1. Účel

1. Nemocnice na Homolce (dále jen „Nemocnice“) od svých dodavatelů (dále jen „Dodavatel“) vyžaduje dodržování těchto pravidel chování v souladu s Politikou bezpečnosti informací, která je k dispozici na oficiálních webových stránkách https://www.homolka.cz/o-nemocnici/politika-bezpecnosti-informaci.
2. Dodavatel bere na vědomí, že Nemocnice je provozovatelem základní služby s informačním systémem základní služby v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů.
3. Dodavatel musí při plnění smluvního vztahu (dále jen „Předmět plnění“) pro Nemocnici dodržovat níže uvedená pravidla.
4. Dodavatel musí dodržovat Bezpečnostní požadavky pro zdravotnické prostředky vždy, pokud je to technicky možné.

2. Obecná pravidla

1. Předmět plnění nesmí být zatížen žádnými faktickými ani právními vadami a musí odpovídat všem technickým a technologickým požadavkům, technickým a bezpečnostním normám pro daný druh Předmětu plnění, a to jak normám závazným, tak i doporučujícím.
2. Dodavatel se zavazuje upozorňovat Nemocnici včas na všechny hrozící vady svého plnění či potenciální výpadky nebo rizika plnění, jakož i poskytovat Nemocnici veškeré informace, které jsou pro plnění smlouvy nezbytné
3. Dodavatel se zavazuje upozornit Nemocnici na potenciální rizika vzniku škod a včas a řádně dle svých možností provést taková opatření, která riziko vzniku škod zcela vyloučí nebo sníží.
4. Dodavatel se zavazuje nakládat s veškerými daty, informacemi a údaji, ke kterým se dostane v rámci Předmětu plnění takovým způsobem, aby nemohlo dojít k jejich ztrátě, vyzrazení, neoprávněné či neodborné manipulaci. Dále se zavazuje používat tato data pouze k danému účelu a neumožnit jejich zpřístupnění nepovolané osobě.
5. Dodavatel se zavazuje dodržovat veškerou platnou legislativu, zejména pak tu v oblasti kybernetické bezpečnosti a ochrany osobních údajů, zejména pak 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 zákon č. 110/2019 Sb., o zpracování osobních údajů.
6. Náklady, které je třeba vynaložit na zavedení bezpečnostních požadavků, nese Dodavatel.

3. Zdravotnický prostředek

1. Zdravotnické prostředky jsou nedílnou součástí zajišťování poskytování základní služby Nemocnice a zároveň vstupují jako podpůrné aktivum podle § 2 písm. f) vyhlášky o kybernetické bezpečnosti do rozsahu Systému řízení bezpečnostní informací Nemocnice. Z tohoto důvodu je Dodavatel povinen poskytnout dostatečnou součinnost při plnění povinností v oblasti kybernetické bezpečnosti.

2. Zdravotnické prostředky jsou technická aktiva definovaná zákonem č. 375/2022 Sb., o zdravotnických prostředcích a diagnostických zdravotnických prostředcích in vitro.

V případě, že je Předmětem plnění samostatný zdravotnický prostředek:

4. Konfigurace

1. Dodavatel je povinen řídit se pokyny výrobce zdravotnického prostředku a zajistit konfiguraci zdravotnické prostředku dle pokynů a doporučení výrobce.
2. Dodavatel je povinen nastavit vnitřní síťové prostupy pouze na nezbytné minimum dle pokynů a doporučení výrobce tak, aby nebyly otevřeny nepotřebné porty.

