SERVISNÍ SMLOUVA číslo 360526

uzavřená podle § 1746 odst. (2) zákona č. 89/2012 Sb., Občanského zákoníku

I.
Smluvní strany

1. **Objednatel:**

   Zdravotnická záchranná služba Jihočeského kraje
   se sídlem: B. Němcové 1931/6, 370 01 České Budějovice
   jednající: MUDr. Jakub Jan Hájek, MBA, ředitel
   IČ: 481 999 31
   bankovní spojení: ČSOB, a.s.
   č.ú.: 234602215/0300
   (dále jen „objednatel“)

2. **Zhotovitel:**
   APENEX, s.r.o.
   se sídlem: Boženy Němcové 66, 370 01 Č. Budějovice
   jednající: Ing. Petr Petr, MBA
   IČ: 26102692
   DIČ: CZ26102692
   bankovní spojení: Československá obchodní banka, a. s.
   č.ú.: 254861468/0300
   (dále jen „zhotovitel“)

II.
Předmět smlouvy

Touto smlouvou se zhotovitel zavazuje provádět servisní činnost (činnost směřující k odstranění závady či poruchy) na zařízeních objednatele uvedených v příloze č. 1 této smlouvy v rozsahu stanoveném v příloze č. 2 této smlouvy (dále jen „servisní činnost“), a objednatel se zavazuje hradit za to zhotoviteli cenu sjednanou v této smlouvě.

III.
Způsob provádění servisní činnosti

1. Zhotovitel bude provádět servisní činnost vždy na výzvu objednatele uplatněnou u zhotovitele telefonicky buď telefonicky na čísle ***386321354*** nebo prostřednictvím e-mailové adresy info@apenex.cz

2. Objednatel je povinen při nahlášení požadavku na servisní činnost uvést potřebné informace o povaze vyžádaného servisního zásahu a kontaktní údaje na vyřizující osobu oprávněnou za objednatele ve věci servisního zásahu jednat.

3. Zhotovitel je povinen zahájit servisní činnost v reakční době, jejíž délky jsou rozlišeny podle priority poruchy a jsou stanoveny v příloze č. 2 této smlouvy. Priority poruch se pro účely této smlouvy dělí do těchto kategorií:

Porucha – priorita 1 – výpadek základních funkcí systému, například výpadek zdroje, celé části zařízení nebo kompletní výpadek provozu systému, nebo jakékoli části omezující provoz tísňové linky 155.
Porucha – priorita 2 – závažná chyba, která způsobí nečinnost některých částí systému (například výpadek karty s účastnickými porty), avšak nedosahuje intenzity priority 1.
Porucha – priorita 3 – ostatní chyby.

4. Prioritu poruchy a způsob jejího odstranění určuje po konzultaci s objednatelem zhotovitel, který je sdělí objednateli. Zhotovitel objednateli rovněž sdělí, jaké jednotlivé činnosti je třeba k odstranění poruchy vykonat, a jejich posloupnost.

5. V těch případech, kdy zhotovitel zajistí pouze náhradní provoz servisovaného zařízení, zavazuje se provést jeho opravu v nejkratší možné lhůtě, nejdéle však do 14 (čtrnácti) dnů od převzetí vadného dílu servisovaného zařízení. V případě, kdy zhotovitel provede opravu servisovaného zařízení výměnným způsobem (výměna vadného servisovaného zařízení, jeho části nebo jednotlivého dílu, za nové bezvadné servisované zařízení, jeho část nebo jednotlivý díl), přechází vlastnictví k vadnému servisovanému zařízení, jeho části či jednotlivému dílu na zhotovitele.

6. Po odstranění poruchy bude vyřizující osobou jednající za objednatele a zhotovitelem sepsán „Protokol o provedení servisní činnosti“. Datum a hodina podpisu tohoto protokolu představuje údaj o termínu splnění smluvního závazku ze strany zhotovitele. Odmítne-li objednatel podepsat přes výzvu zhotovitele Protokol, nastanou účinky splnění závazku zhotovitele okamžikem odmítnutí.

IV.
Cena a platební podmínky

1. Celková měsíční cena za provádění servisní činnosti dle této smlouvy činí částku **22.000 Kč**. Cena je splatná do 10. dne následujícího kalendářního měsíce.

