Požadavky zadavatele v oblasti informačních a komunikačních technologií

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.
- Nevyplývá-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 (útvar Centra informatiky).
    - Zařízení musí ověřovat důvěryhodnost certifikátu serveru.
- Zařízení nesmí být provozováno v režimu bridge.
- Protokol - síťový provoz výhradně prostřednictvím IPv4.
- Podpora beztřídního 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.
- 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 (útvar 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 přelaďováním RF kanálů a optimalizací vysílacího výkonu.
- Protokol - síťový provoz výhradně prostřednictvím IPv4.
- Podpora beztřídního 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).

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 (Microsoft Defender), 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 aktualizační 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 (Microsoft Defender). 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 instalace 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.

Pokyny pro 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, čitelné a modifikovatelné 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.

Účastník zadávacího řízení vyplní 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.*