MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Registr. číslo	PRÁVNÍ ODBOR
	0284/2024

Smlouva na poskytování správy elektronického systému spisové služby GINIS®

Česká republika – Ministerstvo zdravotnictví
se sídlem: Palackého náměstí 375/4, 128 00 Praha 2
IČO: 00024341
DIČ: CZ00024341
jednající: [redacted]
bankovní spojení: 2528001/0710
IDDS: pv8aaxd

dále jen „**Objednatel**“

a

GORDIC spol. s r.o.
se sídlem: Erbenova 2108/4, 586 01 Jihlava
IČO: 47903783
DIČ: CZ47903783
zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně ve vložce č. 9313 oddílu C
zastoupená: [redacted]
bankovní spojení: Komerční banka, a.s. číslo bankovního účtu: 21409681/0100
IDDS: sxk8tap

dále jen „**Dodavatel**“

společně také jako „**smluvní strany**“ a každý jednotlivě jako „**smluvní strana**“

spolu níže uvedeného data dle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**“) uzavírají tuto Smlouvu

Čl. I – Úvodní ustanovení

1) Smluvní strany uzavírají tuto Smlouvu na základě výsledku zadávacího řízení na nadlimitní veřejnou zakázku na služby zadávanou v otevřeném řízení s názvem *SPRÁVA ELEKTRONICKÉHO SYSTÉMU SPISOVÉ SLUŽBY GINIS VČETNĚ ÚDRŽBY, PODPORY, POSKYTOVÁNI UPDATE A PRACÍ PODLE POŽADAVKŮ OBJEDNAVATELE* (dále jen „**veřejná zakázka**“), v němž byla nabídka Dodavatele vybrána jako ekonomicky nejvýhodnější.

2) Objednatel prohlašuje, že:

   a. splňuje veškeré podmínky a požadavky ve Smlouvě stanovené a je oprávněn Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

3) Dodavatel prohlašuje, že:

   a. splňuje veškeré podmínky a požadavky ve Smlouvě stanovené a je oprávněn Smlouvu uzavřít a řádně plnit závazky v ní obsažené;

   b. se náležitě seznámil se všemi podklady, které byly součástí zadávací dokumentace veřejné zakázky (dále jen „**zadávací dokumentace**“), a které stanovují požadavky na plnění předmětu Smlouvy a je odborně způsobilý ke splnění všech jeho závazků podle Smlouvy;

   c. jím poskytované plnění odpovídá všem požadavkům vyplývajícím z platných a účinných právních předpisů, které se na plnění vztahují;

   d. ke dni uzavření Smlouvy vůči němu není vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů (dále jen „**insolvenční zákon**“), a zároveň se zavazuje Objednatele o všech skutečnostech o hrozícím úpadku bezodkladně informovat;

   e. si je vědom skutečnosti, že Objednatel má zájem na realizaci předmětu Smlouvy v souladu se zásadami odpovědného zadávání veřejných zakázek dle § 6 odst. 4 zákona č. 134/2016 Sb. o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“). Dodavatel se zavazuje po celou dobu trvání Smlouvy a Objednávek, jak je tento pojen definován v čl. IV odst. 2 Smlouvy níže, a vůči všem osobám, které se na plnění předmětu Smlouvy a dílčích objednávek podílejí, zajistit dodržování platných a účinných pracovněprávních předpisů (odměňování, pracovní doba, doba odpočinku, placené přesčasy apod.), právních předpisů týkajících se oblasti zaměstnanosti a bezpečnosti a ochrany zdraví při práci a právních předpisů týkajících se ochrany životního prostředí.

4) Dodavatel dále prohlašuje, že se detailně seznámil s rozsahem a povahou předmětu plnění, že jsou mu známy veškeré relevantní technické, kvalitativní a jiné podmínky nezbytné k realizaci předmětu plnění, a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci předmětu plnění za dohodnutou cenu uvedenou v Příloze č. 5 Smlouvy, a to rovněž ve vazbě na jím prokázanou kvalifikaci pro plnění veřejné zakázky.

5) Dodavatel bere na vědomí, že podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „**ZoKB**“), vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále jen „**VoKB**“), s ohledem na to, že na základě Smlouvy prostřednictvím poskytování údržby, podpory

a update zajišťuje funkčnost technických a programových prostředků eSSL, jak je tento pojem definován v čl. II odst. 1 Smlouvy níže, který je významným informačním systémem podle ZoKB a jehož je Objednatel dle ZoKB správcem, naplňuje definici provozovatele systému ve smyslu § 2 písm. g) ZoKB, a je tedy významným dodavatelem podle § 2 odst. n) VoKB, a jako takový je veden v evidenci významných dodavatelů Objednatele.

6) Dodavatel bere na vědomí, že jako významný dodavatel ve smyslu ZoKB je povinen dodržovat povinnosti vyplývající mu z příslušných ustanovení ZoKB a VoKB, které jsou konkretizovány v Příloze č. 9 Smlouvy.

Čl. II – Účel a předmět Smlouvy

1) Účel, za nímž se Smlouva uzavírá, je řádné zajištění správy elektronického systému spisové služby Objednatele v rozsahu modulů a licencí dle Přílohy č. 2 Smlouvy (dále jen „**eSSL**“), a to včetně řádného zajištění jeho údržby, podpory, poskytování update a prací dle požadavků Objednatele.

2) Předmětem Smlouvy je úprava práv a povinností smluvních stran při poskytování služeb Dodavatelem, a to jak prostřednictvím průběžně poskytovaných služeb, tak jednorázově poskytovaných služeb (společně jako „**Služby**“) na základě Objednávek, jak je tento pojem definován v čl. IV odst. 2 Smlouvy níže, dle aktuálních požadavků Objednatele.

3) Předmětem Smlouvy je závazek Objednatele za řádně dle Smlouvy poskytované Služby zaplatit sjednanou cenu.

Čl. III – Průběžně poskytované služby

1) Dodavatel se zavazuje po dobu trvání Smlouvy poskytovat průběžně poskytované služby dle specifikace uvedené v Příloze č. 1 Smlouvy.

2) Dodavatel je povinen Objednateli včas nahlásit každou plánovanou odstávku helpdesku a hotline ve smyslu části A, odst. 1.2, Přílohy č. 1 Smlouvy, přičemž vždy uvede důvod a předpokládanou dobu trvání takové odstávky, jakož i náhradní řešení pro řešení incidentů.

3) V případě nefunkčnosti helpdesku či hotline z jiných než plánovaných důvodů je Dodavatel povinen bezodkladně, nejpozději do začátku následujícího pracovního dne, zajistit náhradní řešení a o takovém náhradním řešení Objednatele informovat. Začátkem pracovního dne dle předchozí věty se rozumí 08:00 hodin.

4) V rámci poskytování průběžně poskytovaných služeb je Dodavatel povinen vypracovávat měsíční report poskytovaných služeb (dále jen „**report**“), v němž uvede přehled průběžně poskytovaných služeb, které v daném kalendářním měsíci poskytl. Součástí reportu je i Zpráva o stavu systému dle části A, odst. 1.2, písm. d) Přílohy č. 1 Smlouvy.

5) Report za kalendářní měsíc vypracuje Dodavatel bezodkladně po konci kalendářního měsíce, k němuž je report zpracováván a nejpozději do 5. dne následujícího kalendářního měsíce jej zašle Objednateli na vědomí.

6) V případě, že přehled poskytovaných služeb uvedených v reportu neodpovídá Smlouvě a rozsahu průběžně poskytovaných služeb, které Dodavatel v daném měsíci skutečně poskytl, Objednatel k němu bez zbytečného odkladu, nejpozději však do 10 pracovních dnů od jeho doručení, sdělí své odůvodněné výhrady a vrátí jej Dodavateli v přiměřené lhůtě, která nebude delší než 10 pracovních dnů, k přepracování. Nebude-li ani

přepracovaný report odpovídat Smlouvě a rozsahu průběžně poskytovaných služeb, které Dodavatel v daném měsíci skutečně poskytl, je Objednatel oprávněn požadovat slevu z ceny ve výši 10 % z ceny průběžně poskytovaných služeb bez DPH za měsíc dle čl. VII odst. 2 Smlouvy, ust. čl. VII odst. 6 o slevě z ceny tím není dotčeno. Případ, kdy přepracovaný report opakovaně nebude odpovídat Smlouvě, je podstatným porušením Smlouvy ze strany Dodavatele. Opakovaně dle předchozí věty se rozumí alespoň třikrát.

Čl. IV – Jednorázově poskytované služby

1) Dodavatel se zavazuje po dobu trvání Smlouvy umožnit Objednateli poptávat jednorázově poskytované služby dle specifikace uvedené v Příloze č. 1 Smlouvy.

2) Dodavatel bude jednorázově poskytované služby poskytovat na základě písemných objednávek Objednatele (dále jen „**Objednávky**“), které budou smluvní strany uzavírat postupem dle Smlouvy.

3) Před zasláním dílčí objednávky dle čl. IV odst. 4 Smlouvy si Objednatel od Dodavatele vyžádá předběžnou a detailní kalkulaci potřeby časové náročností prací, které budou předmětem Objednávky (dále jen „**kalkulace**“). Pro vyloučení pochybností se uvádí, že předložení kalkulace není návrhem na uzavření smlouvy a nijak nezavazuje Objednatele k tomu, aby postupoval dle čl. IV odst. 4 a násl. Smlouvy.

4) Po předložení kalkulace Objednatel zašle Dodavateli písemnou dílčí objednávku na jednorázově poskytovanou službu, v níž uvede alespoň:

   a. popis požadovaného plnění;

   b. požadovaný termín plnění;

   c. nejvyšší přípustnou cenu za požadované plnění bez DPH a vč. DPH;

   d. datum vystavení dílčí objednávky;

   e. informaci o tom, zda bude požadované plnění podléhat akceptačnímu řízení dle čl. IV Smlouvy;

   f. podpis oprávněné osoby,

   přičemž taková dílčí objednávka je návrhem na uzavření smlouvy.

5) Dodavatel je bezodkladně od doručení dílčí objednávky, nejpozději však do 5 pracovních dnů od jejího doručení, povinen dílčí objednávku dle čl. IV odst. 4 Smlouvy písemně:

   a. akceptovat, nebo

   b. upravit, nebo

   c. s uvedením důvodů odmítnout,

   přičemž akceptace dílčí objednávky je přijetím návrhu smlouvy a úprava dílčí objednávky je novým návrhem na uzavření smlouvy. Nevyjádří-li se Dodavatel k návrhu ve lhůtě dle tohoto článku, platí, že dílčí objednávku odmítl.

6) Případ, kdy Objednatel nepřijme upravenou dílčí objednávku, má stejné účinky jako odmítnutí dle čl. IV odst. 5 písm. c) Smlouvy.

7) Odmítnout dílčí objednávku dle čl. IV odst. 5 písm. c) Smlouvy je po dobu trvání Smlouvy Dodavatel oprávněn nejvýše pětkrát. Případ, kdy by Dodavatel odmítl dílčí objednávku vícekrát, je podstatným porušením Smlouvy ze strany Dodavatele.

8) V případě, kdy hodnota předmětu plnění Objednávky přesáhne částku 50.000,- Kč bez DPH, nabude taková dílčí objednávka účinnosti až uveřejněním 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), ve znění pozdějších předpisů (dále jen „**zákon o registru smluv**“). Pro uveřejnění Objednávky v registru smluv se použije čl. XII odst. 1 Smlouvy.

9) V případě, že Objednatel v dílčí objednávce dle čl. IV odst. 4 Smlouvy uvede, že požadované plnění bude podléhat akceptačnímu řízení, provedou smluvní strany akceptační řízení, jehož předmětem bude ověření, zda poskytnuté plnění odpovídá požadavkům Objednatele uvedeným v Objednávce (dále jen „**akceptační řízení**“) a o jehož výsledku smluvní strany vyhotoví akceptační protokol (dále jen „**akceptační protokol**“).

10) Akceptační řízení je zahájeno předáním plnění Objednateli. Předáním plnění dle předchozí věty se rozumí předání plnění vymezeného v konkrétní Objednávce, jakož i případné související dokumentace. Objednatel bez zbytečného odkladu po předání plnění, nejpozději však do 10 pracovních dnů ode dne předání plnění, posoudí, zda předmětné plnění odpovídá Objednávce, den posouzení vždy uvede na akceptačním protokolu. V případě, že:

    a. plnění odpovídá Objednávce, vyznačí Objednatel tuto skutečnost na akceptačním protokolu výrokem „akceptováno“.

    b. plnění částečně odpovídá Objednávce, vyznačí Objednatel tuto skutečnost na akceptačním protokolu výrokem „vráceno k přepracování“ a určí Dodavateli přiměřenou lhůtu k přepracování.

    c. plnění neodpovídá Objednávce, vyznačí Objednatel tuto skutečnost na akceptačním protokolu výrokem „neakceptováno“.

11) V případě, kdy je v rámci akceptačního řízení na akceptačním protokolu uveden výrok dle čl. IV odst. 10 písm. b) Smlouvy, je Dodavatel povinen v určené lhůtě plnění přepracovat. Po předání přepracovaného plnění smluvní strany pokračují v akceptačním řízení. Pro vyloučení pochybností se uvádí, že vrátit plnění k přepracování je v jednom akceptačním řízení možné pouze jednou a za přepracování není Dodavatel oprávněn navýšit cenu za předmětnou jednorázově poskytovanou službu.

12) Akceptační řízení může skončit pouze výsledkem:

    a. akceptováno dle čl. IV odst. 10 písm. a) Smlouvy, nebo

    b. neakceptováno dle čl. IV odst. 10 písm. c) Smlouvy,

    přičemž den ukončení akceptačního řízení je shodný se dnem uvedeným na akceptačním protokolu dle čl. IV odst. 10 Smlouvy.

13) V případě, že akceptační řízení skončí výsledkem dle čl. IV odst. 12 písm. a) Smlouvy, Objednatel v den ukončení akceptačního řízení převezme předané plnění.

14) Případ, kdy akceptační řízení skončí výsledkem dle čl. IV odst. 12 písm. b) Smlouvy, je podstatným porušením Objednávky a má stejné účinky jako odmítnutí požadavku dle čl. IV odst. 5 písm. c) Smlouvy.

Čl. V – Další práva a povinnosti smluvních stran, komunikace

1) Dodavatel je povinen po celou dobu účinnosti Smlouvy udržovat v platnosti pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Dodavatelem třetí osobě při výkonu jeho podnikatelské činnosti, přičemž pojistná částka takového pojištění musí činit nejméně 10.000.000,- Kč. Na výzvu Objednatele je plnění povinnosti dle předchozí věty Dodavatel povinen bezodkladně, nejpozději však do 2 pracovních dnů prokázat, a to předložením dokladu o uzavřeném pojištění, přičemž takovým dokladem se rozumí pojistná smlouva, pojistka nebo potvrzení pojišťovny, resp. jiného pojistného zprostředkovatele o existenci pojištění dle tohoto článku. Případ, kdy Dodavatel nesplní povinnost prokázat existenci platné pojistné smlouvy dle předchozí věty, je podstatným porušením Smlouvy ze strany Dodavatele.

2) Dodavatel je povinen Objednatele informovat o všech svých poddodavatelích, uvedených spolu s rozsahem jimi poskytovaného plnění v Příloze č. 7 Smlouvy. Dodavatel je povinen uvádět identifikační údaje poddodavatele v rozsahu, v jakém jsou uvedeny jeho vlastní identifikační údaje na titulní straně Smlouvy.

3) O změně v seznamu poddodavatelů týkající se identifikačních údajů poddodavatele nebo rozsahu jím poskytovaného plnění je Dodavatel povinen Objednatele informovat bez zbytečného odkladu poté, kdy změna nastala, nejpozději však do 7 dnů od tohoto okamžiku. Informační povinnost dle § 105 odst. 3 ZZVZ tím není dotčena.

4) Dodavatel je oprávněn změnit poddodavatele jen s předchozím písemným souhlasem Objednatele. V případě, že dochází ke změně poddodavatele, jehož prostřednictvím Dodavatel prokazoval kvalifikaci v zadávacím řízení, nový poddodavatel musí disponovat kvalifikací ve stejném či větším rozsahu, než je kvalifikace, kterou původní poddodavatel prokázal za Dodavatele. Poddodavatel, pomocí kterého Dodavatel prokázal část splnění kvalifikace veřejné zakázky, bude poskytovat i tomu odpovídající část plnění. Souhlas dle věty první tohoto odstavce Objednatel udělí bez zbytečného odkladu, v případě změny poddodavatele, jímž Dodavatel prokazoval kvalifikaci v zadávacím řízení bez zbytečného odkladu poté, co Dodavatel předloží doklady prokazující, že nový poddodavatel disponuje kvalifikací ve stejném či větším rozsahu než původní poddodavatel. Případ, kdy by Dodavatel změnil poddodavatele bez předchozího písemného souhlasu Objednatele, je podstatným porušením Smlouvy ze strany Dodavatele.

