SMLOUVA O POSKYTOVÁNÍ SLUŽEB TECHNICKÉ PODPORY

TIFIT s.r.o.

se sídlem:	Ocelářská 344/10, Praha 9, 190 00
zastoupený:	Ing. Michalem Chobotem, jednatelem
IČO:	24133604
DIČ:	CZ24133604
bankovní spojení:	Raiffeisenbank, Bělehradská 18, Praha 2
číslo účtu:	6417476001 / 5500

zapsána v obchodním rejstříku vedeném u Městského soudu v Praze, sp. zn. C 181657

jako poskytovatel na straně jedné (dále jen „poskytovatel“)

a

ÚSTAV HEMATOLOGIE A KREVNÍ TRANSFÚZE

se sídlem:	U Nemocnice 2094/1, 128 00 Praha 2
zastoupený:	prof. MUDr. Petrem Cetkovským, PhD., MBA, ředitelem
IČO:	00023736
DIČ:	CZ0023736
Bankovní spojení:	Česká národní banka
Číslo účtu:	31438021/0710

oprávněná osoba ve věcech smluvních: XXXXX
oprávněná osoba ve věcech technických: XXXXX

jako objednatel na straně druhé (dále jen „objednatel“)

(dále společně jen jako „smluvní strany“)

uzavírají dnešního dne, měsíce a roku dle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „z. č. 89/2012 Sb.“) a na základě vyhodnocení výsledků **výzvy č. 27/2025 v rámci dynamického nákupního systému dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění** (dále jen „z. č. 134/2016 Sb.“), **s názvem „DNS na IT “,** interní ev. č. VZ24019, ev. č. Z2024-039538, zavedeného dne 8.10.2024 (dále jen „veřejná zakázka“), tuto

smlouvu o poskytování služeb technické podpory (dále jen „Smlouva“):

čl. I

Předmět Smlouvy

1. Předmětem plnění této Smlouvy je zajištění prodloužení/obnova aplikační a technické podpory SW monitorovacího systému CheckMK na období 12 měsíců, a to od 8. 12. 2025 do 9. 12. 2026 (dále také jen „zajištění podpory“ nebo „podpora") pro Ústav hematologie a krevní transfuze na základě nabídky poskytovatele ze dne 7.11.2025 a dle specifikace v příloze č. 1 této smlouvy – Technická specifikace a cenová nabídka
2. Místem plnění je sídlo objednatele a dále jakékoli další pracoviště objednatele dle jeho písemného pokynu.
3. Objednatel a Poskytovatel se zavazují komunikovat ohledně předmětu plnění dle této smlouvy prostřednictvím těchto kontaktů:

Poskytovatel			
Jméno	**Funkce**	**Telefon**	**Email**
	jednatel		
Objednatel - Oprávněná osoba ve věcech technických			
Jméno	**Funkce**	**Telefon**	**Email**
	vedoucí odd. IT		
	správce IT		

čl. II

Cena a platební podmínky

1. Cena za předmět plnění dle čl. I odst. 1 a 2 této smlouvy je ceno smluvní je uvedena v příloze č. 1 smlouvy – Technická specifikace a cenová nabídka.
2. Cena zahrnuje veškeré náklady Poskytovatele související se splněním dotčených závazků a je stanovena jako konečná a nepřekročitelná.
3. K dohodnuté ceně bude připočtena sazba DPH platná ke dni uskutečnění příslušného zdanitelného plnění. Poskytovatel odpovídá za to, že sazba daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy.
4. Smluvní strany se dále dohodly, že cena předmětu plnění bude uhrazena jednorázovou platbou na základě faktury. Součástí faktury bude přiložený oboustranně podepsaný dodací list. Dodací list bude ze strany Objednatele potvrzen osobou oprávněnou ve věcech technických dle čl. I odst. 3 této smlouvy.
5. Faktura musí být správná, úplná průkazná, srozumitelná a musí obsahovat veškeré náležitosti dle předpisů o účetnictví, náležitosti dle daňových předpisů (§ 28 odst. 2 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů) a dále tyto údaje:
    a. číslo této smlouvy
    b. předmět plnění a jeho přesnou specifikaci,
    c. termín a místo plnění.