2. Smluvní strany se dohodly, že zhotovitel je oprávněn po uplynutí prvního celého kalendářního roku účinnosti smlouvy požadovat každoročně vždy v 1. čtvrtletí kalendářního roku zvýšení ceny o částku odpovídající průměrné roční míře inflace v předchozím kalendářním roce zveřejněné Českým statistickým úřadem.

3. Pokud dojde k poruše servisovaného zařízení v důsledku úmyslného nebo nedbalostního porušení nebo nedodržení provozních či záručních podmínek ze strany objednatele, jeho zaměstnanců nebo třetích osob (zaviněná porucha) nebo v důsledku zásahu tzv. vyšší moci (např. vandalství, terorismus, válka, občanské nepokoje, požáry, povodně a jiné živelné události, výbuchy, úniky chemických a radioaktivních materiálů a podobně) je objednatel povinen uhradit zhotoviteli vedle paušální částky dle čl. IV odst.1 smlouvy i náklady spojené s provedením servisní činnosti směřující k odstranění takto vzniklé poruchy (náklady na práci servisního technika, cenu spotřebovaného materiálu a náhradních dílů, jakož i všechny ostatní účelně vynaložené náklady), a to podle aktuálního ceníku zhotovitele účinného ke dni objednání servisního zásahu.

4. Servisní činnosti nespadající do předmětu této smlouvy vyúčtuje zhotovitel objednateli vedle paušální částky dle čl. IV. odst. 1 smlouvy, a to podle aktuálního ceníku zhotovitele účinného ke dni objednání servisního zásahu.

5. Cena účtovaná vedle paušální částky je splatná vždy do 14 dnů ode dne provedení činnosti, k níž se cena váže.

6. Ke každé části ceny bude připočtena DPH podle platné právní úpravy. Aktuální ceník zhotovitele je vždy vyvěšen na webových stránkách zhotovitele. Na každou část ceny vystaví zhotovitel fakturu mající zákonné náležitosti daňového dokladu. Faktury zhotovitele mohou být zasílány objednateli elektronicky, formou přílohy e-mailové zprávy zaslané za adresu objednatele sekretariat@zzsjck.cz.

7. V případě prodlení objednatele s úhradou ceny je objednatel povinen uhradit zhotoviteli smluvní pokutu ve výši 0,05 % z dlužné částky za každý den prodlení. V případě prodlení delšího než 30 dnů nebo v případě prodlení s částkou vyšší než 20.000 Kč je zhotovitel oprávněn objednateli oznámit, že přerušuje plnění této smlouvy; to však nemá vliv na povinnost objednatele hradit paušální částku dle čl. IV.1.

V.
Práva a povinnosti stran

1. Programy poskytnuté zhotovitelem v rámci provádění servisní činnosti není objednatel oprávněn měnit, rozmnožovat ani poskytovat třetím osobám.

2. Objednatel je povinen:
   a) zajistit, aby veškeré zásahy na servisovaném zařízení byly prováděny jen prostřednictvím zhotovitele nebo prostřednictvím subjektů, které od zhotovitele k takovým pracím mají písemný souhlas
   b) poskytnout zhotoviteli nezbytnou součinnost a veškeré potřebné informace, které mohou pomoci při odstraňování poruch, které jsou objednateli známy a o které zhotovitel požádá;
   c) dle pokynů zhotovitele provést opatření, která pomohou upřesnit diagnózu a urychlit provedení servisní činnosti, zejména bude-li nutné, umožnit vzdálený přístup do servisovaných zařízení;
   d) zajistit bezodkladný a dostatečný přístup k zařízením vyžadujícím opravu;
   e) informovat včas zhotovitele o neobvyklé funkčnosti servisovaného zařízení a o příznacích poruch, které by signalizovaly budoucí poruchu;
   f) seznámit se s provozními a záručními podmínkami všech servisovaných zařízení a dodržovat je;
   g) umožnit zhotoviteli zajištění dálkového dohledu, pokud je toto předmětem smlouvy;
   h) poskytnout zhotoviteli veškerou další nezbytnou součinnost.

3. V případě prodlení objednatele se splněním kterékoliv své povinnosti stanovené v předchozím odstavci se nemůže zhotovitel dostat do prodlení s plněním svého závazku. Zhotovitel je v takovém případě oprávněn oznámit objednateli, že přerušuje či nezahájí svou servisní činnost do doby splnění povinnosti objednatele. Zároveň je objednatel povinen uhradit zhotoviteli zvýšené náklady spojené s odstraněním poruchy.

