**Požadavky na zabezpečení modalit (zdravotnické techniky) v oblasti kybernetické bezpečnosti**

Dodavatel (dodavatelem je pro účely této přílohy myšlen Prodávající či Zhotovitel uvedený ve Smlouvě) bere na vědomí, že Nemocnice Třinec, p.o. bude rozhodnutím 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 Třinec, p.o. 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 Třinec, p.o. 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 „vyhláška o kybernetické bezpečnosti“).

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

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

1. Aktualizace SW vybavení

Dodavatel je povinen udržovat software vybavení včetně operačního systému v aktuální podporované verzi a provádět instalace bezpečnostních patchů doporučených výrobcem software vybavení. Dodavatel je povinen informovat Nemocnici Třinec, p.o. 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 zdravotnické techniky byl nutný přístup k osobním údajům pacientů, musí být s dodavatelem zdravotnické 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

Dodavatel je povinen logovat veškeré přístupy ke zdravotnické technice, technická data zdravotnické techniky, která jsou nutná pro dohled a servis a logy uchovávat po dobu 3 měsíců. Logy musí být přístupné přes standardní rozhraní určeným pracovníkům Nemocnice Třinec, p.o. Dodavatel 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

Dodavatel je povinen ukládat (zálohovat) kompletní software vybavení zdravotnické techniky v pravidelných intervalech a uchovávat 3 předchozí verze konfigurace nastavení.

1. Servisní počítače a vzdálený servisní přístup

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

V případě, že dodavatel bude provádět servisní zásahy nebo kontrolu zdravotnické techniky z prostředí mimo interní síť Nemocnicí Třinec, p.o., musí používat zabezpečený VPN kanál, který bude zřízen Nemocnicí Třinec, p.o. na základě Smlouvy o vzdáleném přístupu, kterou je dodavatel s Nemocnicí povinen uzavřít a pouze na základě požadavku osoby k tomuto požadavku oprávněné. VZOR smlouvy je součástí VZ.

Přiloha - VZOR dokumentu smlouva VPN Nemocncie Třinec.docx

1. Bezpečnostní incidenty

Dodavatel je povinen informovat Nemocnice Třinec, p.o. o všech bezpečnostních událostech a incidentech, které by mohly mít negativní dopad na Nemocnice Třinec, p.o.

1. Řízení rizik

Nemocnice Třinec, p.o. bude povinna řídit rizika související s dodavateli. Pokud Nemocnice Třinec, p.o. 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. Technický popis a komunikační matice

Dodavatel je povinen Nemocnici Třinec, p.o. dodat technický popis řešení a komunikační matici pro nastavení Firewall politik (komunikační porty).

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

1. Operační systém

Výpočetní techniku, která je připojena ke zdravotnické technice a zároveň do interní Nemocnice Třinec, p.o.,

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

1. Penetrační (bezpečnostní) testování

Dodavatel musí umožnit Nemocnice Třinec, p.o. provedení bezpečnostního testování v předem stanovených termínech.

Nemocnice Třinec, p.o. 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 Třinec, p.o. v míře nezbytné pro splnění povinností Nemocnice Třinec, p.o. 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.

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