6. Faktura bude zaslána na adresu objednatele případně elektronicky na adresu: faktury@uhkt.cz. Splatnost faktury se sjednává v délce 30 kalendářních dnů ode dne doručení faktury objednateli.

7. Smluvní strany se dohodly, že na cenu předmětu plnění nebudou poskytovány zálohy. Smluvní strany se dohodly, že v případě, kdy faktura nebude obsahovat veškeré náležitosti nebo nebude doložena příslušnými písemnými potvrzeními, je objednatel oprávněn fakturu poskytovateli ve lhůtě její splatnosti vrátit. Oprávněným vrácením přestává běžet původní lhůta splatnosti s tím, že ode dne doručení opravené faktury běží nová splatnost.

8. Faktura se platí bankovním převodem na účet druhé smluvní strany uvedený na faktuře. Faktura se považuje za včas uhrazenou, pokud je fakturovaná částka odepsána z účtu objednatele nejpozději v den splatnosti faktury. V případě opožděné platby je objednatel povinen zaplatit poskytovateli zákonný úrok z prodlení.

čl. III

Práva a povinnosti smluvních stran

1. Poskytovatel je povinen poskytovat plnění dle čl. I této Smlouvy řádně, s odbornou péčí, v souladu s právními předpisy a s požadavky objednatele dle specifikace uvedené v příloze 1 této smlouvy.

2. Poskytovatel se zavazuje zachovávat mlčenlivost ve vztahu ke všem informacím a skutečnostem, které se dozví o objednateli, jeho zaměstnancích, pacientech atd. v souvislosti s uzavřením a plněním smlouvy, pokud tyto informace mají povahu obchodního tajemství, osobních údajů nebo mají být z jiných důvodů chráněny před zveřejněním. K mlčenlivosti v tomto rozsahu se zavazuje zavázat i své zaměstnance či jiné osoby, které použije k plnění této smlouvy. Poskytovatel je povinen nakládat s osobními údaji a zejména s údaji o zdravotním stavu, genetickými a biometrickými údaji v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 (GDPR) a příslušnými ustanoveními zákona č. 110/2019 Sb., o zpracování osobních údajů. Povinnost mlčenlivosti platí rovněž o skutečnostech, na něž se vztahuje povinnost mlčenlivosti zdravotnických pracovníků, zejména podle ustanovení § 51 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (Zákon o zdravotních službách), a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů.

3. Poskytovatel se zavazuje předávat objednateli bez zbytečného odkladu veškeré zprávy týkající se předmětu této smlouvy.

4. Objednatel je v případě vady podpory povinen vadu poskytovateli nahlásit na kontakt support@tifit.cz a uvést, jak se projevuje.

5. Objednatel je povinen bez zbytečného odkladu informovat poskytovatele o všech skutečnostech rozhodných pro poskytování služeb ve sjednaném rozsahu a poskytovat mu při tom potřebnou součinnost, podklady a informace.

6. Každá ze smluvních stran jmenuje oprávněnou osobu či oprávněné osoby v čl. I bodu 3. Oprávněné osoby budou zastupovat smluvní stranu ve smluvních a obchodních záležitostech souvisejících s plněním této Smlouvy. Oprávněné osoby nejsou oprávněny tuto Smlouvu měnit ani ji doplňovat.

čl. IV

Smluvní pokuty

1. V případě prodlení objednatele s úhradou řádně fakturované ceny je poskytovatel oprávněn požadovat zaplacení smluvního úroku z prodlení ve výši 0,01 % z nezaplacené částky za každý i započatý den prodlení.

