Bezpečnostní požadavky pro dodavatele informačních a komunikačních technologií

1. Účel

1) Ústav hematologie a krevní transfuze (dále jen „ÚHKT“) od svých dodavatelů (dále jen „Dodavatel“) vyžaduje dodržování těchto bezpečnostních pravidel dodavatelů v oblasti bezpečnosti informací v souladu se souborem zásad a pravidel, které určují způsob zajištění ochrany aktiv (dále jen „Bezpečnostní politika“).

2) 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.

3) Dodavatel bere na vědomí, že ÚHKT bude poskytovatelem regulované služby v souladu s transpozicí Směrnice NIS2 a novou legislativou upravující kybernetickou a informační bezpečnost.

4) Dodavatel musí při plnění smluvního vztahu (dále jen „Předmět plnění“ nebo také jen „smlouva“) pro ÚHKT dodržovat níže uvedená pravidla.

5) Bezpečnostní pravidla musí být dodržována vždy, pokud je to technicky možné s ohledem na Předmět plnění, za využití maximálního úsilí ze strany Dodavatele.

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) ÚHKT výhradně prostřednictvím autentizačních údajů přidělených ÚHKT (např. VPN, IPSec).

3) Dodavatel se zavazuje dodržovat bezpečnostní opatření a pravidla ÚHKT při práci s informacemi a ICT prostředky ÚHKT.

4) Dodavatel se zavazuje upozorňovat ÚHKT včas na všechny hrozící vady svého plnění či potenciální výpadky nebo rizika plnění, jakož i poskytovat ÚHKT veškeré informace, které jsou pro plnění smlouvy nezbytné.

5) Dodavatel se zavazuje upozornit ÚHKT 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 ÚHKT 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.

10) Stanoví-li smlouva nebo zvlášť sjednaná smlouva o kybernetické bezpečnosti něco jiného něž tato pravidla, má ujednání ve smlouvě přednost. Nastane-li rozpor mezi smlouvou a zvlášť sjednanou smlouvu o kybernetické bezpečnosti, má přednost smlouva o kybernetické bezpečnosti.

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, poškození nebo odcizení hardware, software, dat, informací ÚHKT musí Dodavatel vždy neprodleně nahlásit tuto skutečnost oddělení informačních technologií ÚHKT, a to i v případě pouhého podezření na neoprávněný přístup a manipulaci s daty.

3) Dodavatel hlásí relevantní skutečnosti pro zajištění kybernetické a infomační bezpečnosti na technologické kontakty přímo uvedené ve smlouvě, pokud nejdou kontakty uvedneé ve smlouvě, hlásí tyto skutečnosti Dodavatel

4) Při práci na jakémkoli zařízení (například: počítači, notebooku, mobilním telefonu, zdravotnickém prostředku) připojeném do sítě a/nebo k informačním nebo komunikačním systémům ÚHKT musí Dodavatel dodržovat tyto zásady:

   a. umožnit přístup jen proškolenému a řádně nahlášenému zaměstnanci Dodavatele,

   b. chránit výpočetní techniku a všechna data ÚHKT před porušením důvěrnosti, integrity či dostupnosti primárních i podpůrných aktiv,

   c. po ukončení práce v síti a/nebo v informačním systému ÚHKT provést neprodleně odhlášení uživatele.

5) Při práci na serverech ÚHKT 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 informačních aktiv,

   b. Dodavatel nesmí měnit jakákoli oprávnění na serveru nebo informačním a komunikačním systému bez souhlasu oddělení informačních technologií ÚHKT,

   c. Dodavatel nesmí měnit nastavení operačního systému serverů a jeho komponent bez souhlasu oddělení informačních technologií ÚHKT,

   d. Dodavatel musí zajistit bezpečnostní aktualizaci operačního systému a aplikačních částí serverů; bezpečnostní aktualizace kritického charakteru, které mohou ohrozit bezpečnost sítě ÚHKT 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 oddělení informačních technologií ÚHKT.