5) Zadání provedení části plnění dle Smlouvy, resp. příslušné Objednávky, poddodavateli Dodavatelem nezbavuje Dodavatele jeho výlučné odpovědnosti za řádné provedení takového plnění vůči Objednateli. Dodavatel odpovídá Objednateli za plnění předmětu Smlouvy, resp. příslušné Objednávky, které svěřil poddodavateli, ve stejném rozsahu, jako by jej poskytoval sám.

6) Dodavatel bez zbytečného odkladu, nejpozději však do 5 pracovních dnů, informuje Objednatele o tom, že se dozvěděl o některé z následujících skutečností:

   a. Dodavatel nebo jeho poddodavatelé jsou osobami, na které dopadají mezinárodní sankce podle zákona upravujícího provádění mezinárodních, na základě kterých

Objednatel nesmí zadat veřejnou zakázku účastníku zadávacího řízení dle § 48a ZZVZ;

b. Dodavatel nebo jeho poddodavatelé jsou osobami, na které dopadají mezinárodní sankce podle zákona upravujícího provádění mezinárodních sankcí, na základě kterých Objednatel nesmí zpřístupnit finanční prostředky za plnění smlouvy.

7) Dodavatel je povinen po celou dobu trvání Smlouvy na výzvu Objednatele prokázat, že disponuje realizačním týmem dle požadavků stanovených v zadávací dokumentaci. Povinnost dle předchozí věty splní, doloží-li bez zbytečného odkladu poté, co byl Objednatelem k prokázání disponování s realizačním týmem vyzván, nejpozději však do 5 pracovních dnů od takové výzvy, předložit datované čestné prohlášení člena realizačního týmu, které v den předložení nebude starší než 3 dny, o tom, že je zaměstnancem Dodavatele nebo osobou v obdobném postavení.

8) Dodavatel je oprávněn navrhnout výměnu člena realizačního týmu uvedeného v Příloze č. 3 Smlouvy. Výměna člena realizačního týmu je podmíněna písemným souhlasem Objednatele, který Objednatel bez zbytečného odkladu udělí, prokáže-li Dodavatel, že navrhovaný nový člen realizačního týmu splňuje zadávací dokumentací stanovené požadavky na člena realizačního týmu, který je nahrazován.

9) Objednatel je oprávněn ze závažných důvodů, za něž se považují důvody pro okamžité zrušení pracovního poměru dle § 55 odst. 1 písm. b) zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (dále jen „**zákoník práce**“), pro rozvázání pracovního poměru výpovědí dle § 52 písm. h), písm. g) zákoníku práce, požadovat výměnu člena realizačního týmu uvedeného v Příloze č. 3 Smlouvy. Výměnu člena realizačního týmu je Dodavatel povinen provést bezodkladně poté, co jej o ni Objednatel požádá, nejpozději však do 30 dnů. Nový člen realizačního týmu musí splňovat zadávací dokumentací stanovené kvalifikační požadavky na člena realizačního týmu, který je nahrazován.

10) Případy, kdy by Dodavatel nahradil člena realizačního týmu osobou, která nesplňuje zadávací dokumentací stanovené požadavky na člena realizačního týmu nebo nenahradil člena realizačního týmu, ačkoli k tomu byl Objednatelem v souladu s čl. V odst. 8 Smlouvy vyzván, jsou podstatným porušením Smlouvy ze strany Dodavatele.

11) Dodavatel je povinen uchovávat veškerou dokumentaci a doklady vztahující se k poskytovanému plnění (včetně účetních dokladů) v souladu s platnými a účinnými právními předpisy České republiky minimálně deset let od konce roku, ve kterém došlo k ukončení poslední Objednávky, nejméně však od konce roku, v němž došlo k ukončení Smlouvy. Pokud platné právní předpisy České republiky stanovují delší lhůtu, než je uvedena v předchozí větě, je Dodavatel povinen uchovávat dokumentaci týkající se Služeb do uplynutí této lhůty.

12) Dodavatel prohlašuje, že ve smyslu varování Národního úřadu pro kybernetickou a informační bezpečnost, vydaného podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů, ze dne 8. 3. 2023, sp. zn. 350–303/2023, č. j. 2236/2023-NÚKIB-E/350 nemá nainstalovánu a nepoužívá aplikaci TikTok na zařízeních přistupujících k informačním a komunikačním systémům kritické informační infrastruktury, informačním systémům základní služby a významným informačním systémům. V případě, že se prohlášení Dodavatele dle předchozí věty ukáže jako nepravdivé, je Dodavatel povinen, mimo zaplacení smluvní pokuty dle čl. X odst. 7 Smlouvy, bezodkladně ze všech zařízení aplikaci

TikTok odinstalovat a zdržet se jejího dalšího používání. Případ, kdy Dodavatel nesplní povinnost odinstalovat aplikaci TikTok a zdržet se jejího dalšího používání, nebo se jeho prohlášení dle první věty tohoto odstavce opakovaně ukáže jako nepravdivé, je podstatným porušením Smlouvy ze strany Dodavatele.

13) Smluvní strany se zavazují si bez zbytečného odkladu sdělovat všechny relevantní informace nezbytné pro plnění Smlouvy, zejména informace o:

   a. zjištěných překážkách plnění;

   b. uplatněných nárocích třetích stran, které by mohly ovlivnit plnění Smlouvy;

   c. vznesených požadavcích státního dozoru.

14) Smluvní strany se zavazují, že veškerá zásadní sdělení, neurčí-li Smlouva jinak, budou činit písemně na adresy svých sídel uvedené na titulní straně Smlouvy nebo do datových schránek uvedených na titulní straně Smlouvy.

15) Komunikace mezi stranami bude probíhat prostřednictvím kontaktních osob, jimiž jsou:

   [redacted] v případě Objednatele.

   [redacted] v případě Dodavatele.

16) Změna kontaktní osoby dle tohoto článku není změnou Smlouvy a vůči druhé smluvní straně je účinná dnem doručení oznámení o změně kontaktní osoby na e-mailovou adresu:

   a. [redacted] v případě Objednatele.

   b. [redacted] v případě Dodavatele.

Čl. VI – Doba a místo plnění

1) Dodavatel se zavazuje započít s poskytováním průběžně poskytovaných služeb bezodkladně po účinnosti Smlouvy. Bezodkladně dle předchozí věty se rozumí nejpozději následující den po účinnosti Smlouvy.

2) Dodavatel se rovněž zavazuje bezodkladně po účinnosti Smlouvy umožnit Objednateli poptávat jednorázově poskytované služby. Bezodkladně dle předchozí věty se rozumí nejpozději následující den po účinnosti Smlouvy.

3) Místem plnění je sídlo Objednatele uvedené na titulní straně Smlouvy.

Čl. VII – Cena a platební podmínky

1) Celková cena dle Smlouvy nepřesáhne částku 18.400.000,- Kč bez DPH, 22.264.000,- Kč vč. DPH.

2) Cena za jeden kalendářní měsíc poskytování průběžně poskytovaných služeb je určena v Příloze č. 5 Smlouvy a činí 350.000,- bez DPH, 423.500,- Kč vč. DPH.

3) Cena za jednu hodinu poskytování jednorázových služeb je určena v Příloze č. 5 Smlouvy.

4) Dojde-li ke změně sazby DPH, bude Dodavatelem DPH účtována podle právních předpisů platných a účinných v době uskutečnění zdanitelného plnění. Takováto změna Smlouvy nemusí být sjednána formou dle čl. XII odst. 8 Smlouvy. Za správnost stanovení sazby DPH a vyčíslení výše DPH odpovídá Dodavatel.

5) Dodavatel se zavazuje Objednateli poskytovat plnění dle Smlouvy po celou dobu jejího trvání za ceny bez DPH, které jsou uvedeny v Příloze č. 5 Smlouvy a činí 18.340.800,- Kč bez DPH, 22 192 368,- Kč vč. DPH.

6) V případě, že Dodavatel poskytoval průběžně poskytované služby pouze část kalendářního měsíce, má Objednatel nárok na slevu z ceny poskytování průběžně poskytovaných služeb za příslušný kalendářní měsíc. Výsledná cena za poskytování průběžně poskytovaných služeb za příslušný kalendářní měsíc se poměrně sníží tak, aby odpovídala počtu kalendářních dnů, po něž byly průběžně poskytované služby poskytovány.

7) Cena za Služby je splatná na základě daňového dokladu (faktury), která bude kromě náležitostí daňových dokladů dle platných právních předpisů obsahovat registrační číslo Smlouvy stanovené Objednatelem a další náležitosti stanovené Smlouvou.

8) Lhůta splatnosti faktury činí 30 dnů od jejího doručení Objednateli, a to buď na adresu jeho sídla uvedenou na titulní straně Smlouvy, nebo do datové schránky uvedené na titulní straně Smlouvy.

9) Fakturu za průběžně poskytované služby vystaví Dodavatel bez zbytečného odkladu poté, co mu vznikne právo fakturovat průběžně poskytované služby. Dnem vzniku práva dle předchozí věty je poslední den daného kalendářního měsíce, za nějž jsou průběžně poskytované služby fakturovány. Přílohou faktury bude kopie reportu za daný kalendářní měsíc.

10) Fakturu za jednorázově poskytované služby vystaví Dodavatel bez zbytečného odkladu poté, co mu vznikne právo fakturovat jednorázově poskytované služby. Dnem vzniku práva dle předchozí věty je:

    a. den uvedený na Objednávce jako termín plnění, bylo-li plnění v ní specifikované Dodavatelem řádně a v uvedeném termínu poskytnuto, v opačném případě den, kdy Dodavatel plnění řádně poskytl, nebo

    b. den ukončení akceptačního řízení, pokud probíhalo a skončilo výsledkem dle čl. IV odst. 12 písm. a) Smlouvy.

11) V případě uvedeném v čl. VII odst. 10 písm. b) Smlouvy bude přílohou faktury kopie akceptačního protokolu.

12) V případě, že faktura nebude obsahovat náležitosti stanovené Smlouvou, je Objednatel oprávněn ji ve lhůtě splatnosti dle čl. VII odst. 8 Smlouvy s odůvodněním vrátit Dodavateli k přepracování, aniž by se dostal do prodlení se splatností takové faktury. Nová lhůta splatnosti počíná běžet dnem doručení přepracované faktury Objednateli.

13) Objednatel bude hradit přijaté faktury pouze na bankovní účty Dodavatele uvedené na titulní straně Smlouvy a zveřejněné správcem daně způsobem umožňujícím dálkový přístup ve smyslu § 96 odst. 2 zákona o DPH.

14) Dodavatel prohlašuje, že správce daně před uzavřením této Smlouvy nerozhodl, že Dodavatel je nespolehlivým plátcem ve smyslu § 106a zákona o DPH (dále jen „**nespolehlivý plátce**“). V případě, že správce daně rozhodne o tom, že Dodavatel je nespolehlivým plátcem, zavazuje se Dodavatel o tomto informovat Objednatele do 2 pracovních dnů. Stane-li se Dodavatel nespolehlivým plátcem, uhradí Objednatel

Dodavateli pouze základ daně, přičemž DPH bude Objednatelem uhrazena Dodavateli až po písemném doložení Dodavatele o jeho úhradě této DPH příslušnému správci daně.

15) V případě, že se Objednatel dostane do prodlení se zaplacením faktury, má Dodavatel nárok na zaplacení zákonného úroku z prodlení ve výši stanovené nařízením vlády č. 351/2013 Sb., kterým se určuje výše úroků z prodlení a nákladů spojených s uplatněním pohledávky, určuje odměna likvidátora, likvidačního správce a člena orgánu právnické osoby jmenovaného soudem a upravují některé otázky Obchodního věstníku, veřejných rejstříků právnických a fyzických osob a evidence svěřenských fondů a evidence údajů o skutečných majitelích, ve znění pozdějších předpisů (dále jen „**nařízení vlády č. 351/2013 Sb.**“) z dlužné částky.

Čl. VIII – Licenční ujednání

1) Dodavatel prohlašuje, že je oprávněn Objednateli udělit licenci v rozsahu a za podmínek dle tohoto článku Smlouvy.

2) Vznikne-li v důsledku poskytování Služeb autorské dílo či dílo chráněné jako autorské (dále jen „**autorské dílo**“) ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „**autorský zákon**“), zavazuje se Dodavatel udělit ke dni předání a převzetí takového plnění Objednatelem licenci k užití takového autorského díla, a to v rozsahu, na dobu a za podmínek, za kterých užívá Objednatel příslušný modul eSSL.

3) Pro vyloučení pochybností se uvádí, že licenční odměna je zahrnuta v ceně za Služby.

4) Dodavatel je povinen zajistit, aby výsledkem jeho plnění nebo jakékoliv jeho části nebyla porušena práva třetích osob. Pro případ, že užíváním plnění nebo jeho dílčí části nebo prostou existencí plnění nebo jeho dílčí části budou v důsledku porušení povinností Dodavatele dotčena práva třetích osob, nese Dodavatel vedle odpovědnosti za takovéto vady plnění dle Smlouvy odpovědnost za veškeré škody, které tím Objednateli vzniknou. S nositeli chráněných práv duševního vlastnictví vzniklých v souvislosti s realizací plnění dle Smlouvy a navazujících Objednávek je Dodavatel povinen vždy smluvně zajistit možnost nakládání s těmito právy Objednatelem v rozsahu definovaném tímto článkem Smlouvy.

5) Pro vyloučení pochybností se uvádí, že licenci v rozsahu a za podmínek dle tohoto článku Smlouvy je Dodavatel povinen Objednateli zajistit i v případě, kdy je část plnění poskytována prostřednictvím poddodavatele.

6) Dodavatel je povinen Objednateli uhradit jakoukoli újmu vzniklou v důsledku toho, že Objednatel nemohl předmět plnění Smlouvy a na ni navazujících Objednávek užívat řádně a nerušeně. Případ, kdy se jakékoliv prohlášení Dodavatele v tomto článku Smlouvy uvedené ukáže jako nepravdivé nebo Dodavatel poruší jinou povinnost dle tohoto článku Smlouvy, je podstatným porušením Smlouvy ze strany Dodavatele.

Čl. IX – Ochrana informací

1) Dodavatel se zavazuje zajistit utajení důvěrných informací a zachovávat mlčenlivost o všech skutečnostech získaných při plnění předmětu Smlouvy obvyklým způsobem pro utajování takových informací. Údaje, které tvoří obchodní tajemství Dodavatele

ve smyslu § 504 zákona č. 89/2012 Sb., občanský zákoník, v platném znění, a které se smluvní strany zavazují zajišťovat, jsou uvedeny v Příloze č. 6 Smlouvy.

2) Dodavatel bere na vědomí, že Objednatel vystupuje jako orgán veřejné moci, který je povinen zajišťovat důvěrnost příslušných skutečností pouze v rozsahu stanoveném zákonem.

3) Povinnost zachovávat mlčenlivost se neuplatní v případech, kdy je Dodavatel povinen příslušnou skutečnost sdělit na základě zákona, nebo je taková informace všeobecně dostupná, nebo v případě hájení oprávněných zájmů Dodavatele.

4) Povinnost Dodavatele zachovávat utajení dle čl. IX Smlouvy trvá po dobu trvání Smlouvy i po jejím dokončení. Této povinnosti jej může zprostit pouze Objednatel svým písemným prohlášením.

Čl. X – Sankční ustanovení a odpovědnost za újmu

1) V případě, že Dodavatel nezapočne s poskytováním průběžně poskytovaných služeb ve lhůtě stanovené čl. VI odst. 1 Smlouvy, je povinen Objednateli uhradit smluvní pokutu ve výši 0,5 % z měsíční ceny průběžně poskytovaných služeb bez DPH za každý započatý den prodlení.

2) V případě, že Dodavatel neumožní Objednateli poptávat jednorázově poskytované služby ve lhůtě stanovení čl. VI odst. 2 Smlouvy, je povinen Objednateli uhradit smluvní pokutu ve výši 1.000,- Kč za každý započatý den prodlení.

