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.

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. Zaměstnanci Dodavatele mohou přistupovat k informačním a komunikačním prostředkům (ICT prostředky) Nemocnice výhradně prostřednictvím autentizačních údajů přidělených Nemocnicí (např. VPN přístup).
3. Dodavatel se zavazuje dodržovat bezpečnostní opatření a pravidla Nemocnice při práci s informacemi a ICT prostředky Nemocnice.
4. 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
5. 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.
6. Dodavatel se zavazuje informovat Nemocnici o způsobu řízení rizik, zbytkových rizik souvisejících s plněním smlouvy a bez zbytečného odkladu také o změnách ve způsobu řízení a zvládání rizik.
7. 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.
8. 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.
9. Náklady, které je třeba vynaložit na zavedení bezpečnostních pravidel, nese Dodavatel.

3. Bezpečnost komunikace

1. Předmět plnění nesmí být zatížen žádnými faktickými ani právními vadami a musí odpovídat všem technickým požadavkům, technickým a bezpečnostním normám pro daný druh Předmětu plnění, a to jak normám závazným, tak i doporučujícím.
2. V případě ztráty nebo odcizení hardware, software, dat, informací Nemocnice musí Dodavatel vždy neprodleně nahlásit tuto skutečnost odboru ICT Nemocnice, a to i v případě pouhého podezření neoprávněný přístup a manipulaci s daty.
3. Dodavatel hlásí skutečnosti 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. Případně na technologické kontakty přímo uvedené ve smlouvě.
4. Při práci na jakémkoliv zařízení (například: počítači, notebooku, mobilním telefonu, zdravotnickém prostředku) připojeném do sítě a/nebo k informačním systémům Nemocnice musí Dodavatel dodržovat tyto zásady:
    a. umožnit přístup jen proškolenému a řádně nahlášenému zaměstnanci Dodavatele,
    b. chránit výpočetní techniku a všechna data Nemocnice před porušením důvěrnosti, integrity či dostupnosti,
    c. po ukončení práce v síti a/nebo v informačním systému Nemocnice provést neprodleně odhlášení uživatele.
5. Při práci na serverech Nemocnice musí být splněny následující zásady, které se vztahující i na servisní (provozní) smlouvy (s ohledem na specifikace informačních systémů):
    a. server svěřený Dodavateli do správy musí Dodavatel pravidelně udržovat a kontrolovat zejména z pohledu bezpečnosti, dostupnosti a integrity dat,
    b. dodavatel nesmí měnit jakákoliv oprávnění na serveru nebo informačním a komunikačním systému bez souhlasu odboru ICT Nemocnice,
    c. dodavatel nesmí měnit nastavení operačního systému serverů a jeho komponent bez souhlasu odboru ICT Nemocnice,
    d. dodavatel musí zajistit bezpečnostní aktualizaci operačního systému a aplikačních částí serverů; bezpečnostní aktualizace kritického charakteru, které mohou ohrozit bezpečnost sítě Nemocnice musí aplikovat neprodleně po jejich vydání,
    e. dodavatel je povinen udržovat aktuální dokumentaci k provozovaným informačních a komunikačním systémům, kterou po každé aktualizaci musí předat odboru ICT Nemocnice
6. Při práci v interní sítí Nemocnice odpovídají zaměstnanci Dodavatele, kteří mají přidělen přístup do interní sítě Nemocnice, za své činnosti prováděné v rámci této sítě. Zaměstnanci Dodavatele nesmí, zejména:
    a. zneužívat síťové prostředky pro osobní účely a zatěžovat kapacitu sítě nebo síťových zařízení,
    b. šířit či jinak nakládat se škodlivým malwarem,
    c. využívat nástroje sloužící k maskování identity,
    d. provádět bezdůvodné skenování portů či jiných parametrů sítě a síťových zařízení,

e. provádět jakoukoliv formou monitorování sítě, které může vést k zachycení dat, pokud není Předmětem plnění smlouvy,

f. obcházet autentizaci uživatele nebo obcházet zabezpečení jakéhokoliv počítače, sítě nebo uživatelského účtu,

g. provádět jakékoliv nepracovní aktivity vedoucí k omezování nebo odepírání služeb jiným uživatelům,

h. užívat jakékoliv programy, skripty nebo příkazy, nebo zasílat zprávy v jakékoliv formě s úmyslem omezit nebo znemožnit poskytování služeb nebo terminálových relací lokálně nebo přes síť, internet nebo intranet,

i. využívat bezpečnostních mezer nebo vytvářet útoky na komunikaci v počítačových sítích (např. přístup k datům, jichž není zaměstnanec zamýšleným příjemce, přihlašování na server nebo účet zaměstnancem, který není k tomuto přístupu výslovně oprávněn, s výjimkou případů, kdy tyto aktivity jsou součástí řádných pracovních úkolů),

j. předávat informace o konfiguraci a topologii sítě cizím osobám; tyto informace je oprávněn předat pouze odpovědný zaměstnanec Nemocnice, pokud jsou takové informace nutné z hlediska přípravy či Předmětu plnění.

4. Kybernetické bezpečnostní události a incidenty

1. Dodavatel musí vyvinout maximální úsilí pro odvracení bezpečnostních hrozeb a kybernetických útoků pro informační a komunikační systémy Nemocnice.
2. Dodavatel musí zajistit maximální součinnost při analýze kybernetických bezpečnostních událostí a incidentů Nemocnice a následně zavádět vhodná nápravná opatření určené Nemocnicí.
3. V případě podezření či potvrzení vzniku bezpečnostní hrozby pro informační a komunikační systém Nemocnice je dodavatel povinen neprodleně písemně (e-mailem) či telefonicky (a následně také písemně) informovat o této skutečnosti Manažera kybernetické bezpečnosti Nemocnice.
4. V případě že se dodavatel stane obětí kybernetického útoku musí tuto skutečnost neprodleně nahlásit písemně (e-mailem) či telefonicky (a následně písemně) Manažerovi kybernetické bezpečnosti Nemocnice.

5. Požadavky na dodávané informační systémy

1. Požadavky na dodávané informační systémy

a. Informační systém musí být vytvářen tak, aby dostatečně chránil data před narušením důvěrnosti, dostupnosti a integrity.

b. Informační systém musí být vytvořen tak, aby byla každá operace uložena v provozním záznamu (logu) s jedinečným identifikátorem uživatele, který tuto operaci vykonal. Musí být zajištěno, aby nemohlo dojít k provádění operací pod cizím identifikátorem uživatele.

c. Uživatel informačního systému musí být nucen používat dostatečně silná a dlouhá hesla (min. 12 znaků).

d. Informační systém musí být vytvořen tak, aby byl počet neúspěšných pokusů o přihlášení omezen. Po deseti neúspěšných pokusech o přihlášení musí být další zadávání dočasně zablokováno nebo spojení rozpojeno.

e. V případě, že je povolen přístup do informačního systému, v němž určuje vstupní heslo administrátor, je povinností autora informačního systému vynutit si změnu tohoto inicializačního hesla.

f. Dodavatel nesmí používat jedno přihlašovací jméno pro několik svých zaměstnanců, každý účet musí být jmenný.

g. Informační systém nesmí obsahovat žádné komponenty své nebo třetích stran na kterých jsou zjištěny nevyřešené bezpečnostní hrozby se skórem CVE 3 a více.

2. V informačních systémech musí být pořizovány auditní záznamy obsahující alespoň:

a. identifikaci uživatele;

b. datum a čas přihlášení a odhlášení;

c. identifikaci místa, odkud se uživatel přihlašoval (pokud je to možné);

d. záznamy o přístupu (úspěšném i neúspěšném), případně o prováděných operacích;

e. záznamy musí být možné vzdáleně číst a následně zpracovávat nebo je systém musí automaticky odesílat na vzdálený bezpečnostní dohledový systém Nemocnice.