5. Zapojení do sítě Nemocnice a segmentace sítě

1. Dodavatel je povinen řídit se pokyny Nemocnice při zapojování zdravotnického prostředku do interní sítě Nemocnice. Dodavatel nesmí zapojit zdravotnický prostředek do interní sítě Nemocnice bez informování, konzultace a souhlasu odboru ICT Nemocnice.
2. Dodavatel je povinen dodat Nemocnici bezpečnostní dokumentaci obsahující bezpečnou konfiguraci zdravotnické prostředku v souladu s požadavky výrobce zdravotnického prostředku.
3. Dodavatel je povinen dodat Nemocnici dokumentaci popisující zdravotnický prostředek z pohledu jeho skladby tzn. z jakých komponent se zdravotnický prostředek skládá.
4. Dodavatel nesmí připojit zdravotnický prostředek svévolně. Připojení zdravotnického prostředku musí být vždy za asistence Nemocnice. Zdravotnický prostředek nesmí být zapojen do subnet obsahující servery nebo do subnet pro koncová zařízení Nemocnice. Každý prostředek připojený do sítě musí být připojen jen do subnetu určeným odborem ICT Nemocnice.
5. Síť, kde bude zdravotnický prostředek zapojen, musí být určena ze strany Nemocnice na základě interních pravidel dříve, než je zdravotnických prostředek do sítě zapojen.
6. Dodavatel je povinen se řídit instrukcemi Nemocnice (a případně sdělit všechny informace, které by mohly mít negativní dopad na bezpečnost, funkčnost a provoz zdravotnického prostředku.
7. Dodavatel nesmí jakkoliv měnit interní síť Nemocnice.

6. Aktualizace software

1. Dodavatel je povinen při zjištění technických zranitelností v softwarovém vybavení neprodleně informovat Nemocnici o výskytu zranitelnosti prostřednictvím e-mailu a telefonicky dle komunikačních kanálů níže. V rámci informování je Dodavatel povinen sdělit závažnost technické zranitelnosti, možný dopad pro Nemocnici a poskytnout součinnost při odstraňování technických zranitelností bez zbytečného odkladu.
2. Dodavatel je povinen zajišťovat u zdravotnických prostředků aktuální podporovaný operační systém tak, aby se předcházelo výskytu technických zranitelností.
3. Dodavatel je povinen instalovat aktualizace operačních systémů a informovat o nich Nemocnici prostřednictvím e-mailu dle komunikačních kanálů níže. V případě nemožnosti instalace

nejnovějšího softwaru je Dodavatel povinen sdělit tyto důvody Nemocnici a poskytnout součinnosti při hledání jiných opatření pro snížení rizik.

7. Skenování technických zranitelností

1. Dodavatel je povinen sdělit Nemocnici citlivost a předpokládanou reakci zdravotnického prostředku při skenování sítě pomocí nástroje pro skenování technických zranitelností.
2. Dodavatel je povinen poskytnout součinnost pro snížení rizik spojených s odhalenými zranitelnostmi ve zdravotnickém prostředku, které jsou objeveny pomocí nástrojů pro skenování zranitelností.
3. Dodavatel je povinen poskytnout součinnost pro snížení rizik spojených s nesprávnou konfigurace zdravotnické prostředku, které budu objeveny pomocí nástrojů pro skenování zranitelností.
4. Dodavatel je povinen udržovat zdravotnický prostředek bez softwarových zranitelností.

8. Přístupová oprávnění

1. V operačních systémech zdravotnického prostředku musí být oddělen administrátorský účet od běžných uživatelských účtů.
2. Administrátorský účet musí mít přístup jen k nejnutnějším úkonům, které jsou potřeba pro Dodavatele a úkonů s tím souvisejících.
3. Administrátorský účet nesmí mít přístup k citlivým údajům pacientů Nemocnice (zvláštní kategorii osobních údajů), ani jiným informacím třetích stran. Pokud je pro tento účel potřeba vytvořit zvláštní účet pro Dodavatele, bude účet vytvořen za součinnosti odboru ICT Nemocnice.
4. Dodavatel musí změnit všechna výchozí hesla k administrátorským účtům.

9. Logování

1. Dodavatel je povinen zpřístupnit logování všech dat a informací jako jsou přístupy a veškerá data, která jsou spojená s dodávaným zdravotnickým prostředkem.
2. Správné uchovávání dat je Dodavatel povinen kontrolovat na pravidelné bázi, při servisní kontrole, nebo instalaci aktualizací a jiných pracích spojených se zdravotnickým prostředkem.
3. Logovaná data nesmí obsahovat citlivé údaje pacientů nebo třetích stran.

10. Šifrování

1. 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 způsobem, který neumožnuje číst data z nosičů bez znalosti klíče/hesla.

11. Servisní počítače a vzdálený servisní přístup

1. K servisním zásahům nebo kontrole zdravotnického prostředku smí Dodavatel používat pouze servisní počítač, který je pro tyto úkony určen.
2. Servisní počítač musí být vybaven antivirovým programem a zapnutým firewallem s aktuálními definicemi a nesmí být používán k osobním účelům.