2. Za nedodržení povinností dle podmínek uvedených v čl. III odst. 1 této Smlouvy poskytovatelem má objednatel právo účtovat smluvní pokutu ve výši 5.000, - Kč za každé jednotlivé porušení povinností.

3. Za nedodržení povinnosti dle podmínky v čl. V odst. 5 této smlouvy této smlouvy je povinen poskytovatel zaplatit smluvní pokutu ve výši pohledávky, která byla postoupena v rozporu s touto smlouvu. Objednatel má zároveň právo odstoupit od smlouvy.

4. Za porušení povinnosti mlčenlivosti podle čl. III odst. 2 této smlouvy se poskytovatel zavazuje zaplatit smluvní pokutu ve výši 50.000, - Kč, a to za každý jednotlivý případ porušení povinnosti.

5. V případě porušení povinností Bezpečnostních požadavků pro dodavatele informačních a komunikačních technologií dle přílohy č. 3 této smlouvy, je dodavatel/poskytovatel povinen uhradit zadavateli/objednateli smluvní pokutu ve výši 10.000 Kč za každé takové porušení.

6. Smluvní pokuta bude vyúčtována samostatným daňovým dokladem, splatnost smluvní pokuty činí 30 dnů ode dne doručení druhé smluvní straně.

čl. V
Ostatní ujednání

1. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této Smlouvy.

2. Smluvní strany jsou povinny plnit své závazky vyplývající z této Smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a s prodlením splatnosti jednotlivých peněžních závazků.

3. Poskytovatel je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů (zákon o finanční kontrole), osobou povinou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů.

4. Poskytovatel souhlasí se zveřejněním všech náležitostí smluvního vztahu včetně případných dodatků a výsledků zadávacího řízení na profilu objednatele nebo jiným způsobem, určeným objednatelem, jako přímo řízené organizace Ministerstva zdravotnictví a dále dle ustanovení § 219 odst. 1 písm. a) ZZVZ a dle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů, zákonem stanoveným způsobem.

5. Smluvní strany sjednávají, že pohledávku dle této Smlouvy nebo Smlouvu samotnou nelze postoupit třetí osobě bez předchozího písemného souhlasu druhé smluvní strany.

6. Smluvní strany této smlouvy se dohodly, že je poskytovatel, coby poskytovatel zdanitelného plnění, povinen bez zbytečného prodlení písemně informovat objednatele o tom, že se stal nespolehlivým plátcem ve smyslu ustanovení § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění (dále jen „zákon o DPH“). Smluvní strany si dále společně ujednaly, že pokud objednatel v průběhu platnosti tohoto smluvního vztahu na základě informace od poskytovatele či na základě vlastního šetření zjistí, že se poskytovatel stal nespolehlivým plátcem ve smyslu § 106a zákona o DPH, souhlasí obě smluvní strany s tím, že objednatel uhradí za poskytovatele daň z přidané hodnoty z takového zdanitelného plnění, dobrovolně správci daně dle § 109a citovaného právního předpisu. Zaplacení částky ve výši daně objednatelem správci daně pak bude cena dle této smlouvy smluvními stranami považováno za splnění závazku uhradit sjednanou cenu, resp. její část. Smluvní strany si v této souvislosti poskytnout veškerou nezbytnou součinnost při vzájemném poskytování informací požadovaných zákonem o DPH. Poskytovatel současně souhlasí s tím, že je povinen objednateli nahradit veškerou skutečnou škodu vzniklou v důsledku aplikace institutu ručení ze strany správce daně. Smluvní strany se dohodly, že objednatel bude hradit sjednanou cenu pouze na účet zaregistrovaný a zveřejněný ve smyslu § 96 odst. 1 zákona o DPH.