4. Zhotovitel je povinen provádět servisní činnost podle této smlouvy ve stanoveném rozsahu a v příslušných časových limitech a zajistit řádnou obsluhu komunikačních kanálů určených pro hlášení poruchy. Dále je zhotovitel povinen provádět servis zařízení podle platných právních předpisů a řádně zaškoleným personálem.

5. Zhotovitel neručí za nesplnění nebo zpožděné splnění svých povinností, pokud mu v tom dočasně nebo trvale zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli (tzv. vyšší moc).

6. Smluvní strany se zavazují zachovávat mlčenlivost o všech důvěrných informacích, které získaly v souvislosti s touto smlouvou, a to až do doby, než tyto informace ztratí význam nebo důvěrný charakter, nebo vejdou v obecnou známost jinak než prozrazením jednou ze smluvních stran. Smluvní strany jsou tímto ustanovením vázány i po ukončení této smlouvy.

VI.
Kybernetická bezpečnost

1. Zhotovitel bere na vědomí, že Objednatel je poskytovatelem regulované služby v režimu vyšších povinností dle zákona č. 264/2025 Sb., o kybernetické bezpečnosti a plní povinnosti vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních.

2. Zhotovitel je povinen dodržovat Kybernetické bezpečnostní požadavky pro technická aktiva, která jsou uvedena jako příloha č. 3 smlouvy.

3. Zhotovitel je povinen neprodleně informovat Objednatele o jakémkoli bezpečnostním incidentu souvisejícím s plněním smlouvy.

VII.
Sankce

1. Za každý případ závažného porušení pravidel kybernetické bezpečnosti dle čl. VI je zhotovitel povinen uhradit smluvní pokutu ve výši 50.000 Kč

VIII.
Účinnost smlouvy a její trvání

1. Smlouva se uzavírá na dobu neurčitou.

2. Každá ze stran může tuto smlouvu vypovědět i bez udání důvodu ve výpovědní lhůtě 3 kalendářních měsíců, a to písemnou výpovědí adresovanou druhé smluvní straně. Výpovědní lhůta počíná běžet od prvního dne následujícího měsíce po doručení výpovědi druhé smluvní straně.

3. Zhotovitel má právo vypovědět tuto smlouvu bez výpovědní lhůty (s účinky ke dni doručení) v případě, že objednatel nezaplatí cenu dle čl. IV. ani ve lhůtě dalších 30-ti (*třiceti*) dnů po splatnosti jakékoliv její části.

4. Objednatel má právo vypovědět tuto smlouvu bez výpovědní lhůty v případě opakovaného nedodržování stanovených časových limitů k odstranění poruchy ze strany zhotovitele.

5. V případě ukončení této smlouvy výpovědí bez výpovědní lhůty náleží zhotoviteli poměrná část ceny za měsíc, v němž k výpovědi došlo.

IX.
Závěrečná ujednání

1. Tato smlouva je vyhotovena ve dvou stejnopisech, z nichž každá smluvní strana obdrží po jednom.

2. Tato smlouva může být měněna pouze písemnými dodatky podepsanými oběma smluvními stranami.

3. Tato smlouva nabývá platnosti dnem jejího podpisu smluvními stranami a účinnosti dnem jejího uveřejnění v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), v platném znění. Objednatel je povinným subjektem, na jehož smlouvy se vztahuje povinnost uveřejnění v registru smluv.

4. V ostatním se právní vztahy smluvních stran řídí Občanským zákoníkem, jakož i ostatními obecně závaznými právními předpisy.

5. Nedílnou součástí této smlouvy jsou její přílohy. Ke dni uzavření této smlouvy jsou jejími přílohami:

Příloha č. 1	Technická specifikace předmětu plnění objednatele
Příloha č. 2	Seznam servisní činnosti
Příloha č. 3	Kybernetické bezpečnostní požadavky pro technická aktiva

V Českých Budějovicích dne 4.6.2026

Za Objednatele:

MUDr. Jakub Jan Hájek, MBA
Ředitel ZZS JčK

V Českých Budějovicích dne

Za Zhotovitele:

Ing. Petr Petr
Jednatel

PŘÍLOHA Č. 1_TECHNICKÁ SPECIFIKACE

Servis telefonní ústředny

Seznam modulů ústředny

Základní systém, řízení		
1	L30220-Y600-G300	**OpenScape/HiPath 4000 Basic System**
1	L30220-Y600-G335	**OpenScape EcoServer 2 Simplex**
1	L30220-Y600-G336	**OpenScape EcoServer 2 Duplex**
2		**Systém box AP37013**
2	L30220-Y600-K253	**Digital User Connections (SLMO24), Slot for Provided Locally**
2	L30220-Y600-A387	**Subscriber Line Module Analog with MWI (SLMAV, 24 Ports)**
1	L30220-Y600-K212	**Trunk Module, 2-Wire, Loop Table 50Hz/16kHz (TM2LP)**
3	L30220-Y600-K231	**Digital Interface Unit for S2 PRI Network/Exchange Interface (DIUN2),**
2	L30220-Y600-A428	**HG 3500 V8 (120 Channels)**
2		**HG3500-STMI**
OpenScape 4000 licence		
1	L30220-G622-A100	**OpenScape 4000 V10 System Base License for EcoServer, VM, Branch/EcoBranch**
1	L30220-G622-A101	**OpenScape 4000 V10 Duplex License**
1	L30220-G622-A110	**OpenScape 4000 V10 SLES Upgrade Protection initial for 6 years**
220	L30220-G622-A121	**OpenScape 4000 V10 Flex User License**
60		**FlexLicence SIP OpenScape4000**
Integrace stávajícího informačního systému operačního řízení ZZS JČK telefonní ústřednou řady OpenScape4000		
1		**OpenScape4000 CSTA interface**
1		**CTSA interface informačního systému operačního řízení ZZS JČK**

Parametry na SLA

Pracovní doba pro servisní zásahy

Pondělí až neděle 0:00-24:00	

Reakční doba	**Hod.**
Priorita1	**2 hodiny**
Priorita2	**8 hodin**
Priorita3	**48 hodin**
Změny konfigurace	**Max. 48 hodin**

Náhradní díly

Garance dodání náhradních dílů do 8 hodin od objednání	

Rozsah práce na zařízení

Rozsah standardních servisních prací servisního technika měsíčně	**5 hodin**
Preventivní údržba (kontrola a údržba zařízení)	**čtvrtletně**
Zálohování dat celého systému	**čtvrtletně**
Vzdálený dohled (pravidelná kontrola zařízení přes modem, konfigurace a servis přes modem)	**Max. 2 hod./měsíc**
Telefonická podpora	**pondělí - neděle v době 0:00-24:00**

PŘÍLOHA Č. 2_SEZNAM SERVISNÍ ČINNOSTI

Pracovní doba pro servisní zásahy	
Opravy systému (pokrývá veškeré opravy HW i SW částí systému PBX a ostatních aplikací k systému, výměnu vadných HW dílů, obnova systému, reinstalace softwarových aplikací)	***pondělí - neděle v době 0:00-24:00***
Reakční doba	**Hod.**
Priorita1	**2 hodiny**
Priorita2	**8 hodin**
Priorita3	**48 hodin**
Změny konfigurace	**Max. 48 hodin**
Náhradní díly	
Dostupnost náhradních dílů (skladem u dodavatele)	
Analýza vadných HW dílů, doprava na místo, výměna a konfigurace - vše zdarma	
Dodání náhradních dílů součástí smlouvy, náhradní díly hrazeny nad rámec měsíčního paušálu	
Rozsah práce na zařízení	
Rozsah standardních servisních prací servisního technika měsíčně Vytvoření, změna nebo zrušení: • služby (Konference, opakování vol-by/Redial, zpětné volání/Callback, pře-směrování hovoru/Call Forwarding, upozornění na čekající hovor/Call Wai-ting, nerušit/Do not Disturb), • pobočky, • pojmenování pobočky, • tlačítka (jméno tlačítka, nastavení zkrácené volby, nastavení funkce na tlačítko) • skupiny (pick-up skupiny, hunting group) • hudby v přidržení (music on hold) • seznam zkrácených voleb (speed dial list) • šéf sekretářské soupravy.	**5 hodin/měsíc**
Preventivní údržba (kontrola a údržba zařízení) - činnosti viz. výkaz práce	***čtvrtletně***
Zálohování dat celého systému	***čtvrtletně***
Vzdálený dohled (pravidelná kontrola systému přes modem/VPN, kontroly na vyžádání, změny na vyžádání technická podpora lokálního správce systému)	**Max. v rozsahu standardních servisních činností**
Telefonická podpora	***pondělí - neděle v době 0:00-24:00***
Cena za hodinu servisních činností nad rámec smlouvy	**1.400 Kč/hod.**

PŘÍLOHA Č. 3_KYBERNETICKÉ BEZPEČNOSTNÍ POŽADAVKY PRO TECHNICKÁ AKTIVA

1. Účel

1. Zdravotnická záchranná služba Jihočeského kraje (dále jen „ZZS JčK“) od svých dodavatelů (dále jen „Dodavatel“) vyžaduje dodržování těchto Kybernetických bezpečnostních požadavků pro technická aktiva.

