - OS pro serverovou část je CentOS/RedHat Linux.
 - Instalace serverové části softwaru je povolena pouze do adresáře /opt (včetně logů, konfigurace, atd.).
 - Klienti jsou vždy na platformě Windows. Uživatelská/klientská část softwaru proto musí být řešena buď jako webová, nebo být uživatelům poskytována ze síťového úložiště (viz požadavky pro případ OS Windows).
 - Správa SW musí být oddělená od správy OS.
 - SW musí umožňovat zálohování nástrojem Veeam a vytvářet pomocí tohoto nástroje konzistentní zálohy.
 - Pokud je pro provoz SW nezbytný HW klíč, musí být takový HW klíč součástí dodávky a musí podporovat provoz SW na virtualizační platformě Vmware.
 - Přístup do SW musí být možné zabezpečit pomocí LDAPs (serveru) / SSO (klient).

Požadavky vyplývající z právní úpravy ochrany osobních údajů:

- Zařízení, je-li součástí předmětu veřejné zakázky software, pak i software, musí umožňovat:
 - dodržování zásad zpracování osobních údajů dle nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „GDPR“);
 - výkon práv subjektů osobních údajů upravených v GDPR;
 - provádět zabezpečení osobních údajů proti narušení jejich důvěrnosti.
- Zařízení, je-li součástí předmětu veřejné zakázky software, pak i software, musí:
 - zpracovávat osobní údaje pouze v rozsahu nezbytném pro dosažení účelu tohoto zpracování;
 - zajišťovat zabezpečení osobních údajů proti narušení jejich integrity a dostupnosti;
 - podporovat pseudonymizaci osobních údajů.

Požadavky na vzdálený přístup:

- při poskytování plnění vzdáleným přístupem zadavatel umožňuje dodavateli vzdálený přístup pouze prostřednictvím klienta VPN, přičemž zadavatel si vyhrazuje právo v průběhu plnění smlouvy klienta VPN změnit na jiného klienta VPN s ohledem na aktuální technologický vývoj;
- pokud zadavatel požaduje provádění nepřetržitého vzdáleného dohledu (monitoring) nad Zařízením či jeho součástmi nebo pokud je tento monitoring nezbytný pro provoz Zařízení, požaduje zadavatel řešení pouze odchozí komunikací směrem z prostředí zadavatele a zajištění prostupnosti na Firewallu zadavatele; není-li možné využít pro monitoring pouze odchozí komunikaci, požaduje zadavatel, aby monitoring probíhal výhradně prostřednictvím IPSEC tunelu, přičemž účastník zadávacího řízení v takovém případě uvede v nabídce důvody použití tohoto řešení, které musí být objektivní.

Požadavky zadavatele na komunikaci s PACS

V případě, že ze smlouvy vyplývá, že Zařízení má komunikovat s PACS zadavatele, platí následující požadavky zadavatele:

- součástí předmětu veřejné zakázky je provedení nastavení workflow Zařízení, tj. připojení k digitálním archivům zadavatele, včetně případně nastavení worklistu a odzkoušení bezproblémového provozu dle požadavků zadavatele;
- účastník zadávacího řízení v nabídce předloží:
 - předpokládaný průměrný objem dat na jednu studii;
 - DICOM Conformance Statement (v elektronické podobě - formát *.pdf., *.docx nebo *.doc);
- Zařízení musí podporovat odesílání DICOM obrazové dokumentace na více DICOM NODŮ, a to minimálně na dva;
- formát dat: DICOM 3.0
- DICOM služby:
 - Query/Retrieve
 - Store
 - Modality Worklist
 - Storage commitment
 - Modality performed procedure step (MPPS)
 - Print (FN Brno nemá DICOM tiskárny, tedy toto je na zvážení a je zde spíše do výčtu služeb DICOM)
- pokud Zařízení produkuje rentgenové záření, musí být součástí odesílaných DICOM dat i údaje o radiační dávce, a to v DICOM header;
- Zařízení musí umožnit nastavit synchronizaci s NTP serverem zadavatele: protokol NTP, server lsb (10.1.250.11), default port 123 (UDP);
- obslužný software Zařízení musí podporovat manuální editaci patientského záznamu (Patient name, Patient ID, Accessional Number, Study Description);
- výše uvedená identifikace záznamu vyšetření nesmí být součástí snímku (tato vlastnost pouze jako volitelné option, ukládání do záznamu formou metadat);
- účastník zadávacího řízení zpracuje následující tabulku mandatorních DICOM tags pro snímky:

DICOM tag name (DICOM tag No.)	Specific values	Ano/Ne
REQUIRED_STUDY_FIELDS:		
STU_StuDat (0008,0020)	value	
STU_StuTim (0008,0030)	value	
STU_AccNum (0008,0050)	min. "null"	
STU_StuID (0020,0010)	min. "null"	
STU_StuInsUID (0020,000d)	string	
STU_RefPhyNam (0008,0090)	string	
Media Storage SOP Class UID (0002,0002)	string	
Imager Pixel Spacing (0018,1164)	value	
Planar Configuration (0028,0006)	pokud je toto dáno povahou Zařízení	
Image Orientation (Patient) (0020,0037)	pokud je toto dáno povahou Zařízení	
Institution Name (0008,0080)	FN BRNO	
Institutional Department Name (0008,1040)	Zkratka oddělení (např. IGEK, IKK, KRNM)	
REQUIRED_SERIES_FIELDS		
SER_Mod (0008,0060)	value (př. MR, CT, MG, DX,...)	
SER_SerNum (0020,0011)	value	
SER_SerInsUID (0020,000e)	string	
REQUIRED_IMAGE_FIELDS		
IMA_ImaNum (0020,0013)	value	
IMA_SOPInsUID (0008,0018)	string	
IMA_SamPerPix (0028,0002)	value	
IMA_Row (0028,0010)	value	
IMA_Col (0028,0011)	value	
IMA_BitAll (0028,0100)	value	
IMA_BitSto (0028,0101)	value	
IMA_PixRep (0028,0103)	value	

Pokyny pro zpracování blokového komunikačního schéma

Pokud Zařízení UMOŽŇUJE připojení do datové sítě, požaduje zadavatel zpracování blokového komunikačního schéma:

Blokové komunikační schéma účastník zadávacího řízení zpracuje v rozsahu a v podrobnostech nezbytných pro úplné porozumění komunikace systému (tj. Zařízení nebo software) prostřednictvím datové sítě, která je nezbytná pro řádné a bezpečné provozování systému v prostředí zadavatele. Za tímto účelem účastník zadávacího řízení vyplní níže uvedenou tabulku, která se považuje za nedílnou součást blokového komunikačního schéma, a zpracuje blokové komunikační schéma, jehož příklad je přílohou č. 1 těchto požadavků. Toto blokové komunikační schéma účastník zadávacího řízení zpracuje ve formátu VSDX, SVG nebo DRAWIO (např. v aplikaci DRAW.IO dostupné z URL: <https://drawio-app.com/>). Obsahem tohoto blokového komunikačního schéma musí být veškeré komponenty nabízeného řešení, které budou zapojeny do datové sítě zadavatele nebo budou provádět datovou komunikaci s jinými komponentami nabízeného řešení, a to s vyznačením vzájemného zapojení všech komponent a s vyznačením jejich komunikace z a do Internetu. **V rozsahu, v jakém je to možné, účastník zadávacího řízení při zpracování blokového komunikačního schéma vyjde z tohoto příkladu.**

Blokové komunikační schéma musí obsahovat:

- návrh IP adresace;
- směr komunikace (jaké zařízení systému navazuje komunikaci na jaké cíle;
- transportní protokol včetně zdrojových a cílových portů;
- aplikační protokol;
- návrh integrace nebo další specifikace přenosu dat DO a Z sítě zadavatele;
- pokud zadavatel požaduje provádění nepřetržitého vzdáleného dohledu (monitoring) nad Zařízením či jeho součástmi nebo pokud je tento monitoring nezbytný pro provoz Zařízení, musí být taková komunikace popsána v blokovém komunikačním schématu; není-li možné využít pro monitoring pouze odchozí komunikaci, musí být v blokovém komunikačním schématu uveden popis IPSEC tunelu ve všech podrobnostech nezbytných pro konfiguraci prostředí zadavatele a pro posouzení úrovně kybernetické bezpečnosti takového řešení.

Pokud Zařízení UMOŽŇUJE připojení do datové sítě, vyplní účastník zadávacího řízení a v nabídce uvede tuto tabulku, a to v rozsahu nezbytném pro posouzení splnění výše uvedených požadavků, jakož i ostatních požadavků uvedených v zadávací dokumentaci:

Zdrojová adresa (označení zařízení)*	Cílová adresa (označení zařízení)	Transportní protokol (TCP / UDP)	Zdrojový port (je-li znám)	Cílový port	Aplikační protokol (služba)

* Zdrojová adresa je adresa zařízení, které navazuje TCP spojení nebo odesílá UDP datagram.