7. Poskytovatel si je vědom skutečnosti, že objednatel má zájem o realizaci předmětu této smlouvy v souladu se zásadami sociálně odpovědného zadávání veřejných zakázek. Poskytovatel se proto výslovně zavazuje zajistit dodržování pracovněprávních předpisů, zejména zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (se zvláštním zřetelem na regulaci odměňování, pracovní doby, doby odpočinku mezi směnami, placené přesčasy atp.), zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů (se zvláštním zřetelem na regulaci zaměstnávání cizinců), a dále předpisy týkající se zaměstnanosti a bezpečnosti a ochrany zdraví při práci vůči svým zaměstnancům. Poskytovatel prohlašuje, že jeho zaměstnanci jsou vedeni v příslušných registrech, například v registru pojištěnců ČSSZ, a mají příslušná povolení k pobytu v ČR. Poskytovatel se zavazuje vyvinout přiměřené úsilí k tomu, aby výše specifikované povinnosti byly plněny i ze strany jeho poddodavatelů. Poskytovatel je povinen zajistit řádné a včasné plnění finančních závazků svým poddodavatelům.

Čl. VI
Kybernetická bezpečnost

1. Poskytovatel bere na vědomí, že v rámci plnění předmětu této smlouvy bude v pozici významného dodavatele potom, co se objednatel stane poskytovatelem regulované služby (povinnou osobou) v souladu s transpozicí 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) a novou právní úpravou kybernetické a informační bezpečnosti. O tom, že se stane objednatel povinnou osobou podle právní úpravy kybernetické a informační bezpečnosti navazující na transpozici směrnice NIS, bude poskytovatele informovat.

2. Poskytovatel je povinen dodržovat a řídit se Bezpečnostními pravidly pro dodavatele v oblasti bezpečnosti informací, která jsou uvedena v příloze č. 3 této smlouvy.

3. Poskytovatel odpovídá za aktuálnost a pravdivost informací o zajištění kybernetické bezpečnosti, a to i poddodavatelů poskytovatele, které předložil před podpisem smlouvy. Tyto informace objednatel vyžaduje pro maximální přijatelné zajištění bezpečnosti dat a informací, které mohou být v rámci plnění smlouvy uloženy a zpracovány v ICT prostředí poskytovatele. Narušení bezpečnosti těchto dat a informací může mít potenciální dopad na provoz systému regulované služby objednatele, a tudíž může způsobit nedodržení povinností uložených právními předpisy upravujícími kybernetickou a informační bezpečnost.

4. Poskytovatel vyplnil povinnou přílohu č. 2 této smlouvy, ve které na jednotlivé otázky odpověděl ANO nebo NE, případně NEAPLIKOVATELNÉ tam, kde je to vhodné. Tabulka v příloze č. 2 této smlouvy je vyplněna poskytovatelem i každým jeho poddodavatelem separátně podle stavu bezpečnosti jejich prostředí ICT.

5. Poskytovatel je povinen nahlásit objednateli jakoukoliv změnu stavu bezpečnosti jeho ICT prostředí, zejména pak ty změny, které mohou mít negativní dopad na objednatele.

čl. VII
Závěrečná ustanovení

1. Pro případ, že se kterékoliv ustanovení této Smlouvy stane neplatným nebo neúčinným, zavazují se smluvní strany nahradit takové ustanovení bez zbytečného odkladu novým, které bude v nejvyšší možné míře odpovídat obsahu a účelu vadného ustanovení. Případná neplatnost některého z ustanovení této Smlouvy nemá za následek neplatnost ostatních ustanovení ve Smlouvě obsažených, pokud z povahy ustanovení nevyplývá, že tuto část nelze od ostatního obsahu této Smlouvy oddělit.

2. Smluvní strany jsou povinny bez zbytečného prodlení písemně informovat ostatní o jakékoliv změně v údajích uvedených ve Smlouvě ohledně jejich osoby a o všech okolnostech, které mají nebo by mohly mít vliv na plnění jejich povinností dle této Smlouvy a současně vyvinout potřebnou součinnost k plnění této Smlouvy.