3) V případě, že Dodavatel nesplní povinnost reagovat na nahlášený incident ve lhůtě uvedené v tabulce č. 1 Přílohy č. 1 Smlouvy, je povinen Objednateli uhradit smluvní pokutu ve výši:

   a. 0,1 % z ceny průběžně poskytovaných služeb za měsíc bez DPH dle čl. VII odst. 2 Smlouvy, a to za každou započatou hodinu prodlení v případě incidentu kategorie V1

   b. 0,05 % z ceny průběžně poskytovaných služeb za měsíc bez DPH dle čl. VII odst. 2 Smlouvy, a to za každou započatou hodinu prodlení v případě incidentu kategorie V2

   c. 0,01 % z ceny průběžně poskytovaných služeb za měsíc bez DPH dle čl. VII odst. 2 Smlouvy, a to za každou započatou hodinu prodlení v případě incidentu kategorie V3

4) V případě, že Dodavatel nesplní povinnost vyřešit incident kategorie V1 ve lhůtě uvedené v tabulce č. 1 Přílohy č. 1 Smlouvy, je povinen Objednateli uhradit smluvní pokutu ve výši 0,5 % z ceny průběžně poskytovaných služeb bez DPH za měsíc dle čl. VII odst. 2 Smlouvy, a to za každou započatou hodinu prodlení. Celková výše smluvní pokuty dle předchozí věty může činit nejvýše 5 % z ceny průběžně poskytovaných služeb bez DPH za kalendářní měsíc dle čl. VII odst. 2 Smlouvy za každé jednotlivé porušení utvrzované povinnosti.

5) V případě, že Dodavatel nesplní povinnost vyřešit incident kategorie V2 ve lhůtě uvedené v tabulce č. 1 Přílohy č. 1 Smlouvy, je povinen Objednateli uhradit smluvní pokutu ve výši 0,3 % z ceny průběžně poskytovaných služeb bez DPH za měsíc dle čl. VII odst. 2 Smlouvy, a to za každou započatou hodinu prodlení. Celková výše smluvní pokuty dle předchozí věty může činit nejvýše 3 % z ceny průběžně poskytovaných služeb bez DPH za kalendářní měsíc dle čl. VII odst. 2 Smlouvy za každé jednotlivé porušení utvrzované povinnosti.

6) V případě, že Dodavatel nesplní povinnost vyřešit incident kategorie V3 ve lhůtě uvedené v tabulce č. 1 Přílohy č. 1 Smlouvy, je povinen Objednateli uhradit smluvní pokutu ve výši 0,1 % z ceny průběžně poskytovaných služeb bez DPH za měsíc dle čl. VII odst. 2 Smlouvy, a to za každý započatý den prodlení. Celková výše smluvní pokuty dle předchozí věty může činit nejvýše 1 % z ceny průběžně poskytovaných služeb bez DPH za kalendářní měsíc dle čl. VII odst. 2 Smlouvy za každé jednotlivé porušení utvrzované povinnosti.

7) V případě, že se prohlášení Dodavatele dle čl. V odst. 12 Smlouvy ukáže jako nepravdivé, je Dodavatel povinen Objednateli uhradit smluvní pokutu ve výši 10.000,- Kč za každé jednotlivé zařízení, na němž má nainstalovánu nebo používá aplikaci TikTok, zároveň je Dodavatel povinen bezodkladně zjednat nápravu v podobě odinstalování aplikace TikTok a zdržení se jakéhokoliv jejího dalšího používání.

8) V případě, že Dodavatel poruší povinnost v určené lhůtě dodat systémové a provozní bezpečnostní dokumentace dle čl. 1.11 Přílohy č. 9 Smlouvy, je povinen Objednateli uhradit smluvní pokutu ve výši 10.000,- Kč za každý jednotlivý případ porušení takové povinnosti.

9) V případě, že Dodavatel neposkytne součinnost při provádění zákaznického auditu dle čl. 5 Přílohy č. 9 Smlouvy, je povinen Objednateli uhradit smluvní pokutu ve výši 100.000,- Kč za každý jednotlivý zákaznický audit, při jehož provádění neposkytl Objednateli součinnost.

10) Smluvní pokuta je splatná na základě písemné výzvy Objednatele, a to do 15 dnů od jejího doručení, není-li ve výzvě uvedena lhůta delší. Smluvní pokutu Dodavatel uhradí na bankovní účet Objednatele uvedený na titulní straně Smlouvy.

11) Dostane-li se Dodavatel do prodlení se zaplacením smluvní pokuty, má Objednatel nárok na zaplacení zákonného úroku z prodlení dle nařízení vlády č. 351/2013 Sb., a to z částky uvedené ve výzvě k zaplacení smluvní pokuty dle čl. X odst. 10 Smlouvy.

12) Ujednání o smluvní pokutě nezbavuje Dodavatele povinnosti nahradit v plném rozsahu škodu, která Objednateli v důsledku porušení utvrzované povinnosti vznikla.

13) Smluvní strany se zavazují jednat tak, aby v co největší míře předcházely vzniku újmy a v případě, že ke vzniku újmy dojde, k její minimalizaci.

14) Žádná ze smluvních stran není povinna nahradit újmu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé smluvní strany. V případě, že Objednatel poskytl Dodavateli chybné zadání a Dodavatel s ohledem na svou povinnost poskytovat Služby s odbornou péčí mohl chybnost takového zadání zjistit, smí se ustanovení předchozí věty dovolávat pouze v případě, že na chybné zadání Objednatele písemně upozornil a Objednatel trval na původním zadání.

15) Žádná ze smluvních stran nemá povinnost nahradit újmu způsobenou porušením svých povinností vyplývajících z této Smlouvy, bránila-li jí v jejich splnění některá z překážek vylučujících povinnost k náhradě škody ve smyslu § 2913 odst. 2 občanského zákoníku.

Čl. XI– Doba trvání Smlouvy, ukončení Smlouvy a odstoupení od Smlouvy

1) Smlouva se uzavírá na dobu 48 měsíců od její účinnosti, nebo do vyčerpání částky uvedené v čl. VII odst. 1 Smlouvy, a to podle toho, která z těchto skutečností nastane dříve. Pro vyloučení pochybností se uvádí, že vyčerpáním částky dle předchozí věty se rozumí stav, kdy souhrn všech Dodavatelem uplatněných práv na zaplacení ceny bez DPH za jím poskytnutá plnění dle Smlouvy dosáhne částky uvedené v čl. VII odst. 1 Smlouvy.

2) Smlouvu je možné ukončit písemnou dohodou smluvních stran opatřenou podpisy oprávněných zástupců smluvních stran. Dohoda dle předchozí věty bude obsahovat ujednání o způsobu vypořádání vzájemných závazků.

3) Objednatel je oprávněn Smlouvu ukončit písemnou výpovědí i bez udání důvodu s výpovědní dobou 3 měsíců. Výpovědní doba počíná běžet prvním dnem kalendářního měsíce následujícího po doručení výpovědi na adresu sídla uvedenou na titulní straně Smlouvy nebo do datové schránky uvedené na titulní straně Smlouvy té smluvní strany, jíž je adresována.

4) Objednatel je oprávněn od Smlouvy odstoupit v případech podstatného porušení Smlouvy ze strany Dodavatele. Za podstatné porušení Smlouvy se mimo případy výslovně ve Smlouvě uvedené považuje též:

   a. případ, kdy je Dodavatel zařazen na některý ze sankčních seznamů dle zákona č. 69/2006 Sb., o provádění mezinárodních sankcí

   b. případ, kdy Dodavatel přestane splňovat požadavky stanovené nařízením Rady EU 2022/576 ze dne 8. dubna 2022

   c. případ, kdy se čestné prohlášení Dodavatele dle Přílohy č. 6 zadávací dokumentace ukáže jako nepravdivé

   d. případ, kdy je s Dodavatelem zahájeno insolvenční řízení ve smyslu insolvenčního zákona

   e. případ, kdy je Dodavatel pravomocně odsouzen pro trestný čin uvedený v Příloze č. 3 ZZVZ

   f. případ, kdy Dodavatel opakovaně porušuje informační povinnost dle čl. 12 Přílohy č. 9 Smlouvy, přičemž opakovaně se rozumí alespoň 3 krát

   g. případ, kdy dojde k významné změně kontroly nad Dodavatelem, přičemž kontrolou se zde rozumí ovlivnění, ovládání či řízení ve smyslu zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů (dále jen „**ZOK**“)

   h. případ, kdy u Dodavatele dojde ke změně kontroly nad zásadními aktivy Dodavatele využívanými k plnění Smlouvy

5) Odstoupení od Smlouvy dle čl. XI odst. 4 Smlouvy musí mít písemnou formu a musí v něm být uvedeno, k jakému okamžiku nastávají účinky odstoupení od Smlouvy.

6) Objednatel je oprávněn odstoupit i od Objednávky, a to v případech jejího podstatného porušení ze strany Dodavatele. V případě dle předchozí věty se přiměřeně použijí ustanovení čl. XI odst. 4 a 5 Smlouvy.

7) Ukončením Smlouvy jakýmkoli ze způsobů uvedených v čl. XI Smlouvy nejsou dotčena ustanovení týkající se smluvní pokuty, ochrany důvěrných informací, náhrady škody a jiných závazků, přetrvávajících ze své povahy i po ukončení Smlouvy.

Čl. XII – Závěrečná ustanovení

1) Smlouva nabývá platnosti dnem podpisu poslední smluvní strany a účinnosti uveřejněním v registru smluv. Uveřejnění Smlouvy v registru smluv zajistí Objednatel, to nezbavuje Dodavatele povinnosti ověřit, že byla uveřejněna v souladu se zákonem o registru smluv.

Pro vyloučení pochybností smluvní strany uvádí, že jejich dohoda na uveřejnění Smlouvy v registru smluv nevylučuje možnost Dodavatele Smlouvu v registru smluv uveřejnit, v takovém případě Dodavatel odpovídá za to, že bude uveřejněna v souladu se zákonem o registru smluv.

2) Smlouva je vyhotovena elektronicky a podepsána uznávanými elektronickými podpisy oprávněných zástupců smluvních stran. Každá smluvní strana obdrží elektronicky podepsaný originál ve formátu pdf.

3) Smlouva a vztahy smluvních stran z ní vyplývající i Smlouvou výslovně neupravené se řídí občanským zákoníkem a dalšími právními předpisy českého právního řádu.

4) V případě, že se některé ustanovení Smlouvy stane neúčinným nebo neplatným, zavazují se Smluvní strany bez zbytečného odkladu poté, co takovou skutečnost zjistí, dodatkem neúčinná nebo neplatná ustanovení Smlouvy upravit tak, aby v co nejširší míře odpovídala původnímu účelu.

5) Smluvní strany se dohodly na vyloučení aplikace ustanovení § 557 a § 1805 občanského zákoníku.

6) Smluvní strany prohlašují, že veškeré případné spory ze Smlouvy se budou řešit nejprve smírně a teprve selže-li tento způsob, obrátí se na věcně a místně příslušný soud v České republice.

7) Smluvní strany prohlašují, že Smlouva představuje jejich úplnou dohodu o předmětu Smlouvy a všech náležitostech, které smluvní strany měly a chtěly ve Smlouvě ujednat, a které považují za důležité pro závaznost Smlouvy. Žádný projev smluvních stran učiněný při jednání o Smlouvě nebo po jejím uzavření nesmí být vykládán v rozporu s ustanoveními Smlouvy a nezakládá závazek žádné ze smluvních stran.

8) Změny Smlouvy je možné činit pouze na základě dohody smluvních stran ve formě písemných vzestupně číslovaných dodatků opatřených podpisy oprávněných zástupců smluvních stran.

9) Nedílnou součástí Smlouvy jsou i její přílohy:

- Příloha č. 1 – Specifikace průběžně poskytovaných služeb a jednorázově poskytovaných služeb
- Příloha č. 2 – Přehled modulů a licencí
- Příloha č. 3 – Realizační tým
- Příloha č. 4 – Politika provozní bezpečnosti MZ
- Příloha č. 5 – Ceník
- Příloha č. 6 – Obchodní tajemství
- Příloha č. 7 – Seznam poddodavatelů
- Příloha č. 8 – Pravidla pro zpracování osobních údajů
- Příloha č. 9 – Pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací podle § 8 odst. 1 písm. a) a d) VoKB

10) Smlouva je projevem svobodné, vážné, určité a omylu prosté vůle smluvních stran a není uzavírána v tísni ani za jednostranně nápadně nevýhodných podmínek, což smluvní strany stvrzují podpisy svých oprávněných zástupců.

V Praze dne

V Jihlavě dne „dle data e. podpisu“

[redacted]

Příloha č. 1 - Specifikace průběžně poskytovaných služeb a jednorázově poskytovaných služeb

Správa elektronického systému spisové služby GINIS Standard (dále jen „**eSSL**“) včetně maintenance, která zahrnuje poskytování update a zajišťující legislativní rozvoj systému a další služby, které jsou vymezeny v této Specifikaci.

Legislativním rozvojem systému se rozumí, že eSSL bude po celou dobu trvání Smlouvy v souladu s platnými právními předpisy České republiky a technickými normami vztahujícími se k předmětu jeho plnění, přičemž se Dodavatel zavazuje provádět všechny své závazky vyplývající ze Smlouvy tak, aby nenarušil a zejména zajistil řádný provoz eSSL. Řádným provozem eSSL se rozumí takový provoz, který je bez legislativních a technických závad.

Služba se vztahuje na rozsah produktů eSSL dle Přílohy č. 2 Smlouvy.

A Průběžně poskytované služby – podpora eSSL (produkční i testovací prostředí)

Dodavatel poskytne v rámci **ceny za jeden kalendářní měsíc poskytování průběžně poskytovaných služeb** následující služby:

1. Správa systému eSSL
   - 1.1 Standardní správa/administrace eSSL a jeho produktových částí
   - 1.2 Incident management
   - 1.3 Údržba systému
     - 1.3.1 Standardní údržba
     - 1.3.2 SW maintenance
   - 1.4. Provedení legislativního update systému
2. Technická a metodická podpora oprávněným pracovníkům Objednatele na pracovišti Objednatele – řešení požadavků
   - 2.1. Podpora v souvislosti se správou systému
   - 2.2. Konzultace
3. Školení uživatelů / zaměstnanců Objednatele

B Jednorázově poskytované služby – podpora eSSL hrazená nad rámec průběžně poskytovaných služeb, kterými jsou:

1. Servisní služby
2. Provádění update na základě úpravy vyžádané Objednatelem
3. Technická podpora
4. Školení

Ad A) Průběžně poskytované služby – podpora eSSL (produkční i testovací prostředí). Pro testovací prostředí platí stejná podpora eSSL jako pro produkční prostředí s výjimkou služby uvedené v bodě 1.2 Incident management. Testovací prostředí bude využito i pro školící účely Objednatele.

1. **Správa eSSL**:

1.1 **Standardní správa/administrace eSSL** (jednotlivých uživatelských modulů) pro provozované multilicence a licence eSSL (*nezahrnuje administraci koncových uživatelů a správu koncových PC)* vč. zajištění průběžné aktualizace funkcí závislých na třetí straně (reakce na změnu stávajícího SW třetí strany), podporu rozhraní Czech Point (Modul RAK) - viz Příloha 2 Smlouvy. Dodavatel je povinen v rámci správy IS proaktivně prověřovat stav IS a na zjištěné informace o stavu systému reagovat dle vlastního uvážení s odbornou péčí a podle svých nejlepších znalostí a schopností tak, aby byl zachován řádný provoz. O těchto skutečnostech je Dodavatel povinen neprodleně informovat Objednatele. Dále je Dodavatel povinen upozornit Objednatele na případnou existenci nedostatků a rizik v souvislosti s provozem eSSL. Současně je Dodavatel povinen poskytovat úplné aktualizované dokumentace k systému v souladu s platnou legislativou (1x ročně) a průběžně poskytovat dokumenty s informacemi o provedených změnách, a to po každé provedené změně. Objednatel bude mít možnost v závislosti na provedených změnách provést uživatelské testování.

1.2 **Incident management** – garantovaná doba reakce na incident a zprovoznění systému;

a) Popis služby

Služba zahrnuje aplikační podporu:

- zpracování měsíčních reportů obsahujících požadavky, incidenty a problémy ve vztahu ke sjednaným SLA (doba reakce a doba obnovení služby);
- vrcholovou administraci eSSL (úložišť el. dokumentů, parametrizace systému, správa aktuálních programových modulů, distribučních sad a sestav);
- řešení incidentů;
- proaktivní průběžné monitorování IS eSSL prostřednictvím dohledového nástroje Dodavatele;
- preventivní údržba a ladění IS eSSL prováděná minimálně 1x měsíčně (kontrola logů a databázových reportů, optimalizace nastavení, údržba apod.);
- poskytování podpory SW vzdáleným přístupem, osobní účastí na pracovišti, telefonicky, e-mailem;
- služba HelpDesk a Hot-line pro hlášení závad dle jednotlivých kategorií, řešení technických problémů, poradenství a konzultace v režimu 8x5 (tj. 8 hodin v pracovní době, v pracovních dnech, pracovní doby viz dále).

b) Obsah služby

Služba se vztahuje na aplikaci eSSL.

- incidenty jsou řešeny pro systém eSSL (systém, servery, databáze) a referenční PC.

c) Parametry služby

Podpora platí v pracovní dny od 8:00 do 16:00 (dále tako jako „**pracovní doba**“) pro produkční prostředí):

- reakční doba pro započetí řešení a lhůta pro odstranění závad nebo zprovoznění systému úrovně V1 až V3 jednotlivých úrovní závad je uvedena níže v Tabulce č. 1.

Úroveň	Popis charakteru závady	Reakční doba	Lhůta pro vyřešení závady nebo zprovoznění systému
V1	SW nelze z důvodu závady produktu eSSL vůbec provozovat nebo má závada produktu kritický vliv na funkcionalitu elektronické spisové služby, totální výpadek, závada vyžaduje okamžité řešení.	do 1 hodiny v pracovní době	do 4 hodin od nahlášení incidentu
V2	Závada produktu eSSL výrazně omezuje správnou funkcionalitu aplikace, avšak elektronickou spisovou službu je možné s omezením provozovat.	do 1 hodiny v pracovní době	do 12 hodin od nahlášení incidentu
V3	Drobné vady, (vady, které nejsou vadami úrovně V1 a V2)	do 1 hodiny v pracovní době	max. do 10 pracovních dnů od nahlášení incidentu

Tabulka č. 1 – Popis jednotlivých úrovní závad, reakční doby a odstranění závad nebo zprovoznění systému

Reakční dobou je míněn maximální čas, ve kterém je Dodavatel povinen zareagovat na nový záznam v systému správy incidentů (helpdesk) nebo po prokazatelném nahlášení incidentu Objednatelem. V případě nefunkčnosti helpdesku musí Dodavatel zajistit náhradní řešení.

Vyřešením závady se rozumí odstranění poruchy/závady trvalým případně dočasným řešením, přičemž v případě dočasného řešení bude postupováno ze strany Dodavatele následovně:

- poskytnout Objednateli návrh dočasného řešení;
- sdělit Objednateli postup dočasného řešení a řešení realizovat;
- zpracovat pro Objednatele postup cílového řešení s termínem vyřešení incidentu a po odsouhlasení řešení ze strany Objednatele řešení realizovat;

V případě zapojení třetí strany je třeba informovat Objednatele o odpovědi na eskalaci problému u třetí strany (v případě produktů třetích stran) a poskytnout návrh dočasného řešení.

V obou případech je Dodavatel povinen zajistit spokojenost uživatele.

d) Akceptační kritéria

Podkladem pro akceptaci plnění služby je **Zpráva o stavu systému** obsahující vyjádření o dostupnosti systému za uplynulý kalendářní měsíc v členění dle Tabulky č. 1.

1.3 **Údržba systému**

1.3.1 **Standardní údržba – součástí správy eSSL**: činnost prováděná u plně funkčního systému s cílem zachovat funkčnost, případně adaptovat systém na měnící se podmínky tak, aby funkčnost byla zachována, systém není v rámci údržby rozvíjen

Průběžná preventivní kontrola a údržba eSSL zejména: preventivní údržba a ladění eSSL prováděné minimálně 1 x měsíčně (optimalizace nastaveni); průběžná týdenní kontrola logů a databázových reportů; průběžná kontrola a monitorování rozhraní, monitor nestandardních pracovních postupů a činností dle požadavku Objednatele (délku trvání monitoringu a jeho specifikaci určí Objednatel), údržba aplikačního, databázového serveru, úložišť elektronických dokumentů a programových modulů.

1.3.2 **SW maintenance**

Služba zahrnuje dodání pravidelných i mimořádných updatů a patchů eSSL. Maintenance zahrnuje rovněž i dodání update vytvořených v souvislosti se změnami či úpravami příslušných právních předpisů České republiky a přímo použitelných předpisů EU a podporu spojenou s konzultacemi.

Veškeré změny budou podchyceny ve změnovém dokumentu provedené analogicky dle bodu A, 1.1.

a) Popis služby:

Služba v rámci eSSL zahrnuje:

- dodání pravidelných i mimořádných updatů a patchů eSSL;
- dodání update vytvořených v souvislosti se změnami či úpravami příslušných právních předpisů České republiky a přímo použitelných předpisů EU;
- poskytnutí podpory (rad a informací) ke správnému a efektivnímu provozování a užití dodaných modulů eSSL v pracovní době prostřednictvím kontaktu technické podpory aplikace HelpDesk oprávněnému pracovníkovi Objednatele s garantovanou dobou odezvy max. do 8 hodin od nahlášení. V případě doby odezvy 8 hodin se jedná o 8 hodin v pracovní době. Nejedná se o konzultace podle bodu 2.2.

-

b) Obsah dodávky služby:

Služba se vztahuje na aplikaci eSSL.

c) Parametry služby

Parametry služby:

- instalace na servery eSSL, dodávání instalačních CD k eSSL. Případně umístění instalace do úložiště a informování oprávněného pracovníka Objednatele;
- dodání dokumentu s popisem změn současně s dodáním aktualizace IS eSSL – aplikace;
- poskytnutí rad ke správnému a efektivnímu provozování a užití dodaných modulů eSSL v pracovní době prostřednictvím kontaktu technické podpory oprávněnému pracovníkovi Objednatele (doba odezvy není garantována).

1.4. **Provedení legislativního update** – 1x / rok

- v případě, že zajištění legislativního rozvoje vyžaduje provedení update, bude tato služba Dodavatelem zajištěna 1x /rok v rámci ceny za jeden kalendářní měsíc poskytování průběžně poskytovaných služeb.

2. **Technická a uživatelská podpora** oprávněným pracovníkům Objednatele na pracovišti Objednatele – řešení požadavků

- informační a konzultační činnost: asistence při instalaci softwaru, řešení systémových problémů, vysvětlení chybových hlášeni, návrh opravných opatření, zodpovězení obecných otázek na použití softwaru, objasnění jednotlivých funkcí IS, spolupráce na řešení problémů, ladění systému, podpora při řešení změn. Nejedná se o přímou činnost v rámci IS, pouze s provozováním IS souvisí. Technická podpora může být poskytována na vyžádání oprávněného pracovníka Objednatele (viz dále konzultace v rámci vyhrazených člověkohodin na konzultace v rámci ceny za jeden kalendářní měsíc poskytování průběžně poskytovaných služeb za služby), anebo z iniciativy dodavatele např. jako poskytované rady a informace v souvislosti s běžnou údržbou systému (v rámci ceny za jeden kalendářní měsíc poskytování průběžně poskytovaných služeb).

2.1 Podpora v souvislosti se správou systému (standardní správou, incident managementem, údržbou, řešením požadavků) – bude poskytována jako:

a) reakce na dotaz nebo žádost o informaci v pracovní době prostřednictvím HelpDesku, telefonicky nebo e-mailem oprávněného pracovníka Objednatele;

b) podpora z iniciativy Dodavatele v souvislosti s poskytováním správy systému prostřednictvím HelpDesku, telefonicky nebo e-mailem oprávněnému pracovníkovi Objednatele (např. zaslání preventivních doporučení Objednateli, poskytnutí rad ke správnému a efektivnímu provozování a užití dodaných modulů eSSL);

c) podpora v souvislosti s update systému: formou poskytováni informací, rad a zaškoleni v přímé souvislosti s provedením update vzdáleným přístupem, telefonicky, nebo e-mailem oprávněnému pracovníkovi Objednatele.

2.2 Konzultace v rozsahu 5 člověkohodin za kalendářní měsíc (jako součásti ceny za jeden kalendářní měsíc poskytování průběžně poskytovaných služeb) – za „metodickou podporu" a za „technickou podporu" oprávněným osobám Objednatele – poskytováním informací (zaškolením) na pracovišti Objednatele nebo formou telefonickou. Čerpání člověkohodin bude vykazováno v kalendářním měsíci, ve kterém bylo objednáno. Dodavatel umožní automatickou kumulaci (tedy převod hodin do následujícího kalendářního měsíce v případě, že v daném kalendářním měsíci nebudou hodiny v rámci ceny za jeden kalendářní měsíc poskytování průběžně poskytovaných služeb vyčerpány, a to po celou dobu platnosti Smlouvy). Počet člověkohodin technické podpory nebude snižován o počet člověkohodin věnovaných realizaci mimořádných požadavků formou Objednávek ani odpovědí na dotazy nebo žádosti o informace dle bod 2.1, písm. a).

3. **Školení uživatelů Objednatele**

- školení realizovaná ze strany Dodavatele v rozsahu 6 hodin (každá 60 minut) v jednom kalendářní měsíci. Čerpání člověkohodin bude vykazováno v kalendářním měsíci, ve kterém bylo objednáno. Dodavatel umožní automatickou kumulaci (tedy převod hodin do následujícího kalendářního měsíce v případě, že v daném kalendářním měsíci nebudou hodiny v rámci ceny za jeden kalendářní měsíc poskytování průběžně poskytovaných služeb vyčerpány, a to po celou dobu platnosti Smlouvy).

Ad B) Jednorázově poskytované služby – podpora eSSL hrazená nad rámec průběžně poskytovaných služeb stanovených v bodu A.

Jedná se o jednorázově poskytované služby za cenu dle sazebníku (Cenový koš zakázky), v předpokládaném rozsahu 192 hodin za období jednoho kalendářního roku.

Práce podle požadavku Objednatele na základě Objednávky. Objednávka bude Objednatelem vystavena na základě předběžné a detailní kalkulace, potřeby časové náročnosti práce předložené Objednateli Dodavatelem.

1. **Servisní služby, činnosti a ad-hoc služby** uvedené v Tabulce „Cenový koš zakázky“ v Příloze č. 5 Smlouvy, a poskytované na základě požadavku ze strany Objednatele formou mimořádných Objednávek.

Reakční doba a doba řešení pro jednotlivé stupně požadavků je uvedena v Tabulce č. 2.

Stupeň	Popis charakteru požadavku	Reakční doba	Doba řešení požadavku
P1	Splnění požadavku je možné změnou nastavení Systému	do 1 pracovního dne od obdržení požadavku	Dle dílčí Objednávky, nejpozději do 10 pracovních dnů od obdržení požadavku
P2	Splnění požadavku je možné změnou kódu Systému	do 1 pracovního dne od obdržení požadavku	Dle dílčí Objednávky

Tabulka č. 2 - Popis charakteru požadavku

2. **Provádění update na základě úpravy vyžádané Objednatelem** nad rámec ceny za jeden kalendářní měsíc poskytování průběžně poskytovaných služeb

   Služba je umožněna vzdáleným přístupem, osobní účastí na pracovišti, a zahrnuje na základě Objednávky:

   - podporu při provádění update a patchů eSSL (tj. při instalaci, testování, přejímce a uvedení do ostrého provozu), spolupráce na řešení problémů, ladění systému a podpoře při řešení změn, včetně změn nastavení s vlivem na ostatní provozované systémy;
   - vytvoření nové instalační sady aplikace pro Objednatele;
   - instalace na servery eSSL.

3. **Technická podpora** oprávněným pracovníkům Objednatele na pracovišti Objednatele nad rámec ceny za jeden kalendářní měsíc poskytování průběžně poskytovaných služeb na základě požadavku Objednatele formou mimořádných Objednávek.
4. **Školení** uživatelů / zaměstnanců Objednavatele nad rámec ceny za jeden kalendářní měsíc poskytování průběžně poskytovaných služeb na základě požadavku Objednatele formou mimořádných Objednávek.

   Skladba provedených prací dle bodů 2, 3 a 4 bude pro jednotlivé případy sestavena a kalkulována ze základních činností viz Příloha č. 5 Smlouvy.

Příloha č. 2 – Přehled modulů a licencí

p.č.	Zkratka	Název	Počet licencí
1	ADM	verze 1.7 dle smlouvy GOR-S 9412-0001 byla upgradovana	1
2	ADM	server - zdr.licence neomezená Jádro systému GINIS	1
3	ADM	klient T - ADM	2
4	AKC	klient T - AKC Kontrola vazeb ADM	1
5	ADM	rozšíření pro práci s elektronickým podpisem	1
6	ADM	rozšíření pro práci s elektronickými dokumenty	1
7	ADK	klient T - ADK správa kartotéky externích subjektů	2
8	USU	klient T - USU / Multilicence v budově MZ a Rozšíření USU - el. dok.	1
9	POD	klient T - POD	9
10	TPD	klient T - TPD Gen. podacích deníků	1
11	GINMAS01	automat - GINMAS01	1
12	VYP	klient T - VYP	9
13	VED	klient T - VED	7
14	SPI	server - zdr.licence	1
15	SPI	klient T - SPI	3
16	UKO	server - zdr.licence neomezená	1
17	UKO	klient T - UKO	10
18	UKO	klient T - UKO – multilicence 100	1
19	POD	server - ePOD	1
20	VYP	server eVYP - elektronická výpravna	1
21	XRG ISDS	XRG - DSC Rozhraní na datové schránky a reg. konv.	1
22	ZUD	ZUD rozesílání generovaných sestav HH	1
23	ZUD	ZUD rozesílání avizací termínů	1
24	EVS	EVS - elektronický vzdělávací systém server do 500 osob	1
25	EVS	klient EVS	500
26	EVS	EVS - AVS server do 500 osob	1
27	EVS	klient T - AVS administrace EVS	2
28	RAK	RAK server - zdr.licence neomezená	1
29	RAK	klient T - RAK	9
30	RAK	RAK napojení na centrální registr konverzí XRG-DSC	1
31	Sken GSL	Sken server do 50 tis. dokumentů	1
32	Sken GSL	Instalace GSL (3 vstupy)	1
33	Sken GSL	Sken OCR server do 20 tis. stran A4 za měsíc	1
34	SUD	Rozšíření spisovny - modul SUD - server (do 60.000 dok.)	1
35	SUD	Klient modul SUD	2
36	PAR	Rozšíření spisovny - modul PAR - server (do 60.000 dok.)	1
37	PAR	Klient modul PAR	2
38	ESR	Rozšíření spisovny - modul ESR - server (do 60.000 dok.)	1
39	ESR	Klient modul ESR	2
40		Napojení GINISu na ISZR - web. služby	1

41	EPK	Klient Elektronická podpisová kniha	50
42		Možnost nastavení sekundárního/náhradního konverzního pluginu	1
43		Nastavení vizualizace elektronického podpisu uvnitř PDF	1
44		Fulltextové hledání v metadatech/evidenčních položkách dok./spisů	1
45		Zobrazení miniatur elektronických dokumentů	1
46		Možnost exportu el. dokumentů a spisů v rámci rozluky	1
47	XRG	Licence pro registr CHLAP a KOPr	2
48		Vizualizace el. podpisu	1
49		Rozhraní úřední desky pro 1 reg řešení - Licence rozšíření - zveřejňování	1
50	UDE	XRG-UDE - rozhraní úřední desky pro jedno registrované řešení	1
51	UDA	Klient Licence modul administrace UDA Správa úřední desky	1
52	DKS	Konverzní server ABBYY ke skeneru - Bez OCR	1
53	DKS	Konverzní server - MS Office	1
54	DKS	ABBYY FineReader Engine 11 Professional Runtime License - do 10.000 dokumentů za měsíc, bez OCR	1
55	ADS	Klient - ADS Adm. Sestav	1
56	XRG	XRG rozhraní pro JEHLA	1
57	XRG	XRG rozhraní pro IS OPL	1
58	XRG	XRG rozhraní pro Intranet	1
59		Frankovací stroj Licence 1730 304 rozšíření rozšířené napojení 2D	1
60	Sken GSL	Upgrade Sken OCR na roční 500 tis. stran za rok	1
61	SPI	klient SPI	1
62	DKS	rozšíření - EML konvertor (aplikační)	1
63	DKS	rozšíření - ZFO konvertor (aplikační)	1
64	DKS	rozšíření - MSG konvertor (aplikační)	1
65	DRMS	rozšíření - hromadná oprava metadat	1

MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Příloha č. 3 – Realizační tým

Člen týmu č. 1

Jméno a příjmení:

E-mail:

Telefon/mobil:

Člen týmu č. 2

Jméno a příjmení:

E-mail:

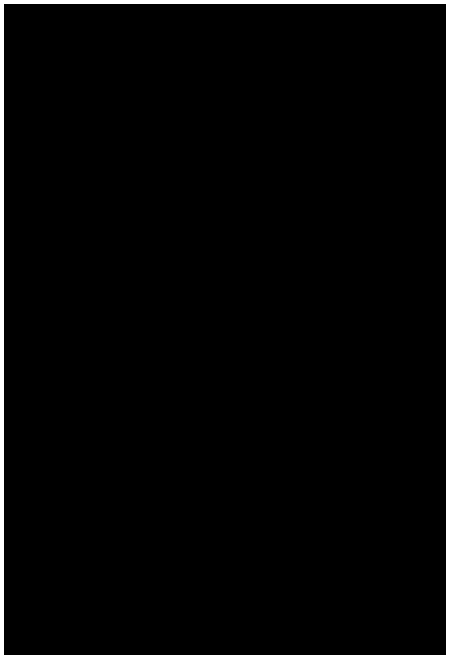
Telefon/mobil:

Člen týmu č. 3

Jméno a příjmení:

E-mail:

Telefon/mobil:



Příloha č. 4 – Politika provozní bezpečnosti MZ

Ministerstvo zdravotnictví České republiky Palackého nám. č 4, 128 01 Praha 2, IČ: 00024341	
	**Verze:** **v2/01** Platnost nové verze od: 27.3.2019 Spisový znak: 06.7.8 Skartační znak a lhůta: V/5

Politika provozní bezpečnosti, poskytování a nabývání licencí programového vybavení a informací MZ ČR

Implementace zákona č. 181/2014 Sb., o kybernetické bezpečnosti

Pořadí revize	Provedené dne	Zpracoval	Schválil
0.	08. 12. 2016	[redacted]	
1.	27. 3. 2019		
Podpis			

Obsah

Seznam zkratek a pojmů

Zkratka	Význam
MZ ČR	Ministerstvo zdravotnictví České republiky
ČR	Česká republika
IDM	Identity Management, správa identit (uživatelských účtů)
SIEM	Security Information and Event Management
IS	Informační systém
ICT	Informační a komunikační technologie
SLA	Service Level Agreement, Dohoda o úrovni poskytované služby
SW	Software
IDS	Intrusion Detection System, Sytém na detekci narušení bezpečnosti perimetru
IPS	Intrusion Prevention System, Sytém pro předcházení narušení bezpečnosti perimetru
CD	Compact Disc, paměťové médium
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
Sb.	Sbírka zákonů České republiky
DVD	Digital Versatile Disc, paměťové médium
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost

1 Úvod

Ministerstvo zdravotnictví je ústředním orgánem státní správy pro zdravotní služby, ochranu veřejného zdraví, zdravotnickou vědeckovýzkumnou činnost, poskytovatele zdravotních služeb v přímé řídící působnosti, zacházení s návykovými látkami, přípravky, prekursory a pomocnými látkami, vyhledávání, ochranu a využívání přírodních léčivých zdrojů, přírodních léčebných lázní a zdrojů přírodních minerálních vod, léčiva a prostředky zdravotnické techniky pro prevenci, diagnostiku a léčení lidí, zdravotní pojištění a zdravotnický informační systém, pro používání biocidních přípravků a uvádění biocidních přípravků a účinných látek na trh. Jako takové vyhlašuje zásady bezpečnosti informací platné pro resort zdravotnictví.

Tato Politika provozní bezpečnosti, poskytování a nabývání licencí programového vybavení a informací je vypracována v souladu s požadavky definovanými v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících předpisů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a jeho prováděcích předpisech.

1.1 Závaznost politiky

Tato politika je závazná pro všechny zaměstnance dotčených organizací resortu MZ ČR a spolupracující organizace. Jednotlivé dotčené organizace v rámci resortu MZ ČR mohou vytvářet vlastní verzi této politiky, ta však musí být vždy v souladu s Bezpečnostní politikou informací MZ ČR a dalšími závaznými dokumenty.

1.2 Revize politiky

Tato politika podléhá revizi nejméně jednou ročně. Za provedení revize dokumentu odpovídá Architekt kybernetické bezpečnosti, finální verzi dokumentu schvaluje Výbor pro řízení kybernetické bezpečnosti.

Záměrem vedení MZ ČR je udržovat přiměřenou ochranu informačních aktiv v souladu se zákony a jinými právními předpisy ČR, a to i v případech, kdy byla odpovědnost za zpracování informací přenesena na spolupracující organizace.

2 Politika provozní bezpečnosti

2.1 Řízení bezpečnosti komunikací a provozu

Účelem řízení bezpečnosti komunikací a provozu je zajistit správný a bezpečný provoz prostředků pro zpracování informací, minimalizovat riziko selhání systému, chránit integritu a dostupnost programů, dat a informačních systémů, chránit důvěrnost informací a zajistit ochranu počítačových sítí.

2.1.1 Pravomoci a odpovědnosti spojené s bezpečným provozem

Za řízení provozu informačního systému odpovídá představený organizačního útvaru informačních a komunikačních technologií. Tuto pravomoc je možné dále delegovat.

Za bezpečnost provozu a zejména za řízení kybernetické bezpečnosti odpovídá Manažer kybernetické bezpečnosti.

2.1.2 Postupy bezpečného provozu

Pro řízení, správu a monitorování aktiv informačního systému jsou vytvořeny pracovní postupy, respektující bezpečnostní zásady, stanovené bezpečnostní politikou MZ ČR a bezpečnostní požadavky, stanovené vlastníky dat. Pracovní postupy jsou dostupné všem dotčeným osobám. Pracovní postupy podléhají pravidelným revizím a jejich změna probíhá prostřednictvím změnového řízení.

Je přísně zakázáno instalovat a provozovat v informačním systému programy, které nebyly schváleny k provozu v produkčním systému. Veškeré zkoušení a testování programů probíhá na testovacím systému.

Organizace se aktivně brání proti vlivu škodlivých programů, chybám v programech a ztrátě dat. Data, která jsou uložena ve vyhrazených prostorech, jsou chráněna a zálohována. Všechny zveřejněné chyby programů jsou co nejdříve opraveny. Provoz IS je monitorován a záznamy jsou archivovány a pravidelně vyhodnocovány.

Nákup služeb, potřebných pro zajištění provozu IS, probíhá výhradně na základě písemných smluv s jasně stanovenými a měřitelnými kritérii dodávek.

2.1.3 Požadavky a standardy bezpečného provozu

Všechny platné legislativní i smluvní požadavky na zajištění bezpečnosti informací jsou dokumentovány a aktivně využívány při tvorbě interních předpisů, souvisejících s provozem informačního systému a zejména se sdílením a zveřejňováním dat.

Všechny řídicí dokumenty v oblasti bezpečnosti provozu ICT jsou podřízeny jednotné formě řízení dokumentace. Řízení dokumentace jednoznačně určuje správce každého dokumentu, platnost dokumentu, strukturu dokumentu, osoby a útvary, podílející se na schválení dokumentu a pravidla pro manipulaci s dokumentem.

Řídicí dokumenty v oblasti bezpečnosti provozu ICT jsou v závislosti na oblasti působnosti rozděleny do tří základních úrovní:

- řídicí dokumenty, zastřešující celkovou koncepci v oblasti bezpečnosti provozu ICT v závislosti na strategických cílech organizace, související legislativě a přijatých závazcích a standardech,
- řídicí dokumenty, zajišťující jednotné prosazení informační bezpečnosti u aktiv informačního systému jako celku a definující základní struktury, standardy a vazby, vytvořené pro zajištění požadované úrovně informační bezpečnosti,
- řídící dokumenty, které zajišťují prosazení informační bezpečnosti specificky pro jednotlivá aktiva (služby) informačního systému a jejich konkrétního nasazení, včetně způsobu pořízení a vyhodnocování provozních záznamů. Řídicí dokumenty pokrývají celý životní cyklus aktiva. Provozní záznamy musí mimo jiné obsahovat průkazné a doložitelné záznamy manažerských rozhodnutí, vztahujících se k danému aktivu, a musí být možno přezkoumat jejich soulad s bezpečnostními politikami, zásadami a předpisy.

2.1.4 Řízení technických zranitelností

V rámci provozní podpory ICT musí být realizováno řízení technických zranitelností. To zahrnuje jak technické zranitelnosti spojené s bezpečnostním nastavením jednotlivých zařízení, tak s aplikací bezpečnostních záplat a aktualizací operačních systémů a všech softwarových aplikací. Postupy nápravy odhalených zranitelností se řídí kategorizací zařízení (v souladu s dopady jeho vyřazení či kompromitace pro informační bezpečnost jako celek), které je danými zranitelnostmi zasaženo.

Náprava odhalených zranitelností může zahrnovat některé z následujících kroků:

- Nasazení patchů nebo upgrade zranitelného software (plán implementace by měl zahrnovat testování patchů/upgrade)
- Náhrada software obsahujícího zranitelnosti za jinou aplikaci
- Konsolidace prostředí nebo přesun do jiného prostředí
- Změna konfigurace systému:
    - Znepřístupnění nebo vypnutí zranitelných služeb
    - Znepřístupnění nebo vypnutí specifických zranitelných funkcí nebo schopností v rámci dané služby
- Nastavení, změna nebo užití silnějších (komplexnějších) hesel
- Omezení přístupu pomocí firewallu nebo filtrů
- Zvýšený monitoring zaměřený na detekci anomálií
- Zvýšení vědomí uživatelů o dané zranitelnosti

V závislosti na naléhavosti, se kterou je třeba technickou zranitelnost řešit, by měla být opatření k odstranění zranitelnosti aplikována buď v souladu s pravidly standardního změnového řízení, nebo případně s pravidly pro řešení bezpečnostních incidentů či jinými eskalačními postupy.

V případě zranitelností s vysokou mírou rizika a rozsáhlým dopadem do ICT infrastruktury stanoví Manažer kybernetické bezpečnosti ve spolupráci se správci dotčených technických aktiv s přihlédnutím k průběžnému provoznímu riziku a možnostem jeho zmírnění

předpokládaný časový harmonogram nápravy. Tato povinnost se týká zejména zranitelností, které jsou aktivně zneužívány, nebo u kterých toto zneužití bezprostředně hrozí. Mezi hlavní možnosti zmírnění rizika patří např. nasazení patchů zranitelných systémů, znepřístupnění či vypnutí služeb, nasazení filtrů na hranici perimetru. Konečné rozhodnutí o způsobu řešení dané situace přijme Manažer kybernetické bezpečnosti a následně jej komunikuje všem dotčeným pracovníkům odpovídajícím způsobem.

Povinností Manažera kybernetické bezpečnosti a Garantů technických aktiv je zejména:

- Náprava či zmírnění dopadů technických zranitelností s ohledem na kategorizaci dotčených zařízení
- Správa programu řízení technických zranitelností pro svěřenou oblast
- Posouzení míry rizika spojené s jednotlivými zranitelnostmi a jejich komunikace s odpovědnými pracovníky vč. návrhu plánu opatření ke zmírnění či eliminaci rizika
- Sledování bezpečnostních informací a informací od dodavatelů popisujících technické zranitelnosti

2.1.5 Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů

Audit kybernetické bezpečnosti a bezpečnostní testy musí vždy provádět osoba kvalifikovaná k této činnosti a současně kvalifikovaná k provádění auditu nebo testování technických zařízení.

Audity a bezpečnostní testy musí být plánovány v souladu s provozními možnostmi všech dotčených systémů tak, aby nedošlo, je-li to možné, k ohrožení provozu jak z pohledu jeho kontinuity a stanovených SLA, tak z pohledu bezpečnosti. O provádění auditu musí být informováni s dostatečným předstihem všichni dotčení pracovníci zajišťující provozní podporu dotčených systémů a s prováděním auditu musí vyslovit souhlas Manažer kybernetické bezpečnosti.

Audit kybernetické bezpečnosti a provozní testy není možné provádět v době, kdy probíhá bezpečnostní incident, případně kdy jsou aplikována neodkladná opatření ke zmírnění dopadů technických zranitelností.

2.2 Řízení změn

V rámci řízení změn jsou:

a) přezkoumávány možné dopady změn,
b) určovány významné změny.

U významných změn se provádí:

a) dokumentace jejich řízení,
b) analýza rizik,
c) přijímaní opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami,
d) aktualizace bezpečnostní politiky a bezpečnostní dokumentace,
e) zajištění jejich testování,
f) zajištění možnosti navrácení do původního stavu.

Na základě výsledků analýzy rizik je v případě KII a PZS možno rozhodnout o provedení penetračního testování nebo testování zranitelností a následně reagovat na nedostatky, zjištěné při testování.

2.3 Řízení přístupu

Účelem řízení přístupu k informacím a prostředkům informačních systémů organizace je zajistit, aby k nim měli přístup pouze oprávnění uživatelé. Pro přístup k těmto prostředkům jsou stanovena pravidla, která určují postupy pro autorizaci, zřizování, změny a odebírání přístupových práv.

2.3.1 Princip minimálních oprávnění

Oprávnění ke všem informačním aktivům jsou přidělována uživatelům, programům či procesům ne nejnižší možné úrovni, která umožní jejich správnou funkci. Všichni uživatelé v libovolném čase pracují s nejnižšími možnými oprávněními stejně jako aplikace jimi spouštěné.

2.3.2 Požadavky na řízení přístupu

Řízení přístupu probíhá na bázi skupin a rolí. Jsou definovány procesy přidělování a správy oprávnění, v pravidelných intervalech je prováděn audit přidělených oprávnění a jsou odstraňovány účty nebo sady oprávnění, které nejsou v souladu s politikou řízení přístupových oprávnění, především pak s principem minimálních oprávnění (viz výše).

2.3.3 Životní cyklus řízení přístupu

Pro řízení životního cyklu řízení přístupů k prostředkům ICT je provozován jednotný identity management systém (IDM), pomocí kterého probíhá řízení a automatizace celého životního cyklu identit. Systém IDM zajišťuje kontrolu nad tokem a využitím informací s cílem zamezit jejich neoprávněnému použití a zcizení.

2.3.4 Řízení privilegovaných oprávnění

Privilegované (administrátorské) účty budou přidělovány takovým způsobem, aby byla zajištěna jednoznačná auditovatelnost všech kroků provedených pod těmito účty ve vztahu ke konkrétním osobám.

Všechny aktivity privilegovaných účtů budou logovány a logy budou ukládány tak, aby byla vyloučena možnost jejich pozměnění či odstranění.

Budou zváženy možnosti implementace řešení pro správu privilegovaných účtů na bázi datového trezoru, případně jiné technické či organizační prostředky pro zvýšení odolnosti proti zneužití privilegovaných účtů či jejich kompromitaci.

2.3.5 Řízení přístupu pro mimořádné situace

V případě mimořádní situace je přípustné dočasné přidělení privilegovaných oprávnění v rozsahu nutném pro zvládání mimořádné situace, aplikaci nápravných opatření či nastolení normálního stavu pracovníkům či dodavatelům, kteří těmito oprávněními standardně nedisponují. Rozhodnutí o přidělení mimořádných oprávnění spadá do kompetence

Manažera kybernetické bezpečnosti, takové rozhodnutí musí být spolu s rozsahem přidělených oprávnění řádně zdokumentováno.

Poté, co pominuly důvody udělení mimořádných oprávnění, musí být dosaženo původního stavu a proveden úplný audit oprávnění v rámci informačního systému.

Všechny aktivity účtů, kterým byla přidělena mimořádná oprávnění, budou logovány a logy budou ukládány tak, aby byla vyloučena možnost jejich pozměnění či odstranění.

2.3.6 Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách

V rámci správy identit je zaveden proces pravidelné revize (auditu) přidělených oprávnění a jejich využívání, jehož cílem je zajištění trvalého souladu přidělených oprávnění s pracovními úkoly uživatelů, udržení konzistentního modelu oprávnění, kontroly přístupů ke skupinovým účtům a dalších parametrů přispívajících k zajištění bezpečnosti spravovaných dat a informací.

2.4 Politika bezpečného chování uživatelů

Uživatelé jsou povinni dodržovat veškerá metodická doporučení, postupy a zohledňovat další informace související se zajištěním bezpečnosti informací a systémů IS MZ ČR. Současně jsou všichni uživatelé informačních systémů MZ ČR povinni všímat si a hlásit jakákoliv slabá místa bezpečnosti informací v systémech nebo službách nebo podezření na ně.

2.4.1 Pravidla pro bezpečné nakládání s aktivy

Uživatel nesmí šířit a vědomě používat software získaný v rozporu s právními předpisy, zejména s autorským zákonem a software, získaný v souladu s těmito předpisy nesmí užívat v rozporu se smlouvou, kterou autor softwaru udělil svolení k jeho užití.

Uživatel smí používat počítačové prostředky jen v rámci své pracovní náplně. Je zakázáno používat aktiva informačního systému pro osobní nebo komerční účely.

Je zakázáno kopírovat a distribuovat části operačního systému a nainstalovaných aplikací a programů. Programy je možné používat jen na takovou činnost, na kterou jsou určené.

2.4.2 Bezpečné použití přístupového hesla

Uživatelé jsou povinni respektovat pravidla tvorby a nakládání s přístupovými hesly. Zejména uživatelé odpovídají za zachování důvěrnosti vlastního hesla a jeho nastavení v souladu s definovanými pravidly (délka, složitost, pravidelná obměna).

Přístupová práva uživatele jsou dána jeho uživatelskou identifikací (přihlašovací jméno, heslo, případně další atributy sloužící k identifikaci uživatele). Uživatel se nesmí žádnými prostředky pokusit získat přístupová práva či privilegovaný stav, který mu nebyl přidělen administrátorem počítačových prostředků. Pokud uživatel získá privilegovaný stav nebo jemu nepříslušející přístupová práva jakýmkoli způsobem (včetně hardwarové nebo softwarové chyby systému), je povinen tuto skutečnost neprodleně ohlásit administrátorovi. Toto se vztahuje na všechny počítače a počítačové sítě, ke kterým uživatel získá přístup.

Uživatel se nesmí pokusit získat přístup k chráněným informacím a datům jiných uživatelů. Uživatel je dále povinen v rámci svých uživatelských práv maximálně zabezpečit svoje data proti zneužití třetími osobami.

2.4.3 Bezpečné použití elektronické pošty a přístupu na internet

Pro využívání služeb interní elektronické pošty mají oprávnění všichni uživatelé informačního systému. Uživatelé smějí využívat pouze jim přidělené schránky elektronické pošty, používání schránek jiných uživatelů je zakázáno.

Elektronická pošta je určena primárně k pracovním účelům; používat elektronické adresy organizace v Internetu pro mimopracovní aktivity je dovoleno jen výjimečně, se zachováním pravidel etického vystupování a s vyloučením případného konfliktu zájmů tak, aby tato komunikace nemohla být zneužita proti zájmům MZ ČR.

Uživatelé musí být poučeni o hrozbách zavlečení virů a jsou povinni počínat si opatrně při otevírání zpráv a jejich příloh, zejména těch, které pocházejí od neznámých odesílatelů. Pokud si uživatelé nejsou jisti, kontaktují zodpovědného správce.

Osobní užívání prostředků výpočetní techniky je dovoleno jen do té míry, pokud není v rozporu s vykonáváním zaměstnancovy práce, nespotřebovává důležité zdroje, nedává vzniknout vyšším nákladům, nebo není v rozporu s činností ostatních zaměstnanců. Za žádných okolností nesmějí být tyto prostředky užívány k osobnímu finančnímu zisku zaměstnanců nebo třetích osob, nebo ve spojení s politickými kampaněmi nebo lobbingem.

Kromě výše zmíněných omezení a podmínek je dále zakázáno používat komunikační prostředky k:

- přenosu hanlivých, diskriminačních nebo obscénních materiálů;
- ve spojení s porušením osobních práv jiných osob (např. autorská práva);
- porušení příslušných telekomunikačních licencí nebo jiných zákonů týkajících se přenosu dat;
- ve spojení s pokusem o vniknutí do počítače, sítě zaměstnavatele nebo jiného systému nebo k získání neoprávněného přístupu (příp. pokusu o přístup) do počítače, e-mail jiné osoby;
- ve spojení s porušením nebo pokusem o porušení zákona.

MZ ČR respektuje osobní soukromí pracovníků. S ohledem na to, že jsou informační aktiva určena k zajištění činnosti MZ ČR, vyhrazuje si MZ ČR právo nahodilé kontroly využívání prostředků výpočetní techniky pracovníkem v případě důvodného podezření porušení pravidel stanovených interními předpisy a touto politikou. Samotným užíváním těchto prostředků je pracovník v odůvodněných případech srozuměn s případnou kontrolou využívání prostředků výpočetní techniky ze strany MZ ČR.

2.4.4 Bezpečný vzdálený přístup

Umožnění vzdáleného přístupu k aktivům MZ ČR je výjimkou ze standardů bezpečnosti a jako takové vždy podléhá schválení garanta dotčených aktiv a musí být vždy odůvodněno konkrétní potřebou organizace. Uživatelé prostředků umožňujících vzdálený přístup musí dbát předepsaných opatření pro užití těchto prostředků a vzdáleného přístupu.

V případě ztráty či zcizení prostředků umožňujících vzdálený přístup informuje jejich uživatel bezprostředně určeného pracovníka, který zajistní zneplatnění přístupů těchto prostředků k aktivům informačního systému MZ ČR a v případě, že je to technicky možné, zajistí vzdálené smazání dat z daných prostředků.

Uživatelé prostředků umožňujících vzdálený přístup jsou povinni neprodleně provádět všechny doporučené aktualizace a úpravy prostředků umožňujících vzdálený přístup tak, aby byla minimalizována rizika jejich zneužití pro neoprávněný přístup k aktivům informačního systému MZ ČR.

2.4.5 Bezpečné chování na sociálních sítích

Uživatelé, kteří nemají v popisu práce využívání a správu oficiálních účtů MZ ČR na sociálních sítích, nejsou oprávnění využívat prostředky informačního systému MZ ČR k přístupu k sociálním sítím.

Uživatelé, do jejichž pracovní náplně spadá využívání a správa oficiálních účtů MZ ČR na sociálních sítích, dodržují pravidla bezpečné práce se sociálními sítěmi, zejména:

- Dbají na ochranu přihlašovacích údajů, dostatečnou komplexnost hesla, jeho důvěrnost a pravidelnou obměnu (nejméně jedou za tři měsíce),
- Využívají sociální sítě pouze pro oficiální potřeby MZ ČR a sdílejí pouze takové informace, které jsou v souladu s oficiální komunikační politikou a zájmy MZ ČR.

2.4.6 Bezpečnost ve vztahu k mobilním zařízením.

Cílem je zajistit bezpečnost informací při používání mobilních zařízení.

Každé mobilní zařízení je evidováno, má instalovánu proaktivní ochranu před hrozbami, pro případ ztráty nebo krádeže a omezení instalace SW.

V případě potřeby je zajištěno šifrování zařízení pro zajištění bezpečnosti dat.

2.5 Politika práce na dálku

Ministerstvo podporuje moderní technologie umožňující operativní a plnohodnotnou práci mimo pracoviště. Podmínkou je plně dodržet všechna bezpečnostní pravidla, aby nemohlo dojít o ohrožení informační bezpečnosti. Jsou nastavena jednoznačná pravidla práce na dálku a nastaven systém důsledné kontroly.

2.6 Politika ochrany osobních údajů

Základními organizačními předpisy, upravujícími problematiku osobních údajů, včetně charakteristiky zpracovávaných osobních údajů, popisu přijatých a provedených organizačních a technických opatření pro ochranu osobních údajů, jsou Příkaz ministra č. 14/2007, Ochrana osobních údajů zaměstnanců Ministerstva zdravotnictví, a Příkaz ministra č. 39/2018, Implementace Obecného nařízení o ochraně osobních údajů - GDPR.

Od 25. května 2018 je základním právním rámcem pro ochranu osobních údajů Obecné nařízení o ochraně osobních údajů (Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, General Data Protection Regulation - GDPR), které přímo stanovuje pravidla pro zpracování osobních údajů.

2.7 Politika ochrany před škodlivým kódem

2.7.1 Pravidla a postupy pro ochranu komunikace mezi vnitřní a vnější sítí

Ochrana vnitřního perimetru sítě je zajišťována pomocí firewallu, případně dalších technických prostředků (IDS/IPS, apod.). Tyto prostředky jsou centrálně spravovány, je prováděna jejich pravidelná aktualizace, sledování a řešení jejich zranitelností, a další úkony zajišťující jejich plnou funkčnost.

Vzdálené přístupy do vnitřní sítě jsou umožněny pouze autorizovaným uživatelům a technickým prostředkům pomocí šifrované komunikace v rámci virtuální privátní sítě.

2.7.2 Pravidla a postupy pro ochranu serverů, sdílených datových uložišť a pracovních stanic

Na všech pracovních stanicích, serverech a datových úložištích je centrálně instalován a automaticky spouštěn antivirový software, je prováděna jeho pravidelná aktualizace a vyhodnocování jeho účinnosti.

Všechna externí paměťová média připojená k počítači nebo vkládaná do počítače (flash disk, CD/DVD, atp.) jsou automaticky podrobena antivirové kontrole.

V rámci antivirového programu je aktivována funkce ochrany před mallware/adware a jinými hrozbami spojenými s prohlížením webových stránek.

Uživatelé pracovních stanic nemají přístupová práva k administrátorskému účtu a nemohou spouštět neautorizované aplikace a programy.

2.8 Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí (SIEM)

Pro zvýšení kybernetické bezpečnosti je využíván nástroj pro centralizovanou detekci kybernetických bezpečnostních událostí – Security Information and Event Management (SIEM). Tento nástroj konsoliduje data protokolu zdrojových událostí z koncových zařízení a aplikací distribuovaných po celé síti, zajišťuje okamžitou normalizaci a korelaci aktivit na základě prvotních dat s cílem rozlišit mezi reálnými hrozbami a hrozbami, které byly chybně identifikovány. SIEM rovněž koreluje slabá místa zabezpečení systému s daty událostí a síťovými daty, čímž pomáhá při stanovení priorit bezpečnostních incidentů.

Pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí, pro optimalizaci jeho nastavení a pro vyhodnocování a reagování na detekované kybernetické bezpečnostní události budou stanovena v Metodice nasazení a používání SIEM.

2.9 Politika bezpečného používání kryptografické ochrany

2.9.1 Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu

Pro jednotlivá informační aktiva je stanovena požadovaná úroveň ochrany s ohledem na míru citlivosti spravovaných informací. Nasazení kryptografické ochrany a použití kryptografických prostředků se provádí v souladu s bezpečnostními standardy stanovenými pro jednotlivé úrovně citlivosti informací spravovaných daným informačním aktivem.

2.9.2 Pravidla kryptografické ochrany informací

Rozhodnutí o užití kryptografické ochrany navrhuje garant příslušného aktiva a schvaluje Architekt kybernetické bezpečnosti.

V případě užití kryptografických prostředků na uživatelských zařízeních je nastaven systém pro obnovu dat v případě ztráty či zneplatnění klíčů či technických prostředků kryptografické ochrany.

K šifrování elektronické komunikace jsou využívány kvalifikované certifikáty vydané akreditovaným poskytovatelem certifikačních služeb.

Pro ochranu aktiv informačního a komunikačního systému se používají:

a) aktuálně odolné kryptografické algoritmy a kryptografické klíče,
b) systém správy klíčů a certifikátů, který
    - zajistí generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů a likvidaci klíčů, a
    - umožní kontrolu a audit.
c) Prosazuje se bezpečné nakládání s kryptografickými prostředky.
d) Zohledňují se doporučení v oblasti kryptografických prostředků vydaná NÚKIB.

3 Politika poskytování a nabývání licencí

3.1 Pravidla a postupy nasazení programového vybavení a jeho evidence

3.1.1 Nasazování programového vybavení

V rámci pořízení počítačových programů se musí důsledně dbát, aby byl počítačový program pořizovaný v souladu s autorským zákonem. K zajištění oprávněnosti používat nakupovaný počítačový program je pověřený útvar povinen:

a) počítačový program, pokud nebyl vytvořen v rámci povinného subjektu, pořizovat akvizicí pouze u výrobců, jejich autorizovaných dealerů či distributorů počítačových programů, kteří mají právo daný počítačový program distribuovat konečným uživatelům, a za tímto účelem požadovat od dodavatelů počítačových programů příslušná ujištění v rámci smluv na dodávky počítačových programů,
b) v případě, že je počítačový program již nainstalován na nakupovaném hardwaru, požadovat od dodavatelů hardwaru písemná ujištění o tom, že jsou oprávněni počítačové programy instalovat, že instalací počítačového programu nebyla porušena práva k softwaru.
c) programové balíky pořizovat pouze v originálních baleních a na originálních záznamových mediích, s výjimkou počítačových programů instalovaných pomocí dálkového přístupu,
d) k počítačovým programům požadovat originální instalační média a uživatelskou dokumentaci, s výjimkou počítačových programů instalovaných pomocí dálkového přístupu,
e) zajistit řádné převzetí a uložení originální smluvní, licenční a jiné dokumentace v rozsahu umožňujícím prokázat oprávněnost používaní počítačového programu (např. standardních licenčních podmínek, standardních podmínek pro údržbu a podporu, dodací listy, faktury),
f) za dodržení zákona č. 148/1998 Sb. a zákona č. 101/2000 Sb. zajistit řádné registrování užívání počítačových programů v registračních centrech či obdobných evidencích výrobců počítačových programů v případě, že je registrace licenční smlouvou požadována. Registraci lze provést i elektronicky.

3.1.2 Evidence licencí

3.1.2.1 Dokumentace

V případě, že nejde o volně šiřitelné počítačové programy, je základním dokladem o jeho oprávněném použití zaplacená faktura. Oprávněnost používání počítačových programů lze dále prokázat zejména některými z následujících dokumentů:

a) smlouvami na dodávky počítačového programu (pokud byly takovéto smlouvy uzavřeny),
b) nabývacími doklady,
c) licenčními smlouvami upravujícími užívání počítačového programu případně originálními standardizovanými licenčními podmínkami,
d) doklady týkajícími se registrace užívání v registračním centru nebo obdobné evidenci výrobce či distributora počítačových programů (např. kopie registračních karet),
e) elektronickými kopiemi odeslaných a přijatých zpráv v případě pořízení počítačových programů dálkovým přístupem.

Tyto dokumenty musí být evidovány o veškerých užívaných počítačových programech na jediném místě. Odpovědnost za řádné vedení a evidenci nabývací dokumentace nesou příslušné útvary organizace. Zároveň jsou tyto útvary povinny zajistit u počítačových programů nově pořizovaných po nabytí účinnosti těchto pravidel uložení a evidenci originálních instalačních médií po celou dobu užívání počítačového programu.

3.1.2.2 Vedení evidence o instalaci počítačových programů

Kromě dokumentace, týkající se samotného nabytí počítačových programů, musí být zajištěna centrální vedení evidence o instalaci počítačového programu. Účelem takovéto evidence je doložení způsobu, jakým došlo k instalaci počítačového programu, zejména ve vztahu k počtu počítačů, na kterých byl počítačový program nainstalován. Rovněž musí být zpracován k veškerým nakoupeným počítačovým programům instalační protokol, který:

a) identifikuje jednoznačně instalovaný počítačový program, včetně jeho verze a modifikace a data instalace,
b) identifikuje fyzickou osobu, která počítačový program instalovala,
c) identifikuje jednoznačně počítače, případně včetně výměnných disků, na kterých byl počítačový program nainstalován.

Vedení evidence může být v elektronické podobě, v případě že bude zaručena autorizace záznamu.

3.1.2.3 Vedení evidence o počítačových programech instalovaných na jednotlivých počítačích

Ke každému počítači užívaném v rámci organizace musí být zajištěno vytvoření dokladu v písemné nebo elektronické formě (tzv. specifikační list), ve kterém jsou uvedeny všechny počítačové programy, oprávněně nainstalované a užívané na tomto počítači. Tento doklad musí být při každé změně nebo doplnění podepsán pověřeným zástupcem povinného subjektu, dále fyzickou osobou, která provedla instalaci (pokud instalaci neprovedl pověřený zástupce povinného subjektu) a oprávněným uživatelem (uživateli) příslušné stanice. Jsou-li užity typové konfigurace počítačového programu na více stanicích, lze vést specifikační list pro všechny tyto stanice společně jako jediný doklad. Vedení evidence může být v elektronické podobě, v případě že bude zaručena autorizace záznamu. Tento doklad musí být veden a musí být řádně doplňován ve všech případech změn konfigurace počítačových programů na počítači, tedy zejména v případech:

a) odinstalování určitého počítačového programu,
b) instalace nového počítačového programu,

c) aktualizace stávajícího počítačového programu.

