**Příloha č. 3 – Požadavky z oblasti kybernetické bezpečnosti pro dodavatele**

Prodávající bere na vědomí, že Nemocnice Karviná - Ráj, p.o. (dále jen nemocnice) bude samo identifikací dle Národního úřadu pro kybernetickou bezpečnost určena, dle § 3 písm. g) zákona o kybernetické bezpečnosti, provozovatelem základní služby, v odvětví poskytování zdravotních služeb. Informační systém, na kterém je poskytování těchto služeb závislé, je dle § 2 písm. j) zákona o kybernetické bezpečnosti, informačním systémem základní služby a nemocnice je tedy současně i správcem a provozovatelem informačního systému základní služby, dle § 3 písm. f) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Z výše uvedeného vyplývá, že nemocnice je povinna plnit požadavky vycházející ze zákona o kybernetické bezpečnosti a jeho prováděcího právního předpisu vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen VKB). Na základě zřizovatele nemocnice Moravskoslezského krajského úřadu dle usnesení Korporátního výboru řízení kybernetické bezpečnosti číslem 05/KVŘKB/01/2022 se k této nemocnici přistupuje pod výše zmíněnou regulací.

Jelikož technika je nedílnou součástí zajišťování poskytování základní služby nemocnice a zároveň vstupuje jako podpůrné aktivum podle § 2 písm. f) VKB do rozsahu systému řízení bezpečnostní informací nemocnice, bude prodávající povinen za tímto účelem poskytnout dostatečnou součinnost při plnění požadavků v oblasti kybernetické bezpečnosti. Jedná se zejména o níže uvedené provozně technické požadavky na techniku:

**Pokud je součástí předmětu plnění samostatná technologie:**

1. **Aktualizace SW vybavení**

Prodávající je povinen udržovat software vybavení včetně operačního systému v aktuální verzi a provádět instalace bezpečnostních patchů doporučených výrobcem software vybavení. Prodávající je povinen informovat nemocnici o zjištění zranitelností a spolupracovat při jejich řízení.

1. **Přístupová oprávnění**

Systém musí umožnit řízení přístupových oprávnění a oddělení administrátorského a uživatelských účtů. Administrátorský účet nesmí umožnit přístup k osobním údajům pacientů. V případě, že by pro servis pořizované techniky byl nutný přístup k osobním údajům pacientů, musí být s prodávajícím pořizované techniky uzavřena zpracovatelská smlouva podle 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 (dále jen „GDPR“)a zákona č. 110/2019 Sb. o zpracování osobních údajů, ve znění pozdějších předpisů (dále jen „zákon o zpracování osobních údajů“).

1. **Logování**

Prodávající je povinen logovat veškeré přístupy k technice, technická data, která jsou nutná pro dohled a servis a logy uchovávat po dobu 3 měsíců. Logy musí být přístupné přes standardní rozhraní určeným pracovníkům nemocnice. Prodávající nesmí ukládat logy, které obsahují osobní údaje, tyto logy je povinen mazat.

1. **Šifrování dat**

Ukládaná data na datových nosičích, která obsahují osobní údaje pacientů ve smyslu GDPR a zákona o zpracování osobních údajů ve znění pozdějších předpisů, musí být šifrována.

1. **Ukládání konfigurace**

Prodávající je povinen zálohovat kompletní software vybavení pořizované techniky v pravidelných intervalech a uchovávat 3 předchozí verze konfigurace nastavení.

1. **Servisní počítače a vzdálený servisní přístup**

K servisním zásahům nebo kontrole pořizované techniky smí prodávající používat pouze servisní počítač, který je vybaven antivirovým programem s aktuální virovou databází a s výrobcem podporovaným operačním systémem.

V případě, že prodávající bude provádět servisní zásahy nebo kontrolu techniky z prostředí mimo interní síť, musí používat zabezpečený VPN kanál, který bude zřízen nemocnicí na základě Smlouvy o vzdáleném přístupu, kterou je prodávající s nemocnicí povinen uzavřít.

1. **Bezpečnostní incidenty**

Prodávající je povinen informovat nemocnici o všech bezpečnostních událostech a incidentech, které by mohly mít negativní dopad na nemocnici.

1. **Řízení rizik**

Nemocnice bude povinna řídit rizika související s dodavateli. Pokud nemocnice 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.

1. **Síťová komunikace**

Zařízení komunikující v nemocniční síti musí splňovat aktuální síťové a bezpečnostní standardy a pro komunikaci používat zabezpečené protokoly. Prodávající musí poskytnout komunikační matici dodaného zařízení a všechny nepotřebné otevřené komunikační rozhraní a porty musí být v rámci aktuálních hardeningových politik zablokovány. Zapojení zařízení do nemocniční sítě bude prodávající konzultovat a provádět ve spolupráci s ICT oddělením nemocnice.

**Pokud je součástí předmětu plnění také PC, notebook či jiná obdobná výpočetní technika, potom rovněž:**

1. **Operační systém**

Výpočetní techniku je prodávající povinen dodat s operačním systémem ve verzi podporované výrobcem operačního systému, zejména v oblasti bezpečnostních záplat. Pro operační systémy s licencí „Open Source“ (GNU, GPL apod.) musí mít prodávající prokazatelně zajištěnou odpovídající podporu operačního systému.

1. **Penetrační (bezpečnostní) testování**

Prodávající musí umožnit nemocnici provedení bezpečnostního testování v předem stanovených termínech.

Nemocnice bude mít podle § 4 zákona o kybernetické bezpečnosti povinnost zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační systém základní služby a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou.

Vyžadování plnění výše uvedených požadavků, které vyplývají z bezpečnostních opatření nemocnice v míře nezbytné pro splnění povinností nemocnice podle zákona o kybernetické bezpečnosti, není tedy možné považovat podle § 4 zákona o kybernetické bezpečnosti za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

Prodávající má povinnost zajistit bezodkladné odstranění zjištěných nedostatků a nesouladu se stanovenými bezpečnostními požadavky.