3. Obsah této Smlouvy je možné měnit jen písemnými dodatky, podepsanými statutárními zástupci smluvních stran. Součástí této Smlouvy jsou veškeré přílohy uvedené v textu této Smlouvy či v textu případných Dodatků k této Smlouvě.

4. Smluvní strany se dohodly, že právní vztahy touto Smlouvou výslovně neupravené se řídí ustanoveními zákona č. 89/2012 Sb., občanského zákoníku, v platném znění.

5. Pro případ sporu vzniklého mezi smluvními stranami se v souladu s ustanovením § 89a zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů, sjednává jako místně příslušný obecný soud podle sídla objednatele.

6. Smluvní strany prohlašují, že tuto Smlouvu uzavřely na základě vážné a svobodné vůle, nikoliv v tísni za nápadně nevýhodných podmínek, ani nebyla jiným způsobem vynucena, dále prohlašují, že tuto Smlouvu pečlivě pročetly, jejímu obsahu zcela porozuměly a bezvýhradně s ním souhlasí a na důkaz toho připojují své vlastnoruční podpisy.

7. Smluvní vztah je možné ukončit:
   a. písemnou dohodou smluvních stran,
   b. odstoupením od smlouvy nebo její výpovědí v souladu s platnými právními předpisy.

8. Smluvní strana je oprávněna odstoupit od této smlouvy v případě podstatného porušení smlouvy druhou smluvní stranou, tzn. především v případech, kdy poskytovatel nebude plnit řádně a včas objednávky objednatele v dohodnutých termínech, nebude plnit ujednání o cenách, a dále v případně závažných nebo opakujících se vad, přestože byl objednatelem na neplnění podmínek dle této smlouvy písemně upozorněn.

9. Smluvní strany jsou oprávněny tuto smlouvu kdykoliv písemné vypovědět, a to i bez uvedení důvodu, formou doporučeného dopisu. Výpovědní lhůta v délce 3 měsíců začíná běžet 1. dnem měsíce následujícím po měsíci, ve kterém byla doručena výpověď smlouvy druhé smluvní straně.

10. Odstoupení od smlouvy nemá vliv na placení dohodnutých sankcí dle čl. IV této smlouvy a případných způsobených škod.

11. Tato Smlouva se uzavírá na dobu 12 měsíců.

12. Tato Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem uveřejnění v registru smluv

13. Tato Smlouva je vyhotovena ve 2 stejnopisech s platností originálu, z nichž každá ze smluvních stran obdrží Smlouvu v 1 vyhotovení, případně v jednom elektronickém originálu podepsaném kvalifikovaným elektronickým podpisem obou smluvních stran.

Přílohy:
Příloha 1- Technická specifikace a cenová nabídka
Příloha 2 – Hodnocení úrovně kybernetické bezpečnosti
Příloha 3 – Bezpečnostní pravidla pro dodavatele v oblasti bezpečnosti informací

V ……dne …… V Praze …… dne ……

…….
Ing. Michal Chobot, jednatel

…….
Mgr. Michal Tůma, MHA
náměstek pro provoz a investice

TECHNICKÁ SPECIFIKACE A CENOVÁ NABÍDKA:
veřejná zakázka VZ24019-27 - Výzva č. 27/2025 Zajištění předplatného SW TeamViewer

Název položky	Počet licencí/ let	Cena v Kč bez DPH za 1 licenci	Celková cena v Kč bez DPH	DPH (%)	Výše DPH v Kč	Celková cena v Kč vč. DPH
Licence pro Checkmk Enterprise na 12 měsíců						
Rešení infrastrukturního a aplikačnímu monitoringu pro min. 18 000 zařízení/ min. 18 000 služeb na 12 měsíců včetně podpory výrobce	**1**			21%		
CENA CELKEM			**147 000,00 Kč**	21%	**30 870,00 Kč**	**177 870,00 Kč**

Popis	**Sériové číslo**
Checkmk Enterprise	CU46838
Specifikace	
celková kapacita 18 000 zařízení / služeb	
Neomezený počet hostitelů, instancí a uživatelů	
Nasazení: stažení z checkmk.com.	
Podpora: 8 hodin x 5 dní.	
Technická podpora • zajištění nových verzí nebo subverzí programového systému s vyšší nebo upravenou funkcionalitou na základě kontinuálního vývoje programového vybavení, • odstraňování vad programového vybavení, • průběžná aktualizace veškeré dokumentace vztahující se k programovému vybavení, • konzultace a telefonická podpora v českém jazyce při řešení problémů souvisejících s provozem a funkčností programového vybavení.	
Období: 12 měsíců	

Pozn. Zadavatele: Jedná se o licence dle původního licenčního modelu.

Účastník doplní žlutě podbarvená pole.

Příloha č. 6 Výzvy VZ24019-27

Hodnocení úrovně kybernetické bezpečnosti

Dodavatel postupuje:
1. Dodavatel odpoví na všechny otázky, kromě oddílu E, který není povinný.
2. V případě zvolení možnosti Neaplikovatelné, dodavatel vyplní pole komentář, ve kterém poskytne zdůvodnění.
3. Dodavatel vyplňuje pouze sloupce D, případně E.

Číslo	Otázka	Odpověď	Komentář
	Oddíl A - Standardy a nejlepší praktiky		
1.	Jaké standardy a nejlepší praktiky dodavatel aplikuje v rámci svých činností:		
a.	ISO 9001	Ano	
b.	ISO/IEC 27001	Ano	
c.	ISO 22301	Ano	
d.	ISO/IEC 200000-1, ITIL, CobIT	Ano	
	Oddíl B - Obecná bezpečnostní opatření		
2.	Má dodavatel manažera kybernetické bezpečnosti, nebo jinou roli odpovědnou za kybernetickou bezpečnost?	Ano	
3.	Byl u dodavatele v posledních 12ti měsících proveden třetí nezávislou stranou audit či analýza, jejichz obsahem byla kontrola v oblasti kybernetické bezpečnosti?	Ne	
4.	Provedl dodavatel v posledních 12ti měsících hodnocení rizik v oblasti kybernetické bezpečnosti?	Ano	
5.	Má dodavatel zavedenou bezpečnostní politiku, obsahující pravidla, procesy a bezpečnostní opatření v oblasti bezpečného zpracovávání informací a poskytování slu	Ano	
6.	V případě, že má dodavatel zavedenou bezpečnostní politiku, které oblasti jsou v ní pokryty?		
a.	Řízení aktiv a rizik	Ano	
b.	Ochrana dat proti prozrazení, zničení, narušení integrity a dostupnosti	Ano	
c.	Ochrana osobních dat	Ano	
d.	Identifikace a autentizace uživatelů	Ano	
e.	Přístup k datům na základě rolí (RBAC, Role Based Access Control)	Ano	
f.	Řízení privilegovaných přístupů	Ano	
g.	Ochrana koncových stanic	Ano	
h.	Ochrana mobilních zařízení a vzdáleného přístupu	Ano	
i.	Ochrana emailu a vnitrofiremní komunikace (instant messaging)	Ano	
j.	Ochrana přístupu do internetu	Ano	
k.	Ochrana médií	Ano	
l.	Řízení změn	Ano	
m.	Ochrana bezdrátových sítí a komunikace	Ano	
n.	Fyzická bezpečnost informačních aktiv	Ano	
o.	Bezpečnostní školení koncových uživatelů a administrátorů	Ano	
p.	Ochrana proti škodlivému softwaru	Ano	
q.	Ochrana při výměně dat	Ano	
r.	Zvládání kybernetických bezpečnostních událostí a incidentů	Ano	
s.	Řízení rizik dodavatelů	Ano	
t.	Bezpečnost lidských zdrojů	Ano	
u.	Bezpečnostní audity a analýzy	Ano	
v.	Řízení kontinuity činností a havarijní plánování	Ano	
	Oddíl C - Bezpečnostní technologie		
7.	Které níže uvedené bezpečnostní technologie dodavatel provozuje s cílem předcházet bezpečnostním hrozbám ve vztahu k datům a informačním systémům?		
a.	Antivirový software na koncových stanicích	Ano	
b.	Antivirový software na mobilních zařízeních	Ano	
c.	Nástroj pro detekci narušení sítě (IDS/IPS, Intrusion Detection/Prevention System)	Ano	
d.	Nástroj pro řízení privilegovaných účtů a oprávnění (PIM/PAM, Priviledge Identity/Access Management)	Ano	
e.	Více-faktorová autentizace	Ano	