3. Servisní počítač musí mít nainstalován podporovaný operační systém se všemi dostupnými aktualizacemi.
4. V případě, že Dodavatel bude provádět servisní zásahy nebo kontrolu zdravotnického Prostředku v prostředí mimo interní síť Nemocnice, musí používat přístup přes VPN kanál (IPSEC tunel), který bude zřízen Nemocnicí pouze na základě požadavku osoby k tomuto požadavku oprávněné. Tento přístup bude udělen jen na dobu určitou a nezbytně nutnou k servisním úkonům.
5. V případě přístupu dodavatele přes VPN musí servisní počítač technika provádějící úkon splňovat požadavky bodu 1-3.
6. 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. Přenosné médium musí být před vložením do zdravotnického prostředku prověřeno na existenci škodlivých kódů ze strany Dodavatele.

12. Bezpečnostní incidenty

1. Dodavatel je povinen informovat Nemocnici o všech kybernetických bezpečnostních událostech a incidentech, které by mohly mít negativní dopad pro Nemocnici prostřednictvím e-mailu dle komunikačních kanálů níže.
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.

13. Řízení aktiv a rizik

1. Dodavatel je povinen dodat Nemocnici bezpečnostní dokumentaci zdravotnického prostředku, ze které bude vyplývat seznam jednotlivých aktiv, ze kterých se zdravotnický prostředek skládá (tzv. dekompozici aktiv).
2. Nemocnice je 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.

14. Údržba

1. Dodavatel je povinen poskytnout na vyžádání Nemocnice doporučenou konfiguraci dodávaného zdravotnického prostředku.
2. Dodavatel je povinen před každým úkonem ověřit od Nemocnice, že je dostupná zálohovaná konfigurace před tím, než bude proveden zásah do zdravotnického prostředku.
3. Dodavatel má povinnost zajistit bezodkladné odstranění zjištěných nedostatků a nesouladu se stanovenými Bezpečnostními pravidly pro zdravotnické prostředky.

V případě, že je Předmětem plnění také počítač (koncová stanice), server, notebook, tablet nebo jiná výpočetní technika, potom rovněž

15. Přidružená technická aktiva

1. Technická aktiva, která jsou připojena, přenášejí si data se zdravotnickým prostředkem a zároveň jsou připojena do interní sítě Nemocnice, je Dodavatel povinen dodat s operačním systémem ve verzi podporované výrobcem operačního systému. Musí být dodána taková verze operačního sytému, která bude podporována po celou servisní dobu dodaného přístroje.
2. Pro Open Source systémy (GNU/Linux distribuce) je potřeba dodržovat stejné podmínky.
3. Dodavatel je povinen dodržovat pro přidružená technická aktiva vše uvedené v sekcích 1. - 12. Nemůže-li Dodavatel splnit některý z těchto požadavků, je Dodavatel povinen informovat Nemocnici prostřednictvím e-mailu dle komunikační matice níže.

16. Testování zranitelností

1. Dodavatel musí umožnit Nemocnici provedení bezpečnostního testování technických aktiv zdravotnického prostředku.
2. Po sdělení rozsahu a cíle penetračního testu je Dodavatel povinen sdělit případný negativní dopad bezpečnostního testování na technická aktiva zdravotnického prostředku.

17. Komunikační kanály

1. Dodavatel hlásí skutečnosti týkající se technických zranitelností odboru ICT Nemocnice vždy na e-mail: kict@homolka.cz a telefonicky na tel.: +420 257 272 143 (Nemocnice výslovně vyžaduje duplicitní informaci, tedy telefonem a zároveň i e-mailem).
2. Dodavatel hlásí skutečnosti týkající se hodnocení rizik Manažerovi kybernetické bezpečnosti vždy na e-mail mkb@homolka.cz.
3. Dodavatel hlásí skutečnosti týkající se bezpečnostních incidentů Manažerovi kybernetické bezpečnosti na e-mail mkb@homolka.cz.

MUDr. Petr Polouček

Digitálně podepsal MUDr. Petr Polouček
Datum: 2024.05.02 14:18:10 +02'00'