**SMLOUVA O POSKYTOVÁNÍ SLUŽEB DOHLEDOVÉHO CENTRA KYBERNETICKÉ BEZPEČNOSTI**

(dále jen „***smlouva***“)

# Smluvní strany

* 1. **Nemocnice Třebíč, příspěvková organizace**

sídlo: Purkyňovo nám. 133/2, Jejkov, 674 01 Třebíč

IČO: 00839396

zapsána v obchodním rejstříku pod sp. zn. Pr 1441 vedenou u Krajského soudu v Brně

za kterou jedná: Ing. Eva Tomášová, ředitelka

bankovní spojení: Komerční banka, a.s.

číslo účtu: 19-7759270227/0100 (investiční účet)

 12338711/0100 (provozní účet)

(dále jen *„****objednatel****“* či *„****smluvní strana****“*)

**a**

* 1. **[Doplní účastník – Obchodní jméno/název/jméno a příjmení]**

sídlo: [Doplní účastník]

IČO: [Doplní účastník]

DIČ: [Doplní účastník]

zapsána v obchodním rejstříku pod sp. zn. [Doplní účastník] vedenou u [Doplní účastník] soudu v [Doplní účastník]

zastoupený/jednající: [Doplní účastník], [Doplní účastník]

bankovní spojení: [Doplní účastník]

číslo účtu: [Doplní účastník]

(dále jen *„****poskytovatel****“* či *„****smluvní strana****“*)

(společně dále též jako *„****smluvní strany***”)

# Základní ustanovení

1. Tato smlouva je uzavřena dle § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „***občanský zákoník***“); práva a povinnosti stran touto smlouvou neupravená se řídí příslušnými ustanoveními občanského zákoníku.
2. Smluvní strany uzavírají tuto smlouvu ve výběrovém řízení veřejné zakázky malého rozsahu s názvem **Poskytování služeb dohledového centra kybernetické bezpečnosti (SOC)**, systémové číslo P25V00000105 (dále jen „**výběrové řízení**“ a „**veřejná zakázka**“), v rámci kterého byla jako nejvýhodnější vyhodnocena nabídka poskytovatele (dále jen „**nabídka poskytovatele**“), za podmínek uvedených v zadávací dokumentaci veřejné zakázky (dále jen „**zadávací dokumentace**“) a nabídce poskytovatele, a to za účelem vymezení práv a povinností smluvních stran při realizaci veřejné zakázky.
3. Smluvní strany prohlašují, že veškeré podmínky uvedené v zadávací dokumentaci veřejné zakázky, jakož i v nabídce poskytovatele, jsou platné i pro plnění této smlouvy.
4. Jednotlivá ujednání této smlouvy budou vykládána v souladu se zadávacími podmínkami veřejné zakázky a nabídkou poskytovatele.
5. Smluvní strany prohlašují, že údaje uvedené v čl. 1 této smlouvy jsou v souladu se skutečností platnou v době uzavření smlouvy. Smluvní strany se zavazují, že změny těchto údajů oznámí bez prodlení písemně druhé smluvní straně.
6. Je‑li poskytovatel plátcem DPH, prohlašuje, že bankovní účet uvedený v čl. 1 této smlouvy je bankovním účtem zveřejněným ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „***zákon o DPH***“). V případě změny bankovního účtu poskytovatele je poskytovatel povinen doložit, že je majitelem takového nového účtu, a to kopií příslušné smlouvy nebo potvrzením peněžního ústavu; je‑li poskytovatel plátcem DPH, musí být nový účet zveřejněným účtem ve smyslu předchozí věty.
7. Poskytovatel potvrzuje, že jsou mu známy veškeré technické, kvalitativní a jiné podmínky nezbytné k plnění smlouvy a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné k plnění smlouvy.
8. Pro účely komunikace mezi smluvními stranami je poskytovatel povinen zajistit technickou funkčnost své e-mailové schránky.

# Účel smlouvy

* 1. Účelem této smlouvy je poskytovat komplexní služby dohledu plně funkčního dohledového centra kybernetické bezpečnosti Security Operation Center (dále jen „***SOC***“) pro vyhodnocování a zvládání kybernetických bezpečnostních událostí, incidentů a provozních událostí v celé ICT infrastruktuře, kterou objednatel využívá nebo provozuje.

# Předmět smlouvy

## Předmětem této smlouvy je závazek poskytovatele poskytovatel objednateli komplexní služby dohledu plně funkčního dohledového centra SOC v rozsahu níže specifikovaném v čl. 4.2. této smlouvy a závazek objednatele uhradit poskytovateli za poskytnuté plnění cenu dle čl. 6. této smlouvy.

* 1. Pro účely této smlouvy se poskytováním služeb rozumí poskytování služeb bezpečnostního a provozního dohledu nad ICT infrastrukturou objednatele v režimu 7 dní v týdnu 24 hodin denně. Bezpečnostní a provozní dohled bude centralizovat kontrolní činnosti, správu událostí a incidentů, koordinovat analýzy anomálií a aktivně spolupracovat při řízení krizových úkonů při zvládání následků incidentů s interním týmem kybernetické bezpečnosti objednatele (dále jen „***služby***“).
	2. Služby budou poskytovány v následujícím rozsahu:
1. Služba SOC-SLA-1 – Průběžný bezpečnostní dohled, jejímž cílem je úvodní vyhodnocení událostí z dohledovaných systémů a stanovení dalšího postupu k jejich řešení.
2. Služba SOC-SLA-2 – Analýza událostí, jejímž cílem je zajištění co nejrychlejšího vyhodnocení detekované kybernetické bezpečnostní události (dále jen „***KBU***“) či jiné anomálie v infrastruktuře objednatele a zajištění provedení podrobnější analýzy.
3. Služba SOC-SLA-3 – Threat Hunting, jejímž cílem je aktivní vyhledávání skrytých kybernetických hrozeb prostřednictvím kombinace digitální forenzní analýzy a různých taktik reakce na incidenty.
4. Služba CSIRT-SLA-1 – Řešení incidentů, jejímž cílem je zajistit co nejrychlejší obnovení dostupnosti dohledovaných služeb objednatele a současně minimalizovat důsledky takového výpadku.
5. Dodatečné analytické služby v režimu 8 x 5, tj. v pracovních dnech, od pondělí do pátku v čase od 8.00 do 16.00 hod. (dále jen „***dodatečné analytické služby***“).

