Bezpečnostní požadavky dodavatele zdravotnických prostředků

Ústav hematologie a krevní transfuze (dále jen „ÚHKT“) od svých dodavatelů (dále jen „Dodavatel“) vyžaduje dodržování těchto bezpečnostních požadavků.

Vzhledem k tomu, že ÚHKT má zájem na zajištění kybernetické a informační bezpečnosti a vzhledem k tomu, že v souladu s legislativou, která bude platnou a účinnou součástí právního řádu na základě transpozice 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) bude poskytovatelem regulované služby, sjednává s dodavateli tato ujednání.

Dodavatel bere na vědomí, že ÚHKT bude poskytovatelem regulované služby v souladu s transpozicí Směrnice NIS2 a novou legislativou upravující kybernetickou a informační bezpečnost.
Zdravotnické prostředky jsou nedílnou součástí zajišťování poskytování základní služby ÚHKT a zároveň vstupují jako podpůrné aktivum podle § 2 písm. f) vyhlášky č. 181/2018 Sb., o kybernetické bezpečnosti do rozsahu Systému řízení bezpečnostní informací ÚHKT. Z tohoto důvodu je Dodavatel povinen poskytnout dostatečnou součinnost při plnění povinností v oblasti kybernetické bezpečnosti.

Dodavatel musí při plnění smluvního vztahu (dále jen „**Předmět plnění**“) pro ÚHKT dodržovat níže uvedené bezpečnostní požadavky.

Zdravotnickým prostředkem se rozumí nástroj, přístroj, zařízení, software, implantát, činidlo, materiál nebo jiný předmět určené výrobcem k použití, samostatně nebo v kombinaci, u lidí k jednomu nebo několika z těchto konkrétních léčebných účelů:

- diagnostika, prevence, monitorování, predikce, prognóza, léčba nebo mírnění nemoci,
- diagnostika, monitorování, léčba, mírnění nebo kompenzace poranění nebo zdravotního postižení,
- vyšetřování, náhrady nebo úpravy anatomické struktury nebo fyziologického či patologického procesu nebo stavu,
- poskytování informací prostřednictvím vyšetření in vitro, pokud jde o vzorky pocházející z lidského těla, včetně darovaných orgánů, krve a tkání,

který nedosahuje svého hlavního určeného účinku v lidském těle nebo na jeho povrchu farmakologickými, imunologickými ani metabolickými účinky, jehož funkce však může být takovými účinky podpořena.

Za zdravotnické prostředky se považují rovněž tyto výrobky:

- prostředky určené ke kontrole nebo podpoře početí;
- výrobky speciálně určené k čištění, dezinfekci nebo sterilizaci prostředků uvedených výše.

Diagnostickým zdravotnickým prostředkem „in vitro“ se rozumí zdravotnický prostředek, který je činidlem, výsledkem reakce činidla, kalibrátorem, kontrolním materiálem, sestavou, nástrojem, přístrojem, zařízením, softwarem nebo systémem, používaným samostatně nebo v kombinaci, který je výrobcem určen pro vyšetření vzorku in vitro, včetně darované krve a tkání získaných z lidského těla výhradně nebo převážně za účelem získání některé z těchto informací:

a) o fyziologickém nebo patologickém procesu nebo stavu,

b) o vrozeném tělesném nebo mentálním postižení,

c) o predispozici k určitému zdravotnímu stavu nebo nemoci,

d) pro stanovení bezpečnosti a kompatibility s možnými příjemci,

e) k předvídání reakcí na léčbu,

f) pro stanovení a monitorování terapeutických opatření.

Nádoby na vzorky se rovněž považují za diagnostické zdravotnické prostředky in vitro.

Dodavatel musí dodržovat Bezpečnostní požadavky pro zdravotnické prostředky vždy, pokud bude zdravotnický prostředek připojen do interní sítě ÚHKT nebo do interní sítě ÚHKT může být připojen v budoucnu (mají instalován komunikační modul).

Bezpečnostní požadavky pro zdravotnické prostředky musí být dodržovány vždy, pokud je to technicky možné a zdravotnický prostředek to umožňuje, za využití maximálního úsilí ze strany Dodavatele.

V případě, že je Předmětem plnění samostatný zdravotnický prostředek:

1 Konfigurace

1.1 Dodavatel je povinen řídit se pokyny výrobce zdravotnického prostředku a zajistit konfiguraci zdravotnického prostředku dle pokynů a doporučení výrobce.

1.2 Dodavatel je povinen omezit běžící síťové služby a služby operačního systému pouze na nezbytné minimum dle pokynů a doporučení výrobce tak, aby nebyly otevřeny nepotřebné porty.

1.3 Dodavatel je povinen nastavit komunikaci prostřednictvím bezpečných kryptografických protokolů min. TLS 1.2 a komunikačních protokolů SMB 2.0 včetně zapnutého podepisování protokolu.

1.4 Dodavatel je povinen konfigurovat zdravotnických prostředek dle doporučení výrobce v souboru MDS^2 Manufacturer Disclosure Statement for Medical Device Security v nejaktuálnější možné verzi.

2 Zapojení do sítě ÚHKT a segmentace sítě

2.1 Dodavatel je povinen řídit se pokyny ÚHKT při zapojování zdravotnického prostředku do interní sítě ÚHKT. Dodavatel nesmí zapojit zdravotnický prostředek do interní sítě ÚHKT bez informování, konzultace a souhlasu ÚHKT.

2.2 Dodavatel je povinen dodat ÚHKT bezpečnostní dokumentaci obsahující bezpečnou konfiguraci zdravotnického prostředku v souladu s požadavky výrobce zdravotnického prostředku a výsledky penetračních testů, pokud jsou k dispozici. Minimálně je Dodavatel povinen dodat soubor MDS2 Manufacturer Disclosure Statement for Medical Device Security v nejaktuálnější možné verzi.

2.3 Dodavatel je povinen dodat ÚHKT dokumentaci popisující zdravotnický prostředek z pohledu jeho skladby tzn. z jakých síťově připojitelných komponent s vlastní MAC adresou a z jakých softwarových komponent se zdravotnický prostředek skládá. Musí být uvedeny všechny MAC adresy komunikačních modulů zdravotnického prostředku. Dodavatel je povinen dodat Software Bill of Materials (SBOM).

2.4 Dodavatel je povinen dodat ÚHKT dokumentaci popisující požadavky na komunikaci zdravotnického prostředku (komunikační matici). Zejména je potřeba uvést požadavky na komunikaci zdravotnického prostředku do sítě ÚHKT, požadavky na komunikaci s internetem nebo cloudem, požadavky na komunikaci s M4, PACS či laboratorním informačním systémem. Vždy musí být uveden požadavek na komunikační protokol a požadavky na DICOM služby v případě komunikace s PACS.

2.5 Dodavatel nesmí připojit zdravotnický prostředek svévolně. Připojení zdravotnického prostředku musí být vždy za asistence ÚHKT. Zdravotnický prostředek nesmí být zapojen do subnetu obsahující servery nebo do subnetu pro koncová zařízení ÚHKT. Každý zdravotnický prostředek připojený do interní sítě ÚHKT musí být připojen jen do subnetu určeného ÚHKT.

2.6 Subnet, kde bude zdravotnický prostředek zapojen, musí být určen ze strany ÚHKT na základě interních pravidel dříve, než je zdravotnických prostředek do interní sítě ÚHKT zapojen.

2.7 Dodavatel je povinen poskytnout asistenci při ladění síťově bezpečnostních nástrojů, jako jsou IPS (Intrusion Prevention System) či WAF (Web Application Firewall), pokud jsou při instalaci daného zdravotnického prostředku ze strany ÚHKT požadovány.

2.8 Dodavatel nesmí jakkoli měnit interní síť ÚHKT.

2.9 Dodavatel je povinen nastavit zdravotnický prostředek pro autentizaci v síti ÚHKT podle standardu IEEE 802.1x nebo metodou MAC Authentication Bypass (MAB), není-li autentizace podle standardu IEEE 802.1x zdravotnickým prostředkem podporována.

3 Bezpečnost dat zdravotnického prostředku

3.1 Dodavatel je povinen konfigurovat zdravotnický prostředek s cílem zajistit maximální bezpečnost dat při přenosu i uložení, zajistit integritu, dostupnost a důvěrnost dat zpracovávaných zdravotnickým prostředkem na maximální možné úrovni.

3.2 Pokud to zdravotnický prostředek umožňuje, je Dodavatel povinen využívat kryptografickou ochranu zpracovávaných dat.

3.3 Pokud zdravotnický prostředek využívá ke komunikaci standard DICOM, je Dodavatel povinen nakonfigurovat jej v souladu s DICOM profily B.8, B.13, C.3 a D.1, a to v případě, že to zdravotnický prostředek podporuje.

3.4 Pokud zdravotnický prostředek využívá ke komunikaci standard HL7 musí Dodavatel nakonfigurovat bezpečnostní funkce popsané ve verzi HL7 FHIR, je-li zdravotnickým prostředkem podporována.

3.5 Použité kryptografické algoritmy v jednotlivých oblastech zajištění bezpečnosti dat musí být v souladu s dokumentem "Minimální požadavky na kryptografické algoritmy" vydávaným Národním úřadem pro kybernetickou a informační bezpečnost.

4 Aktualizace software

4.1 Dodavatel je povinen při zjištění technických zranitelností v softwarovém vybavení neprodleně informovat ÚHKT o výskytu zranitelnosti prostřednictvím e-mailu a telefonicky dle komunikačních kanálů níže. V rámci informování je Dodavatel povinen sdělit závažnost zranitelnosti, možný dopad pro ÚHKT a poskytnout součinnost při odstraňování zranitelností bez zbytečného odkladu.

4.2 Dodavatel je povinen zajišťovat u zdravotnických prostředků aktuální výrobcem podporovaný operační systém tak, aby se předcházelo výskytu technických zranitelností.

4.3 Dodavatel je povinen instalovat aktualizace operačních systémů.

4.4 V případě nemožnosti aplikace povinností z bodu č. 3.1-3.3 nebo nejnovějšího softwaru je Dodavatel povinen sdělit tyto důvody ÚHKT a poskytnout součinnosti při hledání jiných opatření pro snížení rizik.

5 Skenování technických zranitelností

5.1 Pokud je mu známa, je Dodavatel povinen sdělit ÚHKT citlivost a předpokládanou reakci zdravotnického prostředku při skenování sítě pomocí nástroje pro sken zranitelností ve vlastnictví ÚHKT.

5.2 Dodavatel je povinen poskytnout součinnost pro snížení rizik spojených s odhalenými zranitelnostmi ve zdravotnickém prostředku, které jsou objeveny pomocí nástrojů pro skenování zranitelností.

5.3 Dodavatel je povinen poskytnout součinnost pro snížení rizik spojených s nesprávnou konfigurací zdravotnického prostředku pro připojení do interní sítě ÚHKT, které budu objeveny pomocí nástrojů pro skenování zranitelností.

5.4 Dodavatel je povinen udržovat zdravotnický prostředek bez známých softwarových zranitelností.

6 Přístupová oprávnění

6.1 V operačních systémech zdravotnického prostředku musí být vždy oddělen administrátorský účet od běžných uživatelských účtů.

6.2 Administrátorský účet musí mít přístup jen k nejnutnějším úkonům, které jsou potřeba pro Dodavatele.

6.3 Administrátorský účet nesmí mít přístup k citlivým údajům pacientů (zvláštní kategorii osobních údajů), ani jiným informacím třetích stran.

6.4 Dodavatel musí změnit všechna výchozí hesla k administrátorským účtům.

6.5 Pokud zdravotnický prostředek podporuje autentizaci vůči Active Directory (AD), je dodavatel povinen navrhnout konfiguraci autentizace vůči AD a podle pokynu ÚHKT konfiguraci provést (minimálně pro administrátorské účty).

7 Logování

7.1 Dodavatel je povinen zpřístupnit logování všech dat a informací jako jsou přístupy a veškerá data, která jsou spojená s dodávaným zdravotnickým prostředkem.

7.2 Správné uchovávání dat je Dodavatel povinen kontrolovat na pravidelné bázi, při servisní kontrole, nebo instalaci aktualizací a jiných pracích spojených se zdravotnickým prostředkem.

7.3 Logovaná data nesmí obsahovat citlivé údaje pacientů nebo třetích stran.

8 Servisní počítače a vzdálený servisní přístup

8.1 K servisním zásahům nebo kontrole zdravotnického prostředku smí Dodavatel používat pouze servisní počítač, který je pro tyto úkony určen.

8.2 Servisní počítač musí být vybaven antivirovým programem a zapnutým firewallem s aktuálními definicemi.

8.3 Servisní počítač musí mít nainstalován podporovaný operační systém se všemi dostupnými aktualizacemi.

8.4 Servisní počítač nesmí být používán k jiným než servisním účelům.

8.5 V případě, že Dodavatel bude provádět servisní zásahy nebo kontrolu zdravotnického prostředku v prostředí mimo interní síť ÚHKT, musí používat přístup přes VPN kanál, který bude zřízen ÚHKT pouze na základě požadavku osoby k tomuto požadavku oprávněné.

8.6 V případě přístupu dodavatele přes VPN musí servisní počítač technika provádějící úkon splňovat požadavky 7.1-7.4.

8.7 Pokud je pro poskytování servisu zdravotnického prostředku nutné použít přenosné médium (například USB flash disk), musí být toto médium určeno výhradně a pouze k těmto účelům a musí být šifrováno způsobem, který neumožňuje číst data z nosičů bez znalosti klíče/data. Přenosné médium musí být před vložením do zdravotnického prostředku prověřeno na existenci škodlivých kódů na dedikovaném stroji pro kontrolu USB nosičů.

9 Bezpečnostní incidenty

9.1 Dodavatel je povinen informovat ÚHKT o všech kybernetických bezpečnostních událostech a incidentech, které by mohly mít negativní dopad na ÚHKT prostřednictvím e-mailu dle komunikační matice níže. Informování musí proběhnout bez zbytečného odkladu.

9.2 V případě, že se kybernetická bezpečnostní událost nebo incident týká zdravotnického prostředku, je Dodavatel povinen se podílet svou odborností, znalostí systému na řešení problému a svou součinností pomoci k vyřešení kybernetického bezpečnostního incidentu.

10 Řízení aktiv a rizik

10.1 Dodavatel je povinen se řídit instrukcemi ÚHKT a případně sdělit všechny informace, které by mohly mít negativní dopad na bezpečnost, funkčnost a provoz zdravotnického prostředku.

10.2 Dodavatel je povinen dodat ÚHKT bezpečnostní dokumentaci zdravotnického prostředku, ze které bude vyplývat seznam jednotlivých technických aktiv, ze kterých se zdravotnický prostředek skládá (tzv. dekompozici technických aktiv potřebných pro fungování zdravotnického prostředku na úrovni jednotlivých MAC adres).

10.3 ÚHKT je povinna řídit rizika související s Dodavateli. Pokud ÚHKT identifikuje riziko, jehož míra převyšuje stanovenou akceptovatelnou úroveň a souvisí s předmětem plnění smlouvy, je Dodavatel povinen spolupracovat na stanovení vhodných bezpečnostních opatření ke snížení tohoto rizika a zajistit jeho implementaci na své straně.

11 Údržba

11.1 Dodavatel je povinen před každým úkonem zajistit, že je dostupná zálohovaná konfigurace před tím, než bude proveden zásah do zdravotnického prostředku.

12 Likvidace zdravotnického prostředku

12.1 Pokud Dodavatel provádí vyřazení zdravotnického prostředku z prostředí ÚHKT, je povinen provést jeho bezpečné smazání. Pokud nemá Dodavatel možnost bezpečně smazat data ze zdravotnického prostředku, je povinen předat všechna datová média zdravotnického prostředku ÚHKT. Bezpečným smazáním dat se rozumí odstranění pacientských dat tak, aby tato data nebylo možné žádným způsobem obnovit.

12.2 Dodavatel v případě provádění servisu zdravotnického prostředku odpovídá za ochranu datových médií.

13 Ochrana koncových bodů

13.1 Pokud některé z komponent zdravotnického prostředku umožňují instalaci standardní antivirové ochrany (dále AV) a výrobce ani Dodavatel nevyloučí tuto instalaci z provozních důvodů, je Dodavatel povinen poskytnout ÚHKT součinnost při instalaci AV na všechny podporované komponenty zdravotnického prostředku. Součástí je konfigurace automatické aktualizace AV, pokud tato nebyla výrobcem či Dodavatelem vyloučena z provozních důvodů.

V případě, že je předmětem plnění také počítač (koncová stanice), server, notebook, tablet nebo jiná výpočetní technika, potom Dodavatel rovněž musí zajistit:

14 Přidružená výpočetní technika

14.1 Výpočetní techniku, která přenáší data z nebo do zdravotnického prostředku a zároveň je připojena do interní sítě ÚHKT, je Dodavatel povinen dodat s operačním systémem ve verzi podporované výrobcem operačního systému. Musí být dodána taková verze operačního systému, která bude podporována po celou servisní dobu dodaného zdravotnického prostředku.

14.2 Pro Open Source systémy (GNU/Linux distribuce) je potřeba dodržovat stejné podmínky.

14.3 Dodavatel je povinen dodržovat pro přidruženou výpočetní techniku vše uvedené v sekcích 1. – 13. Nemůže-li Dodavatel splnit pro přidruženou výpočetní techniku některý z těchto kroků, je Dodavatel povinen informovat ÚHKT prostřednictvím e-mailu dle komunikační matice níže.

15 Penetrační testování

15.1 Dodavatel musí umožnit ÚHKT provedení bezpečnostního testování.

15.2 Po sdělení rozsahu a cíle penetračního testu je Dodavatel povinen sdělit případný negativní dopad penetračního testování.

Komunikační kanály:

- Dodavatel hlásí skutečnosti týkající se technických zranitelností, hodnocení rizik nebo bezpečnostní incidenty vždy na e-mail: mkb@uhkt.cz

Dodavatel má povinnost zajistit bezodkladné odstranění zjištěných nedostatků a nesouladu se stanovenými bezpečnostními požadavky na zdravotnické prostředky.