3. Řízení přístupu k informačním systémům

a. Před umožněním přístupu musí být každý uživatel identifikován a autentizován.

b. Informační systém by měl po určité době nečinnosti uživatele (doporučeno 15 minut) tohoto uživatele odhlásit.

c. Po určitém množství neúspěšných autentizačních pokusů (doporučeno 10) se musí ukončit přihlašovací proces.

d. V případě neúspěšné autentizace nesmí informační systém poskytnout uživateli informaci o tom, která část autentizace je chybná.

e. Pro každého uživatele informačního systému musí být možné identifikovat, jaká má přístupová práva.

f. Pro každý prostředek musí být možné vytvořit seznam uživatelů, kteří mají přístupová práva k tomuto prostředku s rozlišením druhu přístupových práv (čtení, úprava atd.).

g. Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo skupině.

h. Informační systém musí být technologicky připojitelný k centrální správě přihlašovacích údajů nemocnice (LDAP, AD, atd..)

4. Data vstupující do informačních systémů musí být kontrolována tak, aby byla zajištěna jejich správnost. V informačních systémech se musí evidovat identifikátor uživatele, který změny provedl. Pro kontrolu dat musí Dodavatel aplikovat opatření:

a. vstupní kontrola (neplatné znaky, rozsah, přetečení, kompletnost, souvislost...),

b. kontrola vnitřního zpracování dat,

c. kontrola oprávněnosti běhu programů,

d. kontrola integrity dat,

e. kontrola obsahu generovaných dat.

5. Vývoj software musí probíhat:

a. legálním softwarem,

b. autorská a licenční ujednání musí být smluvně řešena před samotným vývojem,

c. na testovacím prostředí odděleném od prostředí produkčního,

d. na testovacích datech, která nejsou převzata z provozní databáze; pokud je nutné použít data z provozní databáze, je nutné je anonymizovat,

e. migrace do provozního prostředí může být provedena až po akceptaci výsledků testů ve vývojovém či testovacím prostředí.

6. Požadavky na dodávané informační systémy

1. Je-li informační systém vyvíjen na zakázku, musí splňovat všechny níže uvedené body a jedná-li se o již vyvinutý informační systém, musí být tyto požadavky zohledněny v hlavní smlouvě.

2. Dodávka software

a. Dodávka software musí být řádně smluvně zajištěna a průběžně kontrolována a dokumentována. Pokud není stanoveno ve smlouvě jinak, je Dodavatel povinen software dodat se zdrojovými kódy.

b. U veškerého dodávaného programového vybavení musí být zřejmé, zda se jedná o volně šířený software nebo program podléhající licenční a registrační politice. Pracuje-li počítačový program nebo aplikace, s daty, musí být specifikováno s jakými daty a musí být provedena jejich kategorizace. V případě, že jsou komponenty programu podléhající licenční a registrační politice, software musí být vždy dodán s platnými a správnými licencemi pro dané komponenty.

3. Dodávka hardware

a. Ke každé dodávce musí existovat kromě účetních dokladů i předávací protokol podepsaný Dodavatelem a Nemocnicí. Způsob předání závisí na konkrétním hardware a na smlouvě s Dodavatelem.

4. Dodávka služeb

a. Způsob předání závisí na konkrétní službě a na smluvních podmínkách dohodnutých ve Smlouvě.

b. Dodavatel zajistí monitorování služby tak, aby bylo možné porovnání jejich parametrů, rozsahu a kvality stanovených Smlouvou.

5. Dokumentace

a. Nedílnou součástí dodávky Předmětu plnění je projektová a bezpečnostní dokumentace Předmětu plnění. Rozsah a náplň dokumentace musí být specifikován ve smlouvě s

Dodavatelem. Chybějící, neúplná nebo neaktuální dokumentace je důvodem k reklamaci dodávky a v případě, že ji Dodavatel ve lhůtě stanovené Nemocnicí neopraví, důvodem k odstoupení od Smlouvy.

b. Pokud má být měněn Předmět plnění, musí Dodavatel aktualizovat dokumentaci.

c. Dokumentace pro obsluhu (návody, manuály) musí být dodány v českém jazyce, dokumenty technické, konfigurační a provozní musí být dodány v českém nebo anglickém jazyce

6. Akceptace

a. Každý dodávaný prvek Předmětu plnění musí být plně a široce Dodavatelem otestován, zda splňuje očekávané a smluvně definované parametry, a zda jeho používání nepředstavuje neočekávaná bezpečnostní rizika (penetrační test, práce s daty).

b. Každý prvek Předmětu plnění je předán až podpisem písemného předávacího protokolu oprávněnými zástupci smluvních stran.