f.	Automatizovaný nástroj pro řízení technologických zranitelností (VMS)	Ano	
g.	Nástroj pro řízení přístupu k síti (NAC, Network Access Control)	Ano	
h.	Ochrana před útoky DDoS (Distributed denial-of-service)	Ano	
i.	Firewall	Ano	
j.	Nástroj pro vyhodnocování bezpečnostních událostí (SIEM, Security Informaton and Event Management)	Ano	
k.	Nástroj pro ochranu před únikem dat (DLP)	Ano	
8.	Byly interní systémy dodavatele v posledních 12ti měsících podrobeny penetračnímu testování?	Ano	
Oddíl C - Zvládání kybernetických bezpečnostních událostí a incidentů			
9.	Má dodavatel zaveveden proces zvládání kybernetických bezpečnostních událostí a incidentů?	Ano	
10.	Jsou všichni zaměstnanci dodavatele pravidelně (min. 1x za 24 měsíců) vzdělávání v identifikaci kybernetických bezpečnostních událostí a incidentů?	Ano	
Oddíl D - Zvyšování povědomí			
11.	Má dodavatel zaveden proces vzdělávání a zvyšování bezpečnostního povědomí pro zaměstnance?	Ano	
12.	Jsou noví zaměstnanci dodavatele vyškoleni v oblasti bezpečnosti informací dříve, než získají přístup k datům a informačním systémům?	Ano	
13.	Dokumentuje dodavatel účast pracovníků na bezpečnostních školeních a vzdělávacích programech?	Ne	
14.	Vyžaduje dodavatel po zaměstnancích s přístupem k datům a informačním systémům podepsání individuální dohody o mlčenlivosti?	Ano	
Oddíl E - Poznání organizace - nepovinné			
15.	Je dodavatel orgánem nebo osobou povinnou dle §3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti?	Ne	
16.	Má dodavatel zaveden certifikovaný systém řízení dle ISO/IEC 27001?	Ano	
17.	Jsou poddodavatelé dodavatele vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům?	Ano	
18.	Vyžaduje dodavatel po pracovnících dodavatele s přístupem k datům a informačním systémům podepsání individuální dohody o mlčenlivosti?	Ano	
19.	Jaké negativní dopady pocítil dodavatel v souvislosti s kybernetickou bezpečnostní událostí nebo incidentem, pokud v minulosti nastaly:		
a.	Výpadek sítě	Ne	
b.	Nedostupnost emailu a kancelářských aplikací	Ne	
c.	Neoprávněné zneužití identity	Ne	
d.	Prozrazení chráněných dat	Ne	
e.	Ztráta nebo zničení dat	Ne	
f.	Finanční ztráta	Ne	
g.	Ztráta duševního vlastnictví	Ne	
h.	Poškození pověsti organizace	Ne	
i.	Negativní publicita v médiích	Ne	

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 požadavků pro dodavatele informačních a komunikačních technologií 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 požadavky 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 jakémkoliv 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 jakákoliv 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 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 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
    a. 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

1. 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.