6) Při práci v interní sítí ÚHKT odpovídají zaměstnanci Dodavatele, kteří mají přidělen přístup do interní sítě ÚHKT, 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 jakoukoli formou monitorování sítě, které může vést k zachycení dat, pokud není Předmětem plnění smlouvy,

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

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

h. užívat jakékoli programy, skripty nebo příkazy, nebo zasílat zprávy v jakékoli 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 příjemcem, 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 ÚHKT, pokud jsou takové informace nutné z hlediska přípravy či Předmětu plnění.

7) Za dodržování zákazů zaměstnanci Dodavatele uvedených v tomto článku odpovídá Dodavatel.

4. Kybernetické bezpečnostní události a incidenty

1) Dodavatel musí vyvinout maximální úsilí pro odvracení bezpečnostních hrozeb a kybernetických útoků pro informační a komunikační systémy ÚHKT.

2) Dodavatel musí zajistit maximální součinnost při analýze kybernetických bezpečnostních událostí a incidentů ÚHKT a následně zavádět vhodná nápravná opatření určená ÚHKT.

3) V případě podezření či potvrzení vzniku bezpečnostní hrozby pro informační a komunikační systém ÚHKT je Dodavatel povinen neprodleně písemně (e-mailem) či telefonicky (a následně také písemně) informovat o této skutečnosti Manažera kybernetické bezpečnosti ÚHKT.

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 ÚHKT.

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 primárních a podpůrných aktiv.

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 ÚHKT.*

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 ÚHKT (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

Ke každé dodávce musí existovat kromě účetních dokladů i předávací protokol podepsaný Dodavatelem a ÚHKT. 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 specifikována ve smlouvě s Dodavatelem. Chybějící, neúplná nebo neaktuální dokumentace je důvodem k reklamaci dodávky a v případě, že ji Dodavatel ve lhůtě stanovené ÚHKT 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 ÚHKT (např. datové centrum) není dovolen pohyb cizích osob bez dozoru zaměstnance ÚHKT.

3) Zaměstnanci Dodavatele mohou fyzicky přistupovat k ICT prostředkům ÚHKT pouze v doprovodu oprávněné osoby ÚHKT.

4) V případě práce Dodavatele v prostorách ÚHKT nebo v jím využívaných prostorách v datových centrech musí Dodavatel dále dodržovat tyto zásady:
   a. připojovat vlastní počítač, notebook pouze se souhlasem odpovědné osoby ÚHKT,
   b. v blízkosti ICT prostředků nejíst, nepít a nekouřit.

5) Dodavatel není oprávněn k výměně a odvozu použitých či vadných technologií bez autorizace ÚHKT.

8. Účast poddodavatelů

1) Dodavatel se zavazuje, že při poskytování plnění pro ÚHKT 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 ÚHKT.

2) Dodavatel nezapojí do poskytování plnění dle smlouvy žádného dalšího poddodavatele bez předchozího konkrétního písemného povolení ze strany ÚHKT.

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 ÚHKT, 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 ÚHKT, které se dozvěděl při dodávce Předmětu plnění, a to i po ukončení smluvního vztahu založeného smlouvou. Důvěrnou informací ÚHKT se rozumí informace obchodní, technické, know how, podklady a doklady, osobní údaje, zdravotnická dokumentace či jiné, které jsou významné pro ÚHKT 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 ÚHKT (web, medializace Dodavatele, publikace, tisk apod.) jen s předchozím písemným souhlasem ÚHKT.

10. Porušení pravidel

Porušení těchto pravidel představuje porušení smlouvy uzavřené mezi Dodavatelem a ÚHKT. Pokud Dodavatel poruší tato pravidla hrubým způsobem nebo opakovaně, je ÚHKT oprávněna odstoupit od smluvního vztahu s Dodavatelem. ÚHKT 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 ÚHKT vznikne v důsledku skončení smluvního vztahu.

11. Komunikační kanály

1) Dodavatel hlásí skutečnosti týkající se technických zranitelností na technologické kontakty přímo uvedené ve smlouvě.

2) Dodavatel hlásí skutečnosti týkající se řízení rizik Manažerovi kybernetické bezpečnosti vždy na e-mail mkb@uhkt.cz.

3) Dodavatel hlásí skutečnosti týkající se bezpečnostních incidentů Manažerovi kybernetické bezpečnosti na e-mail mkb@uhkt.cz.