7. Fyzická bezpečnost

1. Je-li informační systém vyvíjen na zakázku, musí splňovat všechny níže uvedené body a jedná-li se o již vyvinutý informační systém, musí být tyto požadavky zohledněny v hlavní smlouvě.
2. Na neveřejných pracovištích a prostorách Nemocnice (např. datové centrum) není dovolen pohyb cizích osob bez dozoru zaměstnance Nemocnice.
3. Zaměstnanci Dodavatele mohou fyzicky přistupovat k ICT prostředkům Nemocnice pouze v doprovodu oprávněné osoby Nemocnice.
4. V případě práce Dodavatele v prostorách Nemocnice nebo v jím využívaných prostorách v datových centrech musí Dodavatel dále dodržovat tyto zásady:
   a. připojovat vlastní počítač, notebook pouze se souhlasem odpovědné osoby Nemocnice,
   b. v blízkosti ICT prostředků nejíst, nepít a nekouřit.
5. Dodavatel není oprávněn k výměně a odvozu použitých či vadných technologií bez autorizace Nemocnice.

8. Účast poddodavatelů

1. Dodavatel se zavazuje, že při poskytování plnění pro Nemocnici budou všichni poddodavatelé, které Dodavatel využívá k poskytnutí plnění dle smlouvy, dodržovat veškeré požadavky vyplývající ze smlouvy. Dodavatel odpovídá za to, že jeho Poddodavatelé nebudou jednat v rozporu s ujednáními smlouvy, kterou mezi sebou uzavřel Dodavatel a Nemocnice.
2. Dodavatel nezapojí do poskytování plnění dle smlouvy žádného dalšího poddodavatele bez předchozího konkrétního písemného povolení ze strany Nemocnice.
3. Pokud Dodavatel využívá při poskytování plnění poddodavatele, zavazuje se, že budou dodržovat stejné bezpečnostní požadavky a pravidla požadovaná po Dodavateli.

4. Dodavatel se zavazuje bezodkladně doložit Nemocnici, na základě předchozí výzvy, smluvní dokumenty se svými poddodavateli, ze kterých bude vyplývat závazek poddodavatele poskytovat plnění v souladu s bezpečnostními požadavky a pravidly požadovanými po Dodavateli.
5. Dodavatel odpovídá za to, že jeho poddodavatelé nebudou jednat v rozporu s bezpečnostními požadavky a pravidly.

9. Poskytování informací třetím stranám

1. Je-li informační systém vyvíjen na zakázku, musí splňovat všechny níže uvedené body a jedná-li se o již vyvinutý informační systém, musí být tyto požadavky zohledněny v hlavní smlouvě.
2. Dodavatel je povinen dodržovat mlčenlivost o důvěrných informacích Nemocnice, které se dozvěděl při dodávce Předmětu plnění, a to i po ukončení smluvního vztahu založeného Smlouvou. Důvěrnou informací Nemocnice se rozumí informace obchodní, technické, know how, podklady a doklady, osobní údaje, zdravotnická dokumentace či jiné, které jsou významné pro Nemocnici a/nebo jsou konkurenčně významné a nejsou veřejně či v obchodních kruzích běžně dostupné.
3. Pokud Dodavatel přijde do styku s osobními údaji, musí se řídit platnou legislativou na ochranu osobních údajů stanovenou výše.
4. Dodavatel může šířit informace o Předmětu plnění či o spolupráci s Nemocnicí (web, medializace Dodavatele, publikace, tisk apod.) jen s předchozím písemným souhlasem Nemocnice.

10. Porušení pravidel

1. Porušení těchto pravidel představuje porušení smlouvy uzavřené mezi Dodavatelem a Nemocnicí. Pokud Dodavatel poruší tato pravidla hrubým způsobem nebo opakovaně, je Nemocnice oprávněna odstoupit od smluvního vztahu s Dodavatelem. Nemocnice má pak nárok na náhradu veškeré škody, která jí vznikla v důsledku porušení pravidel Dodavatelem, které bylo důvodem pro odstoupení od smlouvy, tak i škody, která Nemocnici vznikne v důsledku skončení smluvního vztahu.

11. 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 řízení 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: 2024.01.03 09:44:48 +01'00'