**Požadavky zadavatele v oblasti informačních a komunikačních technologií**

Zdravotnické prostředky a jejich příslušenství (dále jen „**Zařízení**“) včetně software musí splňovat následující požadavky zadavatele, ledaže zdravotnický prostředek nevyužívá výpočetní techniku ani software.

**S výjimkou Zařízení, která nebudou připojena do datové sítě zadavatele, zadavatel požaduje, aby účastník zadávacího řízení jako součást své nabídky zpracoval blokové komunikační schéma dle pokynů na konci těchto požadavků. Zadavatel požaduje zpracování blokového komunikačního schéma rovněž pro aplikační software, který je součástí předmětu veřejné zakázky.**

**Pokud Zařízení NEBUDE připojeno do datové sítě zadavatele:**

* Zadavatel požaduje zamezení používání USB portu Zařízení uživatelem, a to pomocí ochrany heslem

**Pokud Zařízení BUDE připojeno do datové sítě FN Brno, a to drátovým připojením, musí splňovat následující požadavky zadavatele:**

* Připojení k síti typu Fast Ethernet nebo Gigabit Ethernet
* Rozhraní - konektor RJ-45, propojovací kabel UTP cat. 5e mezi zařízením a přípojkou datové sítě v potřebné délce.
* 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 BUDE připojeno do datové sítě FN Brno, a to 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 (Zařízení nesmí odesílat rámce, které pro adresaci využívají všechny čtyři MAC adresy).
* 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).

**Pokud Zařízení BUDE připojeno do datové sítě zadavatele, ale NESPLŇUJE výše uvedené požadavky zadavatele na připojení do datové sítě:**

* Zadavatel bude oprávněn za účelem naplnění požadavků kybernetické a informační bezpečnosti omezit rozsah a podmínky připojení Zařízení do datové sítě zadavatele. Zadavatel si za tímto účelem vyhrazuje právo jednostranně na základě blokového komunikačního schéma stanovit rozsah a podmínky připojení Zařízení do datové sítě zadavatele, které budou pro dodavatele závazné.

**Požadavky na antivirovou ochranu Zařízení:**

* 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 je součástí předmětu veřejné zakázky dodávka počítače a poskytnutí software, které nejsou registrovány současně se Zařízením jakožto zdravotnický prostředek dle zákona č. 268/2014 Sb., a tento software je určen pro operační systém Microsoft Windows, musí takový počítač a software umožňovat splnění následujících požadavků zadavatele:**

* Instalaci operačního systému (dále též jen „**OS**“) a software (dále též jen „**SW**“) provede zadavatel. Zadavatel zavede OS do domény fnbrno.cz.
* Instalace serverové i klientské části SW je povolena pouze do %PROGRAMFILES%. 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 – od verze 3.5 výše, Microsoft ActiveX – aktuální verze, Microsoft SilverLight – poslední vydaná verze, Oracle Java – pouze aktuální verze.
* 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 LDAP (server) / SSO (klient).

**Jestliže je součástí předmětu veřejné zakázky dodávka počítače a poskytnutí software, které nejsou registrovány současně se Zařízením jakožto zdravotnický prostředek dle zákona č. 268/2014 Sb., a tento software je určen pro operační systém Linux, musí takový počítač a software umožňovat splnění následujících požadavků 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 LDAP (server) / 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 vzdálený přístup prostřednictvím klienta openVPN.

**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. **V rozsahu, v jakém je to možné, účastník zadávacího řízení při zpracování blokového komunikačního schéma vyjde z tohoto příkladu.**

Účastník zadávacího řízení vyplní tuto tabulku:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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.*