2. Dodavatel (pro účely Smlouvy Prodávající či Zhotovitel) bere na vědomí, že ZZS JčK je poskytovatel regulované služby v oblasti poskytování zdravotních služeb v režimu vyšších povinností dle zákona č. 264/2025 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

3. Dodavatel musí při plnění smluvního vztahu (dále jen „Předmět plnění“) pro ZZS JčK dodržovat níže uvedené požadavky.

4. Dodavatel musí dodržovat tyto Kybernetické bezpečnostní požadavky pro technická aktiva vždy, pokud je to technicky možné.

2. Definice a legislativní rámec

1. Technickým aktivem se dle §2 odst. 1 zákona č. 264/2025 Sb. rozumí technický prostředek, programový prostředek nebo vybavení, které je součástí regulované služby nebo napomáhá jejímu poskytování. Technickým aktivem je zejména hardware, software, firmware, síťové prvky, úložiště dat a další technologické komponenty tvořící informační a komunikační infrastrukturu ZZS JčK.

2. ZZS JčK je poskytovatelem regulované služby v režimu vyšších povinností dle zákona č. 264/2025 Sb., o kybernetické bezpečnosti. Bezpečnostní opatření uvedená v tomto dokumentu vycházejí z vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. Dodavatel je povinen tyto požadavky zohlednit při plnění smluvního vztahu se ZZS JčK.

3. 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 ZZS JčK včas na všechny hrozící vady svého plnění či potenciální výpadky nebo rizika plnění, jakož i poskytovat ZZS JčK veškeré informace, které jsou pro plnění smlouvy nezbytné

3. Dodavatel se zavazuje upozornit ZZS JčK 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, ve znění pozdějších předpisů.

6. Náklady, které je třeba vynaložit na zavedení bezpečnostních požadavků, nese Dodavatel.

4. 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 ZZS JčK musí Dodavatel vždy neprodleně nahlásit tuto skutečnost odboru ICT ZZS JčK, a to i v případě pouhého podezření neoprávněný přístup a manipulaci s daty.

3. Dodavatel hlásí skutečnosti OIKT ZZS JčK vždy na e-mail: it@zzsjck.cz. 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 ZZS JčK musí Dodavatel dodržovat tyto zásady:

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

    b) chránit výpočetní techniku a všechna data ZZS JčK před porušením důvěrnosti, integrity či dostupnosti,

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

5. Při práci na serverech ZZS JčK 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 OIKT ZZS JčK,

    c) dodavatel nesmí měnit nastavení operačního systému serverů a jeho komponent bez souhlasu OIKT ZZS JčK,

    d) dodavatel musí zajistit bezpečnostní aktualizaci operačního systému a aplikačních částí serverů; bezpečnostní aktualizace kritického charakteru, které mohou ohrozit bezpečnost sítě ZZS JčK 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 OIKT ZZS JčK

6. Při práci v interní sítí ZZS JčK odpovídají zaměstnanci Dodavatele, kteří mají přidělen přístup do interní sítě ZZS JčK, 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) 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,

h) 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),

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

5. Kybernetické bezpečnostní události a incidenty

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

2. Dodavatel musí zajistit maximální součinnost při analýze kybernetických bezpečnostních událostí a incidentů ZZS JčK a následně zavádět vhodná nápravná opatření určené ZZS JčK.

3. V případě podezření či potvrzení vzniku bezpečnostní hrozby pro informační a komunikační systém ZZS JčK je dodavatel povinen neprodleně písemně (e-mailem) informovat o této skutečnosti Manažera kybernetické bezpečnosti ZZS JčK.

4. V případě že se dodavatel stane obětí kybernetického útoku musí tuto skutečnost neprodleně nahlásit písemně (e-mailem) OIKT ZZS JčK.

6. 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) Dodavatel musí v dodávaných informačních systémech zajistit heslovou politiku.:

i. uživatelské účty: minimální délka hesla 12 znaků;

ii. administrátorské účty: minimální délka hesla 17 znaků;

iii. technická aktiva a servisní účty: minimální délka hesla 22 znaků;

iv. break-glass (nouzové) účty: minimální délka 22 znaků, náhodně generovaný řetězec;

v. systém musí umožňovat zadání hesla o délce minimálně 64 znaků;

vi. vynucená změna hesla minimálně jednou za 18 měsíců;

vii. paměť 12 předchozích hesel (zákaz opakování).

d) Cílovým stavem je zavedení vícefaktorové autentizace (MFA) pro všechny přístupy. Do doby plného nasazení MFA platí výše uvedená heslová politika.

e) 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.

f) 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.

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

2. V informačních systémech musí být pořizovány auditní záznamy. Záznamy musí obsahovat minimálně:

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 ZZS JčK.

3. Auditní záznamy musí být uchovávány po dobu minimálně 18 měsíců. Záznamy musí být chráněny proti neoprávněné manipulaci, smazání nebo změně.

4. Informační systém musí umožňovat automatické odesílání logů do centrálního systému pro správu bezpečnostních informací a událostí (SIEM) ZZS JčK prostřednictvím standardizovaných protokolů (syslog, CEF, LEEF nebo obdobný formát).

5. Řízení přístupu k informačním systémům

a) Každý uživatel musí být identifikován a autentizován při přístupu k informačnímu systému.

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 ZZS JčK (LDAP, AD, atd..)

6. 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.

7. 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.

7. 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 ZZS JčK. 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 ZZS JčK 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.

8. Kryptografické prostředky

1. Dodavatel musí při plnění smluvního vztahu zajistit použití výhradně aktuálně odolných kryptografických algoritmů a protokolů. Dodavatel je zejména povinen:

a) používat pro šifrování komunikace minimálně protokol TLS verze 1.2, přičemž je doporučen TLS 1.3;

b) nepoužívat kryptografické algoritmy označené jako zastaralé nebo nedostatečně odolné (zejména MD5, SHA-1, DES, 3DES, RC4);

c) pro symetrické šifrování používat minimálně AES-128, doporučen AES-256;

d) pro asymetrické šifrování používat minimálně RSA 2048 bitů nebo ekvivalent na eliptických křivkách (ECDSA P-256 a vyšší);

e) pro hašování používat minimálně SHA-256;

f) řídit se aktuálními doporučeními NÚKIB pro oblast kryptografických prostředků.

2. Dodavatel je povinen v rámci Předmětu plnění doložit seznam použitých kryptografických algoritmů a protokolů. V případě zjištění nedostatečné odolnosti použitého algoritmu je Dodavatel povinen zajistit migraci na odolnější algoritmus v přiměřené lhůtě stanovené ZZS JčK.

9. 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 ZZS JčK (např. datové centrum) není dovolen pohyb cizích osob bez dozoru zaměstnance ZZS JčK.

3. Zaměstnanci Dodavatele mohou fyzicky přistupovat k ICT prostředkům ZZS JčK pouze v doprovodu oprávněné osoby ZZS JčK.

4. V případě práce Dodavatele v prostorách ZZS JčK nebo v jím využívaných prostorách v datových centrech musí Dodavatel dále dodržovat tyto zásady:

    a) připojovat vlastní počítač, notebook pouze se souhlasem odpovědné osoby ZZS JčK,

    b) v blízkosti ICT prostředků nejíst, nepít a nekouřit.

5. Dodavatel není oprávněn k výměně a odvozu použitých či vadných technologií bez autorizace ZZS JčK.

10. Účast poddodavatelů

1. Dodavatel se zavazuje, že při poskytování plnění pro ZZS JčK 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 ZZS JčK.

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

3. Pokud Dodavatel využívá při poskytování plnění poddodavatele, zavazuje se, že budou dodržovat stejné bezpečnostní požadavky požadované po Dodavateli.

4. Dodavatel se zavazuje bezodkladně doložit ZZS JčK, na základě předchozí výzvy, smluvní dokumenty se svými poddodavateli, ze kterých bude vyplývat závazek poddodavatele poskytovat plnění v souladu s bezpečnostními požadavky požadovanými po Dodavateli.

5. Dodavatel odpovídá za to, že jeho poddodavatelé nebudou jednat v rozporu s bezpečnostními požadavky.

11. Řízení dodavatelského řetězce

1. Dodavatel je povinen neprodleně informovat ZZS JčK o jakékoliv změně vlastnické struktury Dodavatele nebo jeho významných subdodavatelů, zejména o nabytí podílu subjektem ze třetí země.

2. Dodavatel je povinen informovat ZZS JčK o jakémkoliv požadavku orgánu třetí země na zpřístupnění dat nebo systémů ZZS JčK

3. Dodavatel je povinen poskytnout ZZS JčK přehled svých významných subdodavatelů podílejících se na plnění smluvního vztahu a informovat o jejich změnách.

4. Dodavatel je povinen zajistit, aby jeho subdodavatelé dodržovali minimálně stejnou úroveň bezpečnostních opatření stanovenou tímto dokumentem.

5. Dodavatel je povinen mít zpracovanou exit strategii (plán pro případ ukončení smluvního vztahu) zajišťující bezpečný přechod služby, migraci dat a předání veškeré dokumentace ZZS JčK.

6. Dodavatel je povinen umožnit ZZS JčK nebo jí pověřené osobě provedení auditu bezpečnostních opatření v rozsahu stanoveném smlouvou.

7. Dodavatel je povinen informovat ZZS JčK o způsobu řízení rizik kybernetické bezpečnosti v rámci svého plnění, včetně identifikovaných zbytkových rizik, a to nejpozději při uzavření smlouvy a dále při každé významné změně.

8. Dodavatel je povinen na vyžádání ZZS JčK poskytnout identifikaci fyzických osob, které v rámci plnění smluvního vztahu přicházejí do kontaktu s důvěrnými informacemi, aktivy nebo systémy ZZS JčK, a to zejména osob vykonávajících bezpečnostní role, penetrační testy nebo administraci technických aktiv.

9. Dodavatel je povinen řídit změny v dodávaných řešeních, službách a technických aktivech. O každé plánované změně s potenciálním dopadem na kybernetickou bezpečnost musí Dodavatel informovat ZZS JčK s dostatečným předstihem a změnu provést až po odsouhlasení ze strany ZZS JčK.

10. Dodavatel je povinen zahrnout plnění pro ZZS JčK do svých plánů řízení kontinuity činností a obnovy. Na vyžádání ZZS JčK je Dodavatel povinen prokázat existenci a aktuálnost těchto plánů a poskytnout součinnost při testování plánů kontinuity ZZS JčK.

11. Smlouva s Dodavatelem musí obsahovat ujednání o úrovni poskytovaných služeb (SLA), včetně definice způsobu a úrovně realizace bezpečnostních opatření a vzájemné odpovědnosti smluvních stran za zajištění kybernetické bezpečnosti.

12. Dodavatel je oprávněn užívat data ZZS JčK výhradně pro účely plnění smluvního vztahu. Jakékoliv jiné užití dat, jejich kopírování, sdílení nebo zpřístupnění třetím stranám bez předchozího písemného souhlasu ZZS JčK je zakázáno.

13. Dodavatel je povinen po ukončení smluvního vztahu bezpečně zlikvidovat veškerá data a informace ZZS JčK, která má v držení, a to způsobem odpovídajícím úrovni důvěrnosti těchto dat dle přílohy č. 2 vyhlášky č. 409/2025 Sb. o provedené likvidaci Dodavatel předá ZZS JčK písemné potvrzení.

14. Dodavatel je povinen na vyžádání ZZS JčK předat veškerá data, informace, konfigurační údaje a dokumentaci související s Předmětem plnění, a to ve strojově čitelném formátu a v přiměřené lhůtě stanovené ZZS JčK.

15. V případě obdržení žádosti orgánu cizího státu o zpřístupnění nebo předání dat ZZS JčK je Dodavatel povinen: (a) neprodleně informovat ZZS JčK o takové žádosti, pokud to není v rozporu s právním řádem; (b) přezkoumat zákonnost žádosti; (c) vynaložit veškeré úsilí o zabránění zpřístupnění v rámci možností daného právního řádu; (d) zpřístupnit data pouze v nezbytném rozsahu;

16. ZZS JčK provádí pravidelné přezkoumání plnění smluvních závazků Dodavatele z hlediska kybernetické bezpečnosti. Dodavatel je povinen poskytnout součinnost při tomto přezkoumání a bez zbytečného odkladu řešit zjištěné nedostatky a rizika.

12. 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 ZZS JčK, které se dozvěděl při dodávce Předmětu plnění, a to i po ukončení smluvního vztahu založeného Smlouvou. Důvěrnou informací ZZS JčK se rozumí informace obchodní, technické, know how, podklady a

doklady, osobní údaje, zdravotnická dokumentace či jiné, které jsou významné pro ZZS JčK 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 ZZS JčK (web, medializace Dodavatele, publikace, tisk apod.) jen s předchozím písemným souhlasem ZZS JčK.

13. Bezpečnostní varování

1. V souladu s legislativními povinnostmi byla na straně ZZS JčK zpracována analýza rizik kybernetické bezpečnosti. ZZS JčK tedy přijala následující bezpečnostní opatření.

2. Dodavatel musí zajistit, že v rámci Předmětu plnění:

   a) **nejsou dodávány** produkty, aplikace, řešení, webové stránky a webové služby včetně aplikačního programového rozhraní, poskytovaných společností Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd., nebo jakoukoli její předchůdkyní, nástupnickou, mateřskou, dceřinou či přidruženou společností na zařízeních přistupujících k informačním a komunikačním systémům kritické informační infrastruktury, informačním systémům základní služby a významným informačním systémům**;**

   b) **nedochází** k předávání systémových a uživatelských dat do Čínské lidové republiky, na území zvláštních administrativních oblastí či subjektům usídleným na území Čínské lidové republiky nebo zvláštních administrativních oblastí, a to včetně dat telemetrických, diagnostických, provozních a konfiguračních, a současně nabízené řešení technicky vylučuje možnost takového předávání;

   c) **nedochází** ke vzdálené správě, údržbě, aktualizaci nebo monitoringu technických aktiv vykonávané z území Čínské lidové republiky, zvláštních administrativních oblastí či ze strany subjektů usídlených na území Čínské lidové republiky nebo zvláštních administrativních oblastí, a současně je takový výkon technicky vyloučen;

   d) **nejsou dodávána** mobilní zařízení (mobilní telefony, tablety, notebooky a další obdobná zařízení) původem z Čínské lidové republiky (bylo vyrobeno v Čínské lidové republice nebo jehož výrobcem je subjekt pocházející z Čínské lidové republiky a též na území zvláštních administrativních oblastí, jimiž jsou Hongkong a Macao) v případě, že tyto mobilní zařízení:

      i. budou připojena do interní sítě ZZS JčK včetně bezdrátové sítě;

      ii. budou posílat data do internetu;

      iii. budou spravována vzdáleně Dodavatelem, výrobcem.

   e) nabízené řešení **nevyužívá cloudové služby**, datová centra nebo infrastrukturu pro ukládání či zpracování dat umístěnou na území Čínské lidové republiky nebo jejích zvláštních administrativních oblastí;

   f) nabízené řešení neobsahuje komponenty, jejichž bezpečnostní zranitelnosti podléhají povinnosti hlášení orgánům Čínské lidové republiky před jejich zveřejněním výrobcem nebo před jejich nahlášením ZZS JčK;

   g) Dodavatel, jeho subdodavatel (poddodavatel) ani jakýkoli subjekt v dodavatelském řetězci není usídlen na území Čínské lidové republiky, jejích zvláštních administrativních oblastí (Hongkong, Macao) ani není pod přímým či nepřímým vlastnickým vlivem subjektu usídleného na těchto územích.

14. Porušení požadavků

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

2. ZZS JčK je oprávněna jednostranně odstoupit od smlouvy nebo ji vypovědět v případě významné změny vlastnické struktury Dodavatele, změny kontroly nad Dodavatelem nebo změny kontroly nad zásadními aktivy Dodavatele využívanými pro plnění smluvního vztahu, pokud by taková změna mohla ohrozit kybernetickou bezpečnost regulované služby ZZS JčK.

3. Konkrétní výše smluvních pokut za porušení jednotlivých povinností stanovených tímto dokumentem bude stanovena ve smlouvě uzavřené mezi ZZS JčK a Dodavatelem. Uplatnění smluvní pokuty nevylučuje nárok ZZS JčK na náhradu škody v plné výši.

15. Komunikační kanály

1. Dodavatel hlásí skutečnosti týkající se technických zranitelností, hodnocení rizik a bezpečnostních incidentů OIKT ZZS JčK vždy na e-mail: it@zzsjck.cz.