3.1.2.4 Vedení evidence o vyřazení počítačových programů

V případě, že daný počítačový program nemá nebo nemůže být dále používán vzhledem k morální opotřebovanosti, rozhodnutí o migraci funkcí, či přechodu na jiné softwarové prostředí nebo z jiného důvodu, provede se jeho vyřazení. O vyřazení počítačového programu se provede zápis (protokol o vyřazení). Vyřazení probíhá v souladu s předpisy platnými pro likvidaci majetku u povinného subjektu.

Při vyřazení je nutno postupovat v souladu s ustanoveními licenční smlouvy (např. oznámení dodavateli nebo na registrační místo).

3.1.3 Převod práv k užívání počítačových programů

Při převodu práv k užívání počítačových programů na jinou organizaci je třeba předat i dokumenty podle odst. 3.1.2 výše.

Při převodu práv je nutno postupovat v souladu s ustanoveními licenční smlouvy (např. oznámení dodavateli nebo na registrační místo).

3.2 Pravidla a postupy pro kontrolu dodržování licenčních podmínek

Organizace musí zajistit minimálně jednou ročně provádění pravidelných kontrol dodržování licenčních smluv platných pro nainstalované počítačové programy na všech počítačích a pracovních stanicích využívaných v rámci organizace. O kontrolách a jejich výsledcích musí být vedeny záznamy, uchovávané u povinných subjektů po dobu nejméně tří let.

Pro provádění těchto kontrol budou využity automatické softwarové prostředky zabezpečené tak, aby výsledek automatizované kontroly nemohl uživatel počítače či stanice měnit.

4 Závěrečná ustanovení

Tato politika nabývá účinnosti dnem 27. března 2019, kdy byla schválena Výborem pro řízení kybernetické bezpečnosti.

MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Příloha č. 5 [redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		

MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Příloha č. 6 – Obchodní tajemství

[redacted]

MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Příloha č. 7 – Seznam poddodavatelů

Dodavatel neplní prostřednictvím poddodavatelů.

Příloha č. 8 – Pravidla pro zpracování osobních údajů

Smluvní strany zpracovávají osobní údaje pro účely plnění Smlouvy a/nebo příslušné Objednávky v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále „**GDPR**“) a zákonem č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů (dále „**ZZOÚ**“).

Získá-li Dodavatel v rámci plnění Smlouvy a/nebo příslušné Objednávky přístup k osobním údajům nebo citlivým údajům (dále „**osobní údaje**“) Objednatele, zavazuje se dodržovat podmínky jejich ochrany stanovené ZZOÚ, GDPR, Smlouvou a/nebo příslušnou Objednávkou.

Dodavatel bere na vědomí, že Objednatel jako správce osobních údajů (dále „**Správce**“) zpracovávaných na základě Smlouvy a/nebo příslušné Objednávky je ve vztahu k těmto osobním údajům zároveň v postavení zpracovatele ve smyslu čl. 28 GDPR (dále „**Zpracovatel**“).

Osobní údaje budou na základě Smlouvy zpracovávány automatizovaně a manuálně.

1) Obecné zásady zpracování osobních údajů subjektů údajů

   a. Objednatel jako Zpracovatel pověřuje Dodavatele jako dalšího zpracovatele zpracováváním osobních údajů subjektů údajů, a to způsobem dle čl. 28 odst. 3 GDPR v rozsahu nezbytném pro plnění Smlouvy a/nebo příslušné Objednávky a výhradně za účelem vyplývajícím z účelu Smlouvy a/nebo příslušné Objednávky a z účelu plnění poskytovaného dle Smlouvy a/nebo příslušné Objednávky, vždy v souladu s ZZOÚ.

   b. Pověření ke zpracování osobních údajů se vztahuje i na poddodavatele s tím, že Dodavatel výslovně prohlašuje, že pokud do zpracování osobních údajů zapojí dalšího poddodavatele, bude tento poskytovat dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování osobních údajů splňovalo GDPR a zaváže jej smlouvou ke stejným povinnostem, které má ve vztahu k Objednateli, v důsledku toho se poddodavatelé Dodavatele stanou dalšími zpracovateli ve smyslu čl. 28 odst. 2 GDPR. Dodavatel je povinen informovat Objednatele o veškerých zamýšlených změnách týkajících se přijetí dalších osob nebo zpracovatelů nebo jejich nahrazení a poskytnout mu příležitost vyslovit vůči těmto změnám námitky. Za plnění povinností poddodavatele v oblasti ochrany osobních údajů odpovídá Objednateli Dodavatel.

   c. Povinnosti týkající se ochrany osobních údajů se Dodavatel zavazuje plnit po dobu účinnosti této Smlouvy a/nebo příslušné Objednávky, pokud z ustanovení této Smlouvy a/nebo příslušné Objednávky nevyplývá, že mají trvat i po zániku účinnosti Smlouvy a/nebo příslušné Objednávky.

   d. Dodavatel je povinen postupovat při zpracování osobních údajů s řádnou péčí.

   e. Dodavatel se zavazuje zpracovávat osobní údaje v souladu s povinnostmi uloženými GDPR a ZZOÚ, a to včetně závazků (zejména):

      i. zohledňovat povahu zpracování,

      ii. být nápomocen při vyřizování žádostí subjektu údajů,

      iii. být nápomocen v plnění povinností dle čl. 32 až 36 GDPR,

iv. poskytovat Správci a Objednateli veškeré informace potřebné k doložení skutečnosti, že byly splněny povinnosti dle čl. 28 GDPR,

v. umožnit audity, včetně inspekcí prováděných Správcem, Objednatelem či jimi pověřenými osobami a poskytnout součinnost u těchto auditů.

f. V případě ukončení této Smlouvy je Dodavatel povinen předat Objednateli protokolárně veškeré hmotné nosiče obsahující osobní údaje a smazat veškeré osobní údaje v elektronické podobě v jeho dispozici, neobdrží-li od Objednatele jiné pokyny.

g. Dodavatel je povinen dbát, aby žádný subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbát na ochranu subjektů údajů před neoprávněným zasahováním do soukromého a osobního života a zajistit veškerá práva subjektu údajů, která je z pozice zpracovatele povinen zajišťovat dle GDPR.

h. Dodavatel se zavazuje dodržovat všechny povinnosti, které mu vyplývají z GDPR, jakož i z interních předpisů Objednatele a rozhodnutí či doporučení nebo stanovisek vydaných pro tyto osoby příslušným orgánem státní správy, s nimiž byl seznámen, a to včetně rozhodnutí či stanovisek nebo doporučení vydaných v budoucnu. Za účelem plnění těchto povinností se Objednatel zavazuje bezodkladně po jejich obdržení poskytovat Dodavateli jakákoliv rozhodnutí či doporučení nebo stanoviska vydaná Správcem nebo příslušnými orgány státní správy.

i. Pokud Dodavatel zjistí, že Objednatel nebo Správce porušuje povinnosti stanovené GDPR, je povinen na to Objednatele neprodleně upozornit.

j. V případě, kdy je ze strany Úřadu pro ochranu osobních údajů (dále jen „**ÚOOÚ**“) či jiného správního orgánu provedena kontrola zpracování osobních údajů ze strany Dodavatele či v případě zahájení správního řízení ze strany ÚOOÚ či jiného správního orgánu ve vztahu k zpracování osobních údajů Dodavatelem, je Dodavatel tuto skutečnost povinen okamžitě oznámit Objednateli a poskytnout mu veškeré informace o průběhu a výsledcích této kontroly, resp. průběhu a výsledcích takového řízení.

k. Dodavatel není oprávněn osobní údaje subjektů údajů jím zpracovávané či k nimž mu byl umožněn přístup žádným způsobem ukládat, kopírovat, tisknout, opisovat, činit z nich výpisky či opisy či je pozměňovat, pokud toto není nezbytné pro plnění jeho povinností dle této Smlouvy a/nebo příslušné Objednávky.

l. Dodavatel je povinen umožnit Objednateli na základě jeho vyžádání kontrolu dodržování povinností při zpracování osobních údajů, tj. zejména umožnit přístup do prostor, v nichž jsou osobní údaje uchovávány, předložit seznam osob s přístupem k osobním údajům a/nebo doložit, že veškeré osoby přistupující k osobním údajům splňují požadavky pověřené osoby.

2) Záruky o technickém a organizačním zabezpečení osobních údajů subjektů údajů

a. Dodavatel je povinen zabezpečit řádnou technickou a organizační ochranu zpracovávaných osobních údajů a výslovně prohlašuje, že zavede vhodná technická a organizační opatření tak, aby zpracování osobních údajů splňovalo požadavky GDPR.

b. Dodavatel je povinen při zpracování osobních údajů zajistit ochranu osobních údajů minimálně na takové úrovni, aby byly dodrženy veškeré záruky o technickém

a organizačním zabezpečení osobních údajů uvedené níže.

c. Dodavatel je povinen zajistit taková opatření, aby nemohlo dojít k neoprávněnému ani nahodilému přístupu k osobním údajům, k jejich úplné ani částečné změně, zničení či ztrátě, neoprávněným přenosům či sdružení s jinými osobními údaji, či k jinému neoprávněnému zpracování v rozporu s touto Smlouvou a/nebo příslušnou Objednávkou. Dodavatel zároveň užije taková opatření, která umožní určit a ověřit, komu byly osobní údaje předány.

d. Dodavatel je povinen za účelem ochrany osobních údajů zajistit zejména, že:

   i. přístup k osobním údajům bude umožněn výlučně pověřeným osobám, které budou v pracovněprávním, příkazním či jiném obdobném poměru k Dodavateli, budou předem prokazatelně seznámeny s povahou osobních údajů a rozsahem a účelem jejich zpracování a budou povinny zachovávat mlčenlivost o všech okolnostech, o nichž se dozví v souvislosti se zpřístupněním osobních údajů a jejich zpracováním (dále jen „pověřené osoby“). Splnění této povinností zajistí Dodavatel vhodným způsobem, zejména vydáním svých vnitřních předpisů, příp. prostřednictvím zvláštních smluvních ujednání.

   ii. Zaměstnanci Dodavatele a jiné osoby, které budou zpracovávat osobní údaje dle Smlouvy a/nebo příslušné Objednávky, budou zpracovávat osobní údaje pouze za podmínek a v rozsahu Objednatelem stanoveném a odpovídajícím této Smlouvě, příslušné Objednávce, GDPR a ZZOÚ, zejména zajistí zachování mlčenlivosti o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i pro dobu po skončení zaměstnání nebo příslušných prací pověřených osob. Splnění této povinností zajistí Dodavatel vhodným způsobem, zejména vydáním svých vnitřních předpisů, příp. prostřednictvím zvláštních smluvních ujednání.

   iii. Při zpracování osobních údajů budou osobní údaje uchovávány výlučně na zabezpečených serverech nebo na zabezpečených nosičích dat, jedná-li se o osobní údaje v elektronické podobě.

   iv. Při zpracování osobních údajů v jiné než elektronické podobě budou osobní údaje uchovány v místnostech s náležitou úrovní zabezpečení, do kterých budou mít přístup výlučně pověřené osoby.

   v. Přístup k osobním údajům bude pověřeným osobám umožněn výlučně pro účely zpracování osobních údajů v rozsahu a za účelem stanoveným touto Smlouvou a/nebo příslušnou Objednávkou.

e. Dodavatel je povinen na písemnou žádost Objednatele přijmout v přiměřené lhůtě stanovené Objednatelem další záruky za účelem technického a organizačního zabezpečení osobních údajů, zejména přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům.

f. Dodavatel je povinen zpracovat a dokumentovat přijatá a provedená technickoorganizační opatření k zajištění ochrany osobních údajů v souladu s GDPR, jinými právními předpisy a předpisy, přičemž zajišťuje, kontroluje a odpovídá zejména za:

   i. plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům;

ii. zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování;

iii. zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje; a

iv. opatření, která umožní určit a ověřit, komu byly osobní údaje předány.

g. V případě zjištění porušení záruk dle této Smlouvy a/nebo příslušné Objednávky je Dodavatel povinen zajistit stav odpovídající zárukám neprodleně poté, co zjistí, že záruky porušuje, nejpozději však do 3 pracovních dnů poté, co je k tomu Objednatelem vyzván.

h. V oblasti automatizovaného zpracování osobních údajů je Dodavatel v rámci opatření podle předchozích odstavců povinen také:

i. zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze pověřené osoby;

ii. zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby;

iii. pořizovat a uchovávat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a zabránit neoprávněnému přístupu k datovým nosičům.

i. Dodavatel je povinen přijmout všechna opatření k zabezpečení zpracování, a to včetně:

i. schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;

ii. schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;

iii. procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

3) Ohlašování porušení zabezpečení osobních údajů

a. Dodavatel je povinen neprodleně, nejpozději však do 24 hodin, informovat Objednatele o všech případech porušení zabezpečení osobních údajů, které musí být dle čl. 33 a 34 GDPR oznamovány ÚOOÚ nebo subjektu údajů.

b. Dodavatel je povinen poskytnout Správci a Objednateli na jejich žádost veškeré informace, které budou považovat za nutné k řádnému posouzení porušení zabezpečení osobních údajů, minimálně však informace uvedené v čl. 33 odst. 3 GDPR.

c. Dodavatel je povinen poskytnout Objednateli v případě potřeby neprodleně veškerou součinnost při poskytování dodatečných informací o porušení zabezpečení osobních údajů ÚOOÚ a subjektům údajů.

d. Dodavatel je povinen vypracovat plán postupu pro případ porušení zabezpečení osobních údajů. Tento plán bude Dodavatelem předložen na základě vyžádání Objednateli. Dodavatel se zavazuje informovat Objednatele o veškerých podstatných

změnách tohoto plánu.

e. Dodavatel je povinen vést podrobnou evidenci veškerých případů porušení zabezpečení osobních údajů bez ohledu na skutečnost, zda tyto představují riziko pro práva a svobody fyzických osob, s uvedením skutečností, které se týkají daného porušení, jeho účinků a přijatých nápravných opatření. Tato evidence musí obsahovat minimálně informace uvedené v čl. 33 odst. 3 GDPR a Dodavatel je povinen poskytnout ji Objednateli a Správci na jejich žádost.

4) Jestliže vznikne v souvislosti se zajištěním ochrany osobních údajů podle právních předpisů uvedených v tomto článku nebo dle stanoviska ÚOOÚ nebo Evropského sboru pro ochranu osobních údajů potřeba uzavřít dodatek k této Smlouvě nebo zvláštní smlouvu, zavazuje se Dodavatel poskytnout veškerou součinnost nezbytnou k formulaci obsahu takového dodatku, resp. smlouvy a k uzavření takového dodatku, resp. smlouvy.

Příloha č. 9 – Pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací podle § 8 odst. 1 písm. a) a d) VoKB

Tento **Dokument** stanovuje v souladu s ustanovením § 4 odst. 4 zák. č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění (dále jen „**ZoKB**“) a § 8 odst. 1 písm. a) a d) ve spojení s přílohou č. 7 vyhl. č. 82/2018 Sb. (dále jen „**VoKB**“) závazná bezpečnostní opatření zohledňující požadavky systému řízení bezpečnosti informací, která se vztahují na dodavatele, kteří pro Ministerstvo zdravotnictví (dále jen „**Objednatel**“) výhradně či jako součást předmětu plnění dodávají, vyvíjí, implementují a/nebo provádějí servis software či hardware (dále také jen „**SW**“ či „**HW**“), a/nebo kteří v souvislosti s plněním přistupují do informačního systému Objednatele, který byl určen informačním systémem základní služby (dále také „**VIS**“) v souladu se ZoKB a/nebo kteří v rámci poskytovaného plnění zpracovávají, a/nebo přenášejí a/nebo ukládají a/nebo uchovávají informace, data a/nebo provozní údaje Objednatele.

Účelem tohoto **Dokumentu** je dosažení stanovené úrovně bezpečnosti informací v souladu s požadavky ZoKB, VoKB a dokumentace systému řízení bezpečnosti informací Objednatele.

Dodavatelem se pro účely tohoto **Dokumentu** rozumí každá osoba, jež poskytuje Objednateli jakékoliv plnění na základě Smlouvy. Dodavatelem se rozumí také provozovatel informačního nebo komunikačního systému.

Smlouvou se pro účely tohoto **Dokumentu** rozumí smlouva uzavřená mezi Objednatelem a dodavatelem.

Aktivem se pro účely tohoto **Dokumentu** rozumí primární aktivum, nebo podpůrné aktivum ve smyslu § 2 písm. f), nebo g) VoKB.

Není-li dále uvedeno jinak, rozumí se pojmy užívanými v tomto **Dokumentu** pojmy ve smyslu ZoKB, VoKB, nebo dokumentace systému řízení bezpečnosti informací Objednatele.

Pro účely tohoto **Dokumentu** se práva a povinnosti dodavatele stanovená tímto **Dokumentem** považují za bezpečnostní opatření.

Objednatel je správcem informačního systému základní služby ve smyslu ZoKB a VoKB. Dodavatel je povinen poskytovat plnění dle Smlouvy v souladu se všemi právními předpisy upravujícími kybernetickou bezpečnost a v souladu se všemi vnitřními předpisy Objednatele upravujícími systém řízení bezpečnosti informací, resp. tak, aby se dodavatel vyvaroval jakékoliv činnosti, jež by mohla být označena za porušení uvedených právních předpisů a vnitřních předpisů Objednatele upravujících systém řízení bezpečnosti informací.

1. OBECNÉ POŽADAVKY BEZPEČNOSTI INFORMACÍ

Dodavatel je při poskytování plnění povinen plnit následující povinnosti:

1.1 Postupovat v souladu s platnými právními předpisy.

1.2 Dodavatel je povinen zachovat bezpečnost informací a dat obsažených ve **VIS**, nebo v jiných informačních systémech, které jsou plněním Smlouvy dotčeny, a to zejm. z pohledu důvěrnosti, dostupnosti a integrity. Dodavatel prohlašuje, že si je vědom všech povinností, které je povinen z hlediska zachování bezpečnosti informací dodržovat. Je-li nezbytné důvěrnost, dostupnost či integritu informací nebo dat omezit, ohrozit nebo přerušit, může tak dodavatel učinit pouze po předchozím souhlasu Objednatele a jen v rozsahu předem odsouhlaseném.

1.3 Dodavatel je povinen Objednatele písemně informovat o způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním Smlouvy, a to do 15 pracovních dnů od nabytí účinnosti Smlouvy.

1.4 Dodavatel jmenuje nejpozději do 3 pracovních dnů po nabytí účinnosti Smlouvy zodpovědnou kontaktní osobu pro potřeby zajištění plnění bezpečnostních opatření a související komunikace mezi smluvními stranami.

1.5 Zajistit, aby kontaktní osoba dodavatele nejpozději do 30 dnů od nabytí účinnosti Smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování plnění Smlouvy za stranu dodavatele a/nebo jeho poddodavatelé byli prokazatelně seznámeni s tímto **Dokumentem**.

1.6 Zavést opatření pro ochranu zálohy dat vztahujících se k plnění Smlouvy a pravidelně testovat funkčnost těchto záloh.

1.7 V případě potřeby Objednatele musí dodavatel garantovat schopnost zrekonstruovat funkcionalitu aktiva do stavu požadovaného dle Smlouvy.

1.8 Realizovat bezpečnostní opatření pro ochranu dat souvisejících s plněním předmětu Smlouvy.

1.9 Průběžně detekovat technické zranitelnosti předmětu Smlouvy a o zjištěných skutečnostech bez zbytečného odkladu informovat Objednatele. Detekované technické zranitelnosti musí být vyhodnoceny s ohledem na související riziko a musí podle povahy předmětu plnění dojít k nápravným opatřením ze strany Dodavatele. Nápravná opatření musí být schválena Objednatelem.

1.10 Poskytovat Objednateli bez zbytečného odkladu, požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje **SW** či po jeho předání.

1.11 Průběžně dodávat systémové a provozní bezpečnostní dokumentace**,** a to bezodkladně, nejpozději do 14 dnů od provedení poslední změny minimálně v následujícím rozsahu**:**

- provozní a bezpečnostní dokumentace,
- popis principů autentizace, autorizace a vytváření auditních stop,
- popis principů instalace a konfigurace;
- popis nezbytných bezpečnostních konfigurací,
- popis principů zálohování a archivace,
- plány kontinuity činností a havarijní plány.

1.12 Veškeré informace vyžadující vyšší míru ochrany, zejména přístupová oprávnění, hesla, identifikační a jiné kritické údaje, poskytnuté Objednatelem při poskytování plnění budou vhodným způsobem chráněny proti neautorizovanému přístupu; certifikáty a přístupová oprávnění nebudou uchovávány v nešifrovaném tvaru, pokud nebude mezi smluvními stranami pro konkrétní případ dohodnuto jinak.

1.13 V produkčním prostředí systému **VIS** bude obsažen jen kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování systému **VIS**.

1.14 Před spuštěním SW v produkčním prostředí daného **VIS** provede dodavatel kontrolu souladu daného **SW** s bezpečnostními opatřeními Objednatele a v

případě zjištění nesouladu zajistí bez zbytečného odkladu soulad dodávaného **SW** s bezpečnostními opatřeními, pokud byl s takovými opatřeními seznámen.

1.15 Dodavatel odpovídá za to, že **SW** implementované do **VIS** budou obsahovat nejnovější, stabilní, bezpečné a řádně odzkoušené bezpečnostní aktualizace.

2. PERSONÁLNÍ BEZPEČNOST

2.1 Pokud dodavatel využívá při poskytování plnění poddodavatele, zavazuje se zajistit dodržování veškerých bezpečnostních opatření stanovených Objednatelem ve smluvních vztazích se svými poddodavateli a tuto skutečnost doložit na vyžádání předložením příslušného smluvního vztahu uzavřeného s tímto poddodavatelem, případně předložením čestného prohlášení o řádném naplňování této povinnosti.

2.2 Dodavatel a jeho případní poddodavatelé jsou povinni realizovat tato opatření:

- mít stanoven plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí a který obsahuje formu, obsah a rozsah;
- realizovat poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice;
- zajistit realizaci teoretických i praktických školení uživatelů, administrátorů a osob zastávajících bezpečnostní role;
- v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a poddodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení;
- v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat pro osoby zastávající bezpečnostní role pravidelná odborná školení, zohledňující aktuální potřeby v oblasti kybernetické bezpečnosti;
- v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní;
- vést o provedených školení přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly;
- zajišťovat kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role;
- v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajistit předání odpovědností;
- hodnotit účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí;
- určit pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.

3. FYZICKÁ OCHRANA A BEZPEČNOST PROSTŘEDÍ

3.1 Dodavatel se zavazuje, že neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k **VIS**, který je předmětem plnění dle Smlouvy.

3.2 Dodavatel se zavazuje dodržovat režimová opatření (provozní řády) budov a prostor zejména, kde jsou umístěna aktiva **VIS.**

4. OPRÁVNĚNÍ UŽÍVAT DATA A AUTORSTVÍ PROGRAMOVÉHO KÓDU

4.1 Dodavatel je při poskytování plnění pro Objednatele oprávněn užívat data předaná Dodavateli Objednatelem za účelem plnění předmětu Smlouvy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy a zavazuje se nakládat s daty pouze v souladu se Smlouvou a příslušnými právními předpisy, zejména ZoKB a VoKB.

4.2 Dodavatel se při poskytování plnění pro Objednatele zavazuje zajistit, aby při plnění Smlouvy dodržel podmínky stanovené zák. č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

5. KONTROLA A AUDIT DODAVATELE (PRAVIDLA ZÁKAZNICKÉHO AUDITU)

5.1 Dodavatel se zavazuje poskytnout Objednateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti vyplývající z tohoto **Dokumentu**, ze ZoKB a VoKB a umožnit Objednateli provedení auditů prováděných Objednatelem či pověřeným auditorem.

5.2 Dodavatel je povinen Objednateli poskytnout nezbytnou součinnost a zpřístupnit veškerou potřebnou dokumentaci technických a organizačních opatření.

5.3 Kontrola nebo audit mohou být provedeny u Dodavatele nebo jeho poddodavatele.

5.4 Objednatel má povinnost písmeně oznámit Dodavateli provedení kontroly či auditu, a to nejméně 14 dnů před provedením kontroly či auditu.

5.5 Dodavatel je povinen pravidelně provádět kontrolu zavedených bezpečnostních opatření a hodnocení rizik.

5.6 V případě neuspokojivých výsledků hodnocení dodavatele, nebo výsledků provedeného zákaznického auditu, musí dodavatel podniknout nezbytná opatření, která povedou k nápravě.

6. ŘETĚZENÍ DODAVATELŮ

6.1 Dodavatel není oprávněn zapojit do plnění Smlouvy žádného dalšího poddodavatele bez předchozího povolení Objednatele.

6.2 Dodavatel se zavazuje, že se bude řídit požadavky Objednatele na řízení bezpečnosti informací a pokud využívá při poskytování plnění poddodavatele, zajistí, že bude Objednateli poskytnuta veškerá nezbytná součinnost v otázkách řízení bezpečnosti informací také od těchto poddodavatelů.

6.3 Pokud Dodavatel využívá za účelem plnění předmětu Smlouvy poddodavatele, musí být tomuto poddodavateli uloženy na základě Smlouvy s Dodavatelem stejné povinnosti k dodržování smluvních ujednání, jaká jsou sjednaná tímto **Dokumentem** mezi Objednatelem a Dodavatelem.

6.4 Dodavatel se zavazuje předložit Objednateli, na základě jeho písemného vyzvání, příslušnou smlouvu s poddodavatelem.

6.5 Dodavatel má povinnost zajistit, že poddodavatel bude v souladu s požadavky, které Objednatel ukládá na základě tohoto **Dokumentu** Dodavateli.

7. ŘÍZENÍ PŘÍSTUPU

7.1 Přístup k **VIS** je možné povolit pouze po evidenci osoby zastupující dodavatele v registru identit Objednatele nebo obdobném systému, a to na základě požadavku dodavatele na přístup.

7.2 Přidělení oprávnění zaměstnancům dodavatele musí být řízeno principem nezbytného minima a není nárokové.

7.3 Dodavatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci dodavatele ani poddodavatele.

7.4 Nelze připojit koncové zařízení do sítě Objednatele bez předchozího schválení připojení určenou osobou.

7.5 Dodavatel se zavazuje, že všechny jeho informační systémy, které se připojují do síťové infrastruktury Objednatele, jsou a budou chráněny vhodným způsobem proti malware.

7.6 Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění, které přistupují do interní sítě a/nebo **VIS** Objednatele chránily autentizační prostředky a údaje k **VIS** Objednatele. Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako kybernetická bezpečnostní událost ve smyslu příslušné řídící dokumentace a mohou být uplatněny příslušné postupy zvládání kybernetické bezpečnostní události (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu). Dodavatel bere na vědomí, že postup zvládáním kybernetické bezpečnostní události či jiný důsledek porušení bezpečnostních opatření nebude posuzován jako okolnost vylučující odpovědnost dodavatele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy dodavateli či jiné osobě ze strany Objednatele.

8. ŘÍZENÍ ZMĚN A KONTINUITA ČINNOSTÍ

8.1 Objednatel u významných změn dokumentuje jejich řízení, provádí analýzu rizik, přijímá opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami, aktualizuje bezpečnostní politiku a bezpečnostní dokumentaci, zajistí testování **VIS** a zajistí možnost navrácení do původního stavu.

8.2 Objednatel má povinnost informovat dodavatele o výsledcích řízení změn, které mají dopady na plnění předmětu Smlouvy ze strany dodavatele.

8.3 Dodavatel má povinnost přijmout účinná opatření ke snížení nepříznivých dopadů v souladu s výsledky řízení změn.

8.4 Dodavatel se zavazuje poskytnout Objednateli veškerou nezbytnou součinnost při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu.

8.5 Objednatel má oprávnění zapojit dodavatele do řízení kontinuity činností, a to zejména oprávnění k zahrnutí dodavatele do plánu kontinuity činností, který souvisí s **VIS** nebo s jeho **HW** komponentami a souvisejících služeb a/nebo zahrnutí dodavatele do havarijního plánu Objednatele.

9. MONITOROVÁNÍ ČINNOSTÍ

9.1 Dodavatel bere na vědomí, že veškerá jeho aktivita a jeho plnění realizované v prostředí Objednatele budou průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na oprávněné zájmy Objednatele, jakož i s ohledem na obsah Smlouvy a interních dokumentů Objednatele, se kterými byl dodavatel seznámen.

10. ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH INCIDENTŮ

10.1 Dodavatel se zavazuje, že při poskytování plnění pro Objednatele stanoví činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání kybernetických bezpečnostních událostí a incidentů, podle takto stanovených a popsaných pravidel bude postupovat, a bude hlásit všechny kybernetické bezpečnostní události a incidenty včetně případů porušení zabezpečení osobních údajů neprodleně po jejich detekci Objednatelem.

10.2 Dodavatel navrhne řešení tak, aby bylo možné zvládat a detekovat kybernetické bezpečnostní události a incidenty a realizuje opatření pro zvýšení odolnosti informačního systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti a vychází při tom zejména z požadavků stanovených VoKB.

10.3 Dodavatel má povinnost neprodleně informovat Objednatele o kybernetických bezpečnostních incidentech souvisejících s plněním předmětu Smlouvy. Součástí oznámení musí být popis povahy případu kybernetického bezpečnostního incidentu.

10.4 Dodavatel má povinnost provést analýzu příčin kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

11. OCHRANA DŮVĚRNOSTI INFORMACÍ

11.1 Smluvní strany se zavazují zachovat mlčenlivost o veškerých informacích a osobních údajích, o nichž se dozvěděly v souvislosti s plněním Smlouvy, a to včetně předmětu Smlouvy, vlastní spolupráce a vnitřních záležitostí stran.

11.2 Smluvní strany se zavazují, že zajistí, aby všechny osoby oprávněné zpracovávat informace a osobní údaje, o nichž se dozvěděly v souvislosti s plněním Smlouvy se zavázaly k mlčenlivosti. Závazek mlčenlivosti a ochrany důvěrnosti informací zůstává v platnosti i po ukončení Smlouvy.

12. INFORMAČNÍ POVINNOST DODAVATELE

12.1 Dodavatel má povinnost neprodleně informovat Objednatele o kybernetických bezpečnostních incidentech souvisejících s plněním předmětu Smlouvy. Součástí oznámení musí být popis povahy případu kybernetického bezpečnostního incidentu.

12.2 Dodavatel má povinnost informovat Objednatele o způsobu řízení rizik a o rizicích souvisejících s plněním předmětu Smlouvy, a to na základě písemné výzvy Objednatele.

12.3 Dodavatel má povinnost bez zbytečného odkladu informovat Objednatele o významné změně ovládání Dodavatele dle zák. č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) nebo změně vlastnictví základních aktiv a změně v oprávnění Dodavatele nakládat s aktivy, které jsou využívány k plnění předmětu Smlouvy. V případě, že dojde k významné změně kontroly nad dodavatelem, přičemž kontrolou se zde rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentní postavení, je Objednatel oprávněn odstoupit od Smlouvy.

13. POVINNOSTI PŘI UKONČENÍ SMLOUVY

13.1 Dodavatel se zavazuje poskytnout Objednateli veškerou potřebnou součinnost, dokumentaci a informace při ukončení Smlouvy. Dodavatel se zavazuje účastnit se jednání s Objednatelem a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených s provozem, údržbou a rozvojem předmětu Smlouvy na Objednatele a/nebo nového dodavatele, ke kterému dojde po skončení účinnosti Smlouvy.

14. SPECIFIKACE PODMÍNEK PRO FORMÁT PŘEDÁNÍ DAT, PROVOZNÍCH ÚDAJŮ A INFORMACÍ PO VYŽÁDÁNÍ MZDRAV

14.1 Veškerá uživatelská a/nebo provozní data **VIS** musí být Objednateli předána bez zbytečného odkladu po doručení žádosti o export, a to v elektronické, strojově čitelné podobě, v otevřeném formátu, jehož využití není zatíženo právy třetích osob a Objednatel jej může užít bez jakéhokoliv omezení. Součástí předávaných exportovaných dat musí vždy být úplný popis formátu včetně datových typů a vzájemných vazeb v českém jazyce, ledaže by se jednalo o otevřený, standardizovaný formát. Pokud nestanoví Objednatel jinak, je

dodavatel povinen data exportovat v kódování českého jazyka UTF-8. Soulad exportovaných dat s těmito požadavky a jejich úplnost, podléhá akceptaci Objednatele.

15. PRAVIDLA PRO LIKVIDACI DAT

15.1 Dodavatel se zavazuje poskytnout Objednateli veškerou potřebnou součinnost pro likvidaci nepotřebných dat, za tím účelem smluvní strany dohodnou lhůty pro provádění likvidace dat, kde stanoví konkrétní rozsah a časové intervaly pro likvidaci dat. Smluvní strany sjednávají, že k likvidaci dat přistoupí po vzájemném odsouhlasení likvidace, podmínky likvidace musí být v souladu přílohou č. 4 VoKB.