Podrobné požadavky na obsah, rozsah a povahu služeb a způsob jejich poskytování stanoví příloha č. 1 této smlouvy.

* 1. Poskytovatel je povinen v rámci plnění předmětu této smlouvy provést veškeré činnosti, služby a výkony, kterých je potřeba k řádnému poskytování, dokončení a předání plnění.
	2. Dodatečné analytické služby jsou poskytovány výhradně na základě samostatného požadavku (objednávky) objednatele. Objednatel není povinen dodatečné analytické služby požadovat (objednat).
	3. Za účelem splnění předmětu smlouvy objednatel zpřístupní poskytovateli vlastní bezpečnostní dohledové systémy včetně jejich základní konfigurace, a to  v rozsahu potřebném pro řádné plnění této smlouvy.

# Doba a místo plnění

* 1. Poskytování služeb bude zahájeno dnem účinnosti této smlouvy.
	2. Smlouva je uzavřena na dobu určitou, a to na dobu 24 měsíců ode dne nabytí její účinnosti.
	3. Doba poskytování služeb se člení na fázi zkušební, která trvá nejméně 3 měsíce ode dne nabytí účinnosti smlouvy, a fázi provozní, která trvá 21 měsíců od provedení zkušební fáze. Zkušební fáze bezprostředně předchází fázi provozní. Podrobnosti jednotlivých fází stanoví příloha č. 1 této smlouvy.

## Místem plnění je Nemocnice Třebíč s pracovišti v následujících 3 lokalitách:

## areál Nemocnice Třebíč, Purkyňovo nám. 133/2, Třebíč;

## areál LDN, nám. Svobody 358, 676 02 Moravské Budějovice;

## detašované pracoviště Ambulance Ortopedie, Vltavínská 1289/10, 674 01 Třebíč.

## Vzhledem k povaze poskytovaných služeb provádí poskytovatel plnění vzdáleně, pokud z povahy věci nebo dohody smluvní stran v konkrétním případě neplyne, že je zapotřebí plnění zajistit v místě plnění dle předchozího odstavce.

# Cena

* 1. Cena za služby dle čl. 4. odst. 4.3. písm. a. – d. této smlouvy činí [Doplní účastník] Kč bez DPH, slovy: [Doplní účastník] korun českých bez daně z přidané hodnoty.
	2. Cena za dodatečné analytické služby dle čl. 4. odst. 4.3. písm. e. této smlouvy činí [Doplní účastník] Kč bez DPH za hodinu poskytovaných služeb.
	3. Cena je konečná, nejvýše přípustná a zahrnuje veškeré náklady poskytovatele spojené se splněním jeho závazku z této smlouvy.
	4. Je-li poskytovatel plátcem DPH, odpovídá za to, že sazba daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy; v případě, že dojde ke změně zákonné sazby DPH, je poskytovatel k ceně bez DPH povinen účtovat DPH v platné výši. V případě, že poskytovatel stanoví sazbu DPH či DPH v rozporu s platnými právními předpisy, je povinen uhradit objednateli veškerou škodu, která mu v souvislosti s tím vznikla.

# Platební podmínky

* 1. Poskytovatel není oprávněn požadovat po objednateli poskytnutí zálohy.
	2. Cenu za služby poskytnuté ve zkušební fázi objednatel uhradí na základě faktury vystavené po provedení zkušební fáze. Cena za služby ve zkušební fázi je rovna podílu 3/24 z ceny za služby dle čl. 6. odst. 6.1. této smlouvy. Dojde-li k prodloužení trvání zkušební fáze, nemá poskytovatel nárok na zvýšení ceny za služby poskytnuté ve zkušební fázi.
	3. Cenu za služby v provozní fázi se objednatel zavazuje hradit na základě poskytovatelem měsíčně vystavených faktur, a to vždy ve výši 1/24 z ceny za služby dle čl. 6. odst. 6.1. této smlouvy. Budou-li v měsíci, za který se fakturuje, poskytovány i dodatečné analytické služby, bude k takto vystavené faktuře vždy připočtena částka odpovídající součinu ceny za dodatečné analytické služby dle čl. 6. odst. 6.2. této smlouvy a skutečně odpracovaného počtu hodin v takovém měsíci.

## Cena za služby bude hrazena vždy měsíčně zpětně. K celkové fakturované částce dle předchozího odstavce bude poskytovatelem připočtena DPH v zákonné výši. Cena za služby včetně zákonné výše DPH bude hrazena na základě daňových dokladů vystavených poskytovatelem (dále jen „*faktura*“).

## Spolu s fakturou budou objednateli doručeny doklady deklarující rozsah skutečně uskutečněného plnění v příslušném fakturačním období.

## Jednotlivé faktury je poskytovatel oprávněn vystavit nejdříve následující den po dni uskutečnění zdanitelného plnění, kterým je vždy poslední den v měsíci, ve kterém byly služby dle této smlouvy poskytovány.

## Lhůta splatnosti faktury činí 30 kalendářních dnů ode dne jejího doručení objednateli.

* 1. Nebude-li faktura obsahovat některou povinnou nebo dohodnutou náležitost nebo bude-li chybně vyúčtována cena nebo DPH, je objednatel oprávněn fakturu před uplynutím lhůty splatnosti vrátit druhé smluvní straně k provedení opravy s vyznačením důvodu vrácení. Odesláním vadné faktury poskytovateli přestává běžet původní lhůta splatnosti. Nová lhůta splatnosti běží ode dne doručení opravené faktury objednateli.
	2. Objednatel si vyhrazuje právo uplatnit institut zvláštního způsobu zajištění daně z přidané hodnoty ve smyslu § 109a zákona o DPH, pokud poskytovatel bude požadovat úhradu za zdanitelné plnění na bankovní účet, který nebude nejpozději ke dni splatnosti příslušné faktury zveřejněn správcem daně v příslušném registru plátců daně (tj. způsobem umožňujícím dálkový přístup). Obdobný postup je objednatel oprávněn uplatnit i v případě, že v okamžiku uskutečnění zdanitelného plnění bude o poskytovateli zveřejněna v příslušném registru plátců daně skutečnost, že je nespolehlivým plátcem nebo v případě naplnění dalších kritérií uvedených v § 109 odst. 1 a 2 zákona o DPH. V případě, že nastanou okolnosti umožňující objednateli uplatnit zvláštní způsob zajištění daně podle § 109a zákona o DPH, bude objednatel o této skutečnosti poskytovatele informovat. Při použití zvláštního způsobu zajištění daně bude příslušná výše DPH zaplacena na účet poskytovatele vedený u jeho místně příslušného správce daně, a to v původní lhůtě splatnosti. V případě, že objednatel institut zvláštního způsobu zajištění daně z přidané hodnoty ve shodě s tímto ujednáním uplatní a zaplatí částku odpovídající výši daně z přidané hodnoty uvedené na daňovém dokladu vystaveném poskytovatelem na účet poskytovatele vedený u jeho místně příslušného správce daně, bude tato úhrada považována za splnění části závazku objednatele odpovídajícího příslušné výši DPH sjednané jako součást sjednané ceny za zdanitelné plnění.

# Práva a povinnosti smluvních stran

* 1. Při zajišťování služeb se poskytovatel zavazuje počínat si s odbornou péčí tak, aby byl zcela naplněn předmět a účel smlouvy.
	2. Poskytovatel je povinen vynaložit maximální úsilí, aby docílil nejlepšího možného výsledku při plnění předmětu této smlouvy při využití svých znalostí a zkušeností.
	3. Při poskytování služeb postupuje poskytovatel samostatně, je však vázán zejména písemnými pokyny objednatele. Poskytovatel je povinen oznámit objednateli všechny okolnosti, které zjistil při plnění předmětu této smlouvy, které mohou mít vliv na změnu pokynů objednatele. Zjistí-Ii poskytovatel, že pokyny objednatele jsou nevhodné či neúčelné pro plnění předmětu této smlouvy, je povinen na to objednatele neprodleně písemně upozornit. Pokud nevhodné či neúčelné pokyny brání v řádném provádění plnění, je poskytovatel povinen v nezbytně nutném rozsahu přerušit provádění plnění do doby změny pokynů objednatele nebo písemného sdělení, že objednatel trvá na provádění plnění dle svých pokynů.
	4. Poskytovatel je povinen zajistit dostupnost služeb v českém jazyce a komunikaci v českém jazyce.
	5. Poskytovatel je povinen v průběhu poskytování služeb dodržovat obecně závazné předpisy a normy, postupovat s náležitou odbornou péčí, podle nejlepších znalostí a schopností, sledovat a chránit oprávněné zájmy objednatele.
	6. Poskytovatel je povinen v průběhu poskytování služeb neprodleně informovat objednatele o všech skutečnostech, které mají nebo mohou mít vliv na provedení plnění.
	7. Pokud objednatel zjistí, že poskytovatel poskytuje nebo poskytl služby v rozporu se svými povinnostmi vyplývajícími z této smlouvy, je oprávněn požadovat, aby poskytovatel zjištěné vady odstranil v objednatelem stanovené lhůtě.
	8. Poskytovatel je povinen zajistit v rámci plnění smlouvy legální zaměstnávání osob a zajišťovat všem osobám jím zaměstnaným v souladu s právními předpisy, které se budou podílet na plnění této smlouvy, férové a důstojné pracovní podmínky při dodržování odpovídající úrovně bezpečnosti práce, rozvržení pracovní doby a odpočinku, zejména jim zajišťovat dostatek ochranných pracovních pomůcek nezbytných k řádnému výkonu činnosti. Férovými a důstojnými pracovními podmínkami se rozumí takové pracovní podmínky, které splňují alespoň minimální standardy stanovené pracovněprávními a mzdovými předpisy. Poskytovatel je povinen zajistit splnění požadavků tohoto ustanovení smlouvy i u svých poddodavatelů.
	9. Poskytovatel se zavazuje, že při plnění předmětu této smlouvy bude v míře, kterou připouští řádné poskytování služeb, využívat pro komunikaci a korespondenci prostředky elektronické komunikace, bude minimalizovat spotřebu kancelářského materiálu, používat výrobky z recyklovaného materiálu nebo materiálu z obnovitelných zdrojů, nebo výrobky opakovaně použitelné.
	10. Poskytovatel je povinen při provádění plnění jednat s náležitou odbornou péčí, čestně a svědomitě, přičemž je vázán pouze právními předpisy a dalšími obecně závaznými právními předpisy a v jejich mezích je povinen se řídit pokyny objednatele.
	11. Poskytovatel se zavazuje, že plnění či jeho příslušenství, část ani výsledky (výstupy) ani dílčí výsledky (výstupy) své činnosti podle této smlouvy neposkytne bez písemného souhlasu objednatele dalším subjektům.
	12. Poskytovatel je povinen chránit zájmy objednatele, zejména je povinen upozornit objednatele na veškerá nebezpečí škod, která jsou mu známa a která souvisejí s prováděním plnění.
	13. Poskytovatel je povinen zachovávat mlčenlivost o všech skutečnostech, o kterých se při plnění této smlouvy dozvěděl a které současně objednatel při předání označil za důvěrné. Mlčenlivosti může poskytovatele zprostit jen objednatel svým písemným prohlášením či zmocněním a dále v případech stanovených právními předpisy. Povinnost mlčenlivosti trvá i po skončení platnosti této smlouvy a vztahuje se i na zástupce a pracovníky poskytovatele či jeho poddodavatele. Poskytovatel je oprávněn použít informace, data a podklady předané mu objednatelem za účelem plnění této smlouvy pouze a právě pro plnění předmětu této smlouvy, nikoliv pro jiný (objednatelem či osobou oprávněnou jednat ve věcech smluvních nebo technických, příp. kontaktní osobou) písemně neodsouhlasený, účel.
	14. Po ukončení plnění této smlouvy je poskytovatel bez zbytečného odkladu povinen předat objednateli veškeré podklady, které mu objednatel předal nebo které pro objednatele získal od třetích osob.
	15. Poskytovatel je povinen při poskytování služeb dodržovat bezpečnostní pravidla uvedená v příloze č. 2 této smlouvy.
	16. Poskytovatel je povinen poskytovat služby prostřednictvím kvalifikovaného realizačního týmu. Realizační tým poskytovatele je povinen provádět plnění způsobem a za podmínek dle této smlouvy, přičemž odpovědnost za takové provádění plnění nese poskytovatel. Realizační tým je vymezen v příloze č. 3 této smlouvy.

# Odpovědnost za škodu

## Smluvní strany nesou odpovědnost za způsobenou škodu v rámci platných právních předpisů a této smlouvy.

## Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

## Poskytovatel odpovídá i za škodu na díle způsobenou činností těch, kteří pro něj činnost provádějí.

# Pojištění

## Poskytovatel je povinen být po celou dobu plnění této smlouvy pojištěn v rámci pojištění odpovědnosti za škodu způsobenou třetí osobě při výkonu podnikatelské činnosti.

## Doklady o pojištění předloží poskytovatel objednateli kdykoliv v průběhu plnění smlouvy na základě žádosti objednatele.

# Sankční ujednání

## V případě, že poskytovatel nedodrží jakýkoliv stanovený požadavek nebo parametr služeb uvedený v příloze č. 1 této smlouvy, je objednatel oprávněn požadovat po poskytovateli zaplacení a poskytovatel je povinen objednateli zaplatit smluvní pokutu ve výši 10 000 Kč za každý zjištěný případ porušení.

## Za každý zjištěný případ porušení povinnosti zachovávat mlčenlivost dle čl. 8. odst. 8.13. této smlouvy je objednatel oprávněn požadovat po poskytovateli zaplacení smluvní pokuty ve výši 150 000 Kč a poskytovatel se zavazuje takto požadovanou smluvní pokutu objednateli zaplatit.

## V případě, kdy poskytovatel nebude pojištěn v souladu s čl. 10. této smlouvy, je objednatel oprávněn požadovat po poskytovateli uhrazení smluvní pokuty ve výši 10 000 Kč, a to za každý započatý měsíc, v němž poskytovatel nebude mít sjednáno pojištění, a poskytovatel se zavazuje takto požadovanou smluvní pokutu objednateli zaplatit.

## V případě realizace předmětu plnění této smlouvy realizačním týmem poskytovatele v jiném složení, než které je uvedeno v čl. 8. odst. 8.17. této smlouvy, je objednatel oprávněn požadovat po poskytovateli zaplacení smluvní pokuty ve výši 10 000 Kč za každé takové zjištění a poskytovatel se zavazuje takto požadovanou smluvní pokutu objednateli zaplatit.

## V případě porušení jakékoliv povinnosti stanovené v příloze č. 2 této smlouvy je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 100 000 Kč za každé jednotlivé porušení.

## Nesplní-li poskytovatel ve stanovené lhůtě svůj závazek odstranit vady plnění, je objednatel oprávněn požadovat na poskytovateli zaplacení smluvní pokuty ve výši 2 000 Kč za každý započatý den prodlení až do jejich úplného odstranění a poskytovatel se zavazuje takto požadovanou smluvní pokutu objednateli zaplatit.

## Za porušení kterékoli jiné povinnosti plynoucí poskytovateli z této smlouvy je objednatel oprávněn požadovat a poskytovatel povinen objednateli zaplatit smluvní pokutu ve výši 10 000 Kč za každý jednotlivý případ porušení smluvní povinnosti.

## Dojde-li k prodlení s úhradou daňového dokladu – faktury, je poskytovatel oprávněn požadovat po objednateli zaplacení úroku z prodlení ve výši 0,02 % z dlužné částky za každý započatý den prodlení po lhůtě splatnosti až do doby zaplacení dlužné částky.

## Nároky podle tohoto článku jsou splatné do 30 dnů ode dne doručení jejich vyúčtování druhé smluvní straně.

## Zaplacením jakékoliv smluvní pokuty dle tohoto článku smlouvy není dotčen nárok oprávněné strany na náhradu škody způsobené mu porušením povinnosti povinné strany, na niž se smluvní pokuta vztahuje. Ustanovení § 2050 občanského zákoníku se neuplatní.

# Ukončení smlouvy

## Tuto smlouvu lze ukončit dohodou smluvních stran. Dohoda o ukončení smluvního vztahu musí být písemná, jinak je neplatná.

## Od této smlouvy lze odstoupit v případě podstatného porušení povinností jednou smluvní stranou, jestliže je takové porušení povinnosti označeno za podstatné touto smlouvou nebo právním předpisem. Odstoupení od smlouvy je účinné dnem doručení písemného oznámení o odstoupení druhé smluvní straně.

## Smluvní strany se dohodly, že podstatným porušením této smlouvy ze strany poskytovatele je:

1. opakované porušení (tj. více než jedenkrát) jakéhokoliv termínu nebo lhůty plnění dle z této smlouvy,
2. neprovedení zkušební fáze ani ve lhůtě 5 měsíců ode dne nabytí účinnosti smlouvy.

## Smluvní strany se dohodly, že podstatným porušením této smlouvy ze strany objednatele je prodlení se zaplacením řádně vyfakturované ceny delší než 30 kalendářních dnů.

## Odstoupením od této smlouvy nejsou dotčena ustanovení týkající se smluvních pokut a úroků z prodlení a stejně tak práva a povinnosti smluvních stran vzniklá do okamžiku účinnosti odstoupení od smlouvy.

## Tuto smlouvu nelze vypovědět.

# Závěrečná ustanovení

## Smluvní strany berou na vědomí, že osobní údaje získané v souvislosti s uzavřením této smlouvy budou zpracovány v souladu s Nařízením Evropského parlamentu a rady (EU) 2016/679 ze dne 27. 4. 2016 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 také jen „GDPR“) a souvisejícími právními předpisy, výhradně za účelem realizace závazků z této smlouvy.

## Smlouva nabývá platnosti dnem jejího uzavření a účinnosti dnem jejího uveřejnění v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů. Uveřejnění této smlouvy v registru smluv zajistí Objednatel. Datum uzavření této smlouvy se určuje z data připojených elektronických podpisů, přičemž se musí jednat o kvalifikované či zaručené elektronické podpisy osob oprávněných za ně jednat, založené na kvalifikovaném certifikátu pro elektronický podpis dle zák. č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.

## Pokud jakýkoli závazek dle smlouvy nebo kterékoli ustanovení smlouvy je nebo se stane neplatným či nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních závazků a ustanovení dle smlouvy a smluvní strany se zavazují takovýto neplatný nebo nevymahatelný závazek či ustanovení nahradit novým, platným a vymahatelným závazkem, nebo ustanovením, jehož předmět bude nejlépe odpovídat předmětu a ekonomickému účelu původního závazku či ustanovení.

## Tato smlouva je uzavřena elektronicky a vyhotovena v elektronickém originále, který obdrží každá smluvní strana po jeho podpisu.

## Tuto smlouvu je možno platně měnit pouze na základě dohody smluvních stran, formou písemných a vzestupně číslovaných dodatků, podepsaných oběma smluvními stranami.

## Nedílnou součástí této smlouvy jsou její přílohy:

* příloha č. 1 – Specifikace plnění,
* příloha č. 2 – Bezpečnostní pravidla,
* příloha č. 3 – Realizační tým,
* příloha č. 4 – Seznam poddodavatelů, které poskytovatel hodlá použít při plnění
 smlouvy.

## Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly, zcela rozumí jejímu obsahu a s celým jejím obsahem souhlasí. Dále prohlašují, že tato smlouva vyjadřuje jejich pravou a svobodnou vůli. Na důkaz toho připojují vlastnoruční podpisy osob oprávněných za ně jednat.

|  |  |
| --- | --- |
| Za poskytovatele | Za objednatele  |
| V [Doplní účastník] | V Třebíči |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| [Doplní účastník]*podepsáno elektronicky* | **Ing. Eva Tomášová, ředitelka**Nemocnice Třebíč, příspěvková organizace*podepsáno elektronicky* |

**Příloha č. 1 smlouvy – Specifikace plnění**

# Specifikace poskytovaných služeb

* Poskytování komplexních služeb dohledu plně funkčního dohledového centra, které pracuje s bezpečnostními nástroji vlastními (SIEM) a bezpečnostními nástroji objednatele, jako je síťový dohled, dohled nad koncovými body sítě ve formě ochran před škodlivým kódem (ESET PROTECT Advanced On-Prem (ESET Dynamic Endpoint Protection)) a další SW či technologie u objednatele postupně implementované, které sledují všechny tyto nástroje a dávají podnět k analýze v případě, že dojde k jakékoliv nestandardní situaci.
* Bezpečnostní dohledové centrum podporuje práci s nástroji objednatele.
* Bezpečnostní dohledové centrum certifikované dle ČSN EN ISO 27001.
* Bezpečnostní dohledové centrum musí mít certifikaci Trusted introducer pro CSIRT týmy (<https://www.trusted-introducer.org> ) minimálně úroveň Accredited.
* Zajištění analytických činností pro včasné identifikace KBU díky vyhodnocování výstupů z připojených bezpečnostních detekčních nástrojů.
* Připojení a monitoring Nemocnice Třebíč (dále také jen „NTR“) v režimu 24x7.
* Analýza bezpečnostních a provozních anomálií ve veškerém sledovaném síťovém provozu NTR.
* Sledování a analýzy toků na perimetru infrastruktury NTR.
* Sledování a analýzy toků v rámci infrastruktury NTR.
* Odhalování zero-day zranitelností a vektorů útoků.
* V případě zjištění skutečnosti,:
	+ která může ohrozit zabezpečení hardwarové nebo softwarové infrastruktury objednatele,
	+ která může způsobit celkovou nedostupnost některého z vybraných systémů v infrastruktuře NTR
	+ či při které dochází k úniku citlivých dat

(dále jen „bezpečnostní incident“) SOC iniciuje odpovídající reakci, která zahrnuje i bezodkladnou notifikaci kompetentní osoby (osob) NTR, jejíž identifikační a kontaktní údaje objednatel sdělí poskytovateli v písemné formě. Reakce v režimu 24x7 pro informační systém základní služby a zahrnuté IS a v režimu 8x5 pro ostatní systémy. Reakcí se rozumí spuštění příslušného eskalačního schématu, jako je např. kontaktování pohotovostního telefonního čísla, případně e-mailu objednatele nebo dalších způsobů dohodnuté komunikace.

* Podrobná specifikace reakcí a řešení incidentů bude výstupem zkušební fáze provozu SOC.
* Základní návrh nastavení bezpečnostních a monitorovacích systémů NTR bude proveden v rámci zkušební fáze za součinnosti poskytovatele s objednatelem. V průběhu provozní fáze budou předkládány návrhy na změnu nastavení, které zohlední nové zkušenosti s provozem dohledového centra v rámci optimalizačních procesů PDCA cyklu.
* Detekce bezpečnostních incidentů a výpadků bezpečnostních technologií provozovaných v NTR.
* Vulnerability management – objednatel v současnosti neprovozuje vlastní systém pro vulnerability management, plánuje ale jeho pořízení. Poskytovatel bude zpracovávat a zohledňovat výsledky skenování zranitelností, až si objednatel pořídí tento systém. Pak mu poskytovatel bude předkládat návrhy na úpravy a změny testovacích pravidel. Dále také poskytovatel bude předkládat objednateli požadavky na mimořádné skenování zranitelností. Objednatel do doby pořízení vlastního systému pro vulnerability management může požádat poskytovatele o provedení mimořádného skenování zranitelností.
* V případě zjištění výpadku či omezení dostupnosti vybraných informačních systémů, iniciuje SOC spuštění příslušného eskalačního schématu.
* Poskytovatel ve spolupráci s objednatelem bude provádět kontrolu a nastavení korelačních pravidel, reportů a dalších parametrů. Na základě návrhu změn, provede poskytovatel konfiguraci a změny v systému SIEM, veškeré změny musí být schváleny objednatelem.
* Návrh řešení bezpečnostních incidentů formou jejich analýzy a navržení postupu k jejich odstranění, nebo navržení Workaround-u (opravy či náhradního postupu snižujícího závažnost nebo dopady incidentu), než bude možno provést finální úpravu odstraňující podstatu incidentu.
* Zasílání pravidelného měsíčního detailního výkazu o průběhu dostupnosti a plnění služeb objednateli, který zahrnuje:
	+ přehled plnění služby (včetně analýzy anomálních stavů, událostí a incidentů, výpadků, stavu a chování informačních systémů za uplynulé období),
	+ sledování KPI, které zahrnuje minimálně tyto: Mean time to detection, Mean time to response, množství false positive, true positive a jejich poměr, Mean time to resolution, Number of rule tunings applied, Number of rules effectively tuned, Number of false negatives, Mean time to pick-up, Mean time to escalate,
	+ návrhy systematických opatření pro zvýšení bezpečnosti, dostupnosti a prevenci bezpečnostních incidentů a výpadků systémů,
	+ přehled návrhů řešení lokalizovaných incidentů.
* Poskytování detailních informací k vykázaným službám objednateli, prostřednictvím osobních návštěv v sídle objednatele nebo formou videokonference.
* Zajištění proaktivní komunikace při řešení bezpečnostních incidentů, výpadků či omezené dostupnosti informačních systémů, včetně komunikace s třetí stranou (externí dodavatelé systémů, apod.), jako součást optimalizace bezpečnostních procesů mezi objednatelem a poskytovatelem.
* Analýza anomálních stavů či bezpečnostních hrozeb na základě podnětu či požadavku objednatele.
* Zajištění veškeré komunikace v rámci poskytování služeb v českém jazyce (zahrnuje i reporty, dokumentaci a případně další výstupy).
* Všechna data budou poskytovatelem přenášena do SOC v zabezpečené a zašifrované podobě. Data musí být chráněna proti neoprávněným změnám (zásahům) a proti neoprávněnému přístupu. Připojení bude realizováno prostřednictvím Site-to-Site VPN, kterou si zajistí poskytovatel na základě technických možností NTR. Objednatel po dohodě a předchozím odsouhlasení poskytovateli umožní instalaci a připojení zařízení (hw, sw) pro sběr a přenos informací potřebných pro provoz dohledového centra ze sítě NTR.
* Ticketovací systém poskytovatele se bude integrovat s HelpDesk systémem NTR (ALVAO), kde se budou primárně odbavovat všechny tickety a události.
* Reporty – Rozšířený reporting – detailní report o událostech a incidentech s návrhy systematických opatření 1x měsíčně. Vzdálená prezentace reportu, např. formou videokonference. Prezentace měsíčních reportů v rozsahu max. 0,5 MD.
* Reporty – On-demand – Služba zajistí provádění on-demand spouštění některých pravidel a z výstupu bude vytvářet reporty.
* Reporty – Standard – poskytovatel v rámci služby zpracuje a poskytne objednateli každý měsíc report, ve kterém je popsáno:
	+ průběh realizace plnění služby za uplynulé období,
	+ provedené služby za uplynulé období,
	+ návrh doporučených opatření pro další období pro zvýšení bezpečnosti, dostupnosti a v prevenci eliminace incidentů.
* Base line analýza – zajistí porovnání neobvyklých počtů určitých událostí oproti jinému období z minulosti. Služba zajistí shromažďování a možnost náhledu a následného porovnáni historických dat a jejich propojení v kontextu sledované události nebo incidentu.

## Specifikace služby SOC-SLA-1 – Průběžný bezpečnostní dohled

Cílem této služby je úvodní, průběžné, automatizované vyhodnocování bezpečnostních událostí a stanovení dalšího postupu k jejich řešení.

**Služba musí obsahovat:**

* **Průběžný bezpečnostní dohled/monitoring v rámci technologií napojených do SOC:**
	+ příjem strojově detekovaných událostí z dohledových systémů (zákazníka i SOC) identifikovaných na základě definovaných „Detekčních scénářů“,
	+ příjem událostí zpozorovaných analytiky SOC týmu v rámci služby SOC-SLA-3 (Threat Hunting),
	+ příjem událostí a požadavků od pověřených uživatelů zákazníka, případně smluvní, třetí strany.
* **Úvodní vyhodnocení zaznamenaných událostí a rozhodnutí o dalším postupu (Triage):**
	+ probíhá prvotní sběr informací a prověření, zda se nejedná o událost charakteru „False Positive“, a případná úprava detekčních scénářů, které vedly k jejich zaznamenání,
	+ v případě událostí vyžadujících další kontrolu (charakteru „Event of Interest“) dochází k jejich prvotní analýze a klasifikaci,
	+ v průběhu této fáze jsou informovány kontakty dle platné komunikační matice/schématu a definovaných „Scénářů reakce“ (notifikace), dochází také k vytvoření ticketu v HelpDesku a předání k dalšímu řešení.

|  |  |
| --- | --- |
| Rozsah zaručeného provozu služby | Maximální doba trvání úvodního vyhodnocení |
| 24 x 7 (nepřetržitě) | 30 minut od vzniku události |

## Specifikace služby SOC-SLA-2 – Analýza událostí

Služba začíná vstupem ze služby SOC-SLA-1 (vznik tiketu v systému poskytovatele). Cílem této služby je zajistit co nejrychlejší vyhodnocení detekované kybernetické bezpečnostní události (KBU) v infrastruktuře zákazníka a zajištění provedení podrobnější analýzy (Investigation).

Probíhá dodatečný sběr informací s využitím Operations nástrojů, vyhodnocení události a zpřesnění možných dopadů.

**Služba musí obsahovat:**

* dodatečný sběr informací a artefaktů s využitím Operations nástrojů,
* vyhodnocení události,
* určení dopadu a zpřesnění klasifikace události,
* notifikaci kontaktů dle platné komunikační matice a definovaných „Scénářů reakce“,
* update informací v již otevřeném tiketu v HelpDesku.

V případě, že dojde k vyhodnocení události, která naplňuje známky Kybernetického bezpečnostního incidentu (KBI), je zahájen proces "Řešení incidentů" v rámci níže uvedené služby CSIRT-SLA-1 – Řešení incidentů.

Jinak je událost postoupena s doporučením řešitelům dle platné komunikační matice a definovaných scénářů reakce.

|  |  |
| --- | --- |
| Rozsah zaručeného provozu služby | Maximální doba trvání analýzy |
| 24 x 7 (nepřetržitě) | 90 minut (počítáno od vzniku tiketu) |

## Specifikace služby SOC-SLA-3 – Threat Hunting

Služba „Threat Hunting“ (TH) využívá kombinaci digitální forenzní analýzy a různých taktik reakce na incidenty k aktivnímu vyhledávání skrytých kybernetických hrozeb. Soustředí se zejména na aktivity, které mohou běžné techniky detekce hrozeb přehlédnout, případně je identifikují jako nízkoseveritní. Pozoruje varovné signály a aplikuje přístup založený na hypotézách, přičemž využívá informace o útočných taktikách (Mitre ATT&CK), nebo indikátorech kompromitace (IoC).

**Služba musí obsahovat:**

* zajištění pravidelného a procesně podloženého TH,
* doplnění sběru dat tak, aby odpovídal potřebám stanovených procesů,
* vytvoření plánu zajišťujícího periodickou realizaci TH dle stanovených procesů,
* Event-based hunting, Anomaly-based hunting, TTP-based hunting, IoC-based hunting,
* pravidelnou verifikaci TH postupů.

|  |  |
| --- | --- |
| Rozsah zaručeného provozu služby | Periodická realizace |
| 8 x 5 (od 8.00 do 16.00 hod.) | 1x týdně,IoC-based hunting do 2 hod. od přijetí požadavku |

**Garantovaná dostupnost služeb SOC SLA 1-3 mimo plánované a oboustranně ujednané odstávky:**

* max. doba jednoho výpadku činí 75 min.,
* max. kumulovaná doba výpadků za aktuální den a 30 předcházejících činí 120 min.,
* max. kumulovaná doba výpadků za aktuální den a 365 předcházejících činí 240 min.

## Specifikace služby CSIRT-SLA-1 – Řešení incidentů

Cílem této služby je zajistit co nejrychlejší obnovení dostupnosti dohledovaných služeb objednatele a současně minimalizovat důsledky takového výpadku. Služba je založena na sdílení know-how analytického týmu poskytovatele a poskytování spolupráce a součinnost při koordinaci činností a při vyhodnocování vývoje incidentu a reakcích na KBI.

**Služba musí obsahovat:**

* reakci na nahlášení incidentu,
* řešení jednotlivých incidentů:
	+ spolupráce s administrátory při analýze napadeného / dotčeného IS s cílem zabránit vzniku a dalším škodám na IS,
	+ dle pokynů Manažera kybernetické bezpečnosti (MKB) se podílí na zjišťování anomálií a získávání důkazů,
	+ dle pokynů MKB se podílí se na analýze rozsahu škod a příčin KBI,
	+ dle pokynů MKB se podílí na "Hlášení o KBI",
	+ podílí se na formulaci návrhu nápravných a preventivních opatření pro eliminaci opakování KBI v budoucnu,
	+ poskytuje součinnost při tvorbě souhrnné zprávy o KBI s vyhodnocením příčin, rozsahu škod a postupů obnovy,
* sběr podkladů pro aktualizaci dokumentace,
* pravidelný reporting

|  |  |
| --- | --- |
| Rozsah zaručeného provozu služby | Zahájení plnění |
| 24 x 7 (nepřetržitě) | Neprodleně po potvrzení KBI |

## Specifikace dodatečných analytických služeb

Dostupnost poskytování následných analytických služeb v režimu 8 x 5, tj. v pracovních dnech od pondělí do pátku v době od 8.00 do 16.00 hod.

# Fáze poskytování služeb

## Zkušební fáze

**Poskytovatel v rámci zkušební fáze provede:**

* Prvotní analýzu bezpečnostních hrozeb relevantních pro aplikace a služby provozované objednatelem a návrh implementačního postupu pro aplikaci požadavků Objednatele – implementační projekt.
* Posouzení informací ze systému Logmanagementu NTR pro jeho případné doplnění nebo rozšíření, i zdrojů logů, jejichž provozně bezpečnostní informace poskytovatel bude také sbírat, korelovat a analyzovat. Počet monitorovaných systémů, resp. jejich kategorizace se může po dobu poskytování služby změnit jak z podnětu poskytovatele, tak objednatele, jak budou také přibývat zdroje logů v centrálním Logmanagementu NTR.
* Návrh modifikace nastavení monitorovacích nástrojů, včetně atributů a parametrů potřebných pro řádné a efektivní provozování dohledového centra, zahrnující mj.:
	+ doporučení nastavení logování pro jednotlivé zdroje,
	+ provedení objednatelem odsouhlaseného nastavení logování jednotlivých zdrojů,
	+ kontrola a doporučení nastavení korelačních pravidel, reportů, parametrů,
	+ provedení objednatelem odsouhlaseného nastavení korelačních pravidel, reportů, parametrů,
	+ výběr událostí a parametry jejich záznamů a metody sběru z jednotlivých zdrojů,
	+ návrh doplňování logovaných informací z dalších zdrojů pro zlepšení jejich relevantnosti či srozumitelnosti.
* Návrh relevantních procesů, potřebných pro řádné a efektivní provozování dohledového centra, zahrnující mj. činnosti při zjištění bezpečnostního incidentu, výpadku či omezení dostupnosti vybraných informačních systémů, způsoby notifikace kompetentních osob objednatele podle schváleného eskalačního schématu.
* Vytvoření návrhu vzorového reportu (struktury) o událostech a incidentech.
* Vytvoření a odsouhlasení “Exit strategie”.
* Připojení monitorovacích nástrojů NTR na dohledové centrum.

**Výstupem zkušební fáze bude:**

* Vytvoření technických podmínek nezbytných pro řádné poskytování služby v provozní fázi.
* Napojení požadovaných zdrojů a informací objednatele do prostředí poskytovatele služeb SOC.
* Definice logovacích schémat, která určí, z jakých zdrojů, jakým způsobem a pomocí jakých senzorů (agent, sonda, apod.) budou data sbírána, případně obohacována a korelována. Pokud existuje stávající logovací schéma, je možné jej využít a v rámci přípravné fáze projektu doplnit o požadovaná data. Součástí služby je také revize definovaných schémat, a to minimálně jednou ročně, případně v rámci významné změny (dle definice v procesu objednatele).
* Revize a popis integrace do procesu zvládání KBI objednatele (např. klasifikace …).
* Definice, popis reakčních scénářů (IRP, Workbooky/SOP, Playbooky – automatizované části reakcí).
* Optimalizace nastavení relevantních procesů a jejich integrace s bezpečnostními procesy objednatele.
* Aplikace popsaných detekčních scénářů a logovacích schémat.
* Kategorizace událostí a incidentů a způsob reakce na tyto incidenty včetně definování SLA.
* Vyhodnocení a optimalizace stávajících detekčních a prevenčních nástrojů KYBEZ objednatele.
* Odladění komunikačních a eskalačních schémat.
* Exit strategie, která musí obsahovat minimálně následující body:
	+ předání řešených událostí a incidentů včetně potřebných nápravných opatření (mitigací) a sesbíraných artefaktů,
	+ předání vytvořených reakčních scénářů,
	+ předání typově řešených událostí (knowledge management událostí),
	+ předání aktuálních dokumentací, vč. Popisu společně optimalizovaných procesů,
	+ předání informací v takové podobě, kterou objednatel může po ukončení poskytování služby informačně využít, data musí být ve strojově zpracovatelné podobě.
* Table TOP testy.
* Simulace a reakce na KBI v rozsahu NÚKIB požadovaných vektorů útoku:
	+ Phishing (lákání citlivých údajů, apod.),
	+ Spear-phishing (cílený a informovaný útok e-mailem),
	+ Podvodný e-mail (lákání finančních obnosů, vydírání),
	+ Denial of service (DoS, DDoS),
	+ Scanning (scan rozsahu vnější sítě),
	+ Sniffing (scan ve vnitřní síti, zachytávání komunikace),
	+ Pokus o zneužití zranitelnosti (známých CVE nebo zranitelností nultého dne),
	+ Drive-by download,
	+ Útok skrze dodavatele služeb,
	+ Spam (nevyžádaná pošta),
	+ Útoky skrze webové aplikace (buffer overflow, SQL injection, cross-site scripting),
	+ Ransomware,
	+ Škodlivý obsah (virus, červ, trojský kůň, apod.),
	+ Nelegální těžba kryptoměn (Coinminer),
	+ Malicious Insider.
* Vytvoření a předání implementační studie, včetně vzorového reportu o událostech a incidentech.
* Prezentace nastavení služby a výstupů zkušební fáze vybraným zaměstnancům objednatele.
* Vyhodnocení zkušební fáze a přechod do provozní fáze.

**Všechny výše uvedené skutečnosti budou zahrnuty do hmotných výstupů služeb zkušební fáze, které budou tvořit implementační studii.**

**Implementační studie bude obsahovat mj.:**

* Návrh modifikace nastavení existujících monitorovacích nástrojů.
* Scénáře pro řešení bezpečnostních a provozních incidentů a událostí včetně SLA.
* Návrh vzorového reportu o událostech a incidentech.

Výstupy zkušební fáze budou předloženy poskytovatelem objednateli v písemné elektronické podobě a budou podléhat schválení objednatele. Zkušební fáze je provedena,
je-li dokončena a jsou-li předány veškeré výstupy dle předchozích odstavců.

## Provozní fáze

Poskytovatel zajistí běžný provoz dohledového centra po dobu 21 měsíců od provedení zkušební fáze.

**Příloha č. 2 smlouvy – Bezpečnostní pravidla**

Objednatel je ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále také jen ***„ZoKB“***), provozovatelem základní služby v odvětví zdravotnictví (dále též „***provozovatel***“). Poskytovatel se v této souvislosti zavazuje poskytovat podporu při zajišťování kybernetické bezpečnosti a plnění povinností vyplývajících ze ZoKB a jeho prováděcích předpisů, v níže uvedeném rozsahu:

1. Poskytovatel se zavazuje přijmout a dodržovat bezpečnostní opatření identifikovaná provozovatelem, která jsou relevantní a přiměřená pro plnění této smlouvy.
2. Poskytovatel zajistí vlastní kybernetickou bezpečnost tak, aby bylo minimalizováno riziko zasáhnout přes poskytovatele sítě a informační systémy provozovatele. Poskytovatel je povinen při plnění podle této smlouvy zachovat bezpečnost informací a dat obsažených v informačním systému základní služby (dále také jen ***„ISZS“***), nebo v jiných informačních systémech, které jsou plněním této smlouvy dotčeny, a to zejm. z pohledu důvěrnosti, dostupnosti a integrity. Poskytovatel je povinen informace a data obsažená v ISZS, nebo v jiných informačních systémech, které jsou plněním této smlouvy dotčeny, chránit proti jejich neoprávněnému užití třetí osobou
3. Plnění dle této smlouvy je poskytovatel povinen poskytovat tak, aby důvěrnost, dostupnost a integrita informací a dat nebyla porušena, ohrožena, ani omezena v souladu s požadavky dokumentace systému řízení bezpečnosti informací u provozovatele. Je-li k plnění dle této smlouvy nezbytné důvěrnost, dostupnost či integritu informací nebo dat omezit, ohrozit nebo porušit, může tak poskytovatel učinit pouze po předchozím souhlasu provozovatele a jen v rozsahu jím předem odsouhlaseném.
4. Poskytovatel není oprávněn užít informace ani data obsažená v ISZS nebo jiných informačních systémech, které jsou plněním této smlouvy dotčeny, k jiným účelům než ke splnění závazků z této smlouvy.
5. Poskytovatel je povinen provozovatele písemně informovat o způsobu řízení rizik na straně poskytovatele a o zbytkových rizicích souvisejících s plněním této smlouvy, a to bez zbytečného odkladu po nabytí účinnosti této smlouvy. Poskytovatel je povinen zejména identifikovat jednotlivá konkrétní rizika spojená s plněním dle této smlouvy, jednotlivá konkrétní opatření k jejich eliminaci a zbytková rizika, která není možné přijatými opatřeními eliminovat. Poskytovatel je povinen řídit rizika související s plněním této smlouvy po celou dobu účinnosti smlouvy a na žádost provozovatele způsob řízení rizik provozovateli prokázat. Provozovatel je oprávněn řízení rizik poskytovatelem kontrolovat a poskytovatel je povinen k tomu provozovateli poskytnout součinnost. Provozovatel je oprávněn provádět kontrolu způsobu řízení rizik poskytovatelem pouze v takovém rozsahu, aby tím nepřiměřeně nezasahoval do plnění dle této smlouvy, neohrozil důvěrnost, dostupnost a integritu dat poskytovatele a nezvyšoval náklady na straně poskytovatele.
6. Poskytovatel se zavazuje po dobu trvání této smlouvy zajistit přístup k technickému, technologickému a personálnímu vybavení, které je potřebné pro řádné a včasné plnění této smlouvy.
7. Poskytovatel se zavazuje poskytnout provozovateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti vyplývající z této smlouvy, jakož i ze ZoKB a vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále také jen ***„VoKB“***). Poskytovatel se zavazuje umožnit provozovateli provedení kontrol dodržování povinností poskytovatele, včetně auditů prováděných provozovatelem či auditorem, kterého provozovatel k auditu pověří, a poskytnout k těmto kontrolám a auditům veškerou potřebnou součinnost.
8. V rámci prevence kybernetických bezpečnostních incidentů, které by mohly mít potenciální nepříznivý vliv na základní služby, nebo které by se mohly týkat kybernetické bezpečnosti sítí a informačních systémů provozovatele (dále jen „incidenty“):
	1. Poskytovatel přijímá od provozovatele varování před incidenty a hrozbami v návaznosti na výstrahy, varování a další informace sloužící k minimalizování, odvrácení nebo nápravě následků incidentů.
	2. Poskytovatel přijímá od provozovatele identifikaci relevantních varování, ochranných či reaktivních opatření vydaných Národním úřadem pro kybernetickou a informační bezpečnost (dále též „***NÚKIB***“). V návaznosti na tuto identifikaci poskytovatel provádí preventivní opatření.
	3. Poskytovatel předchází vzniku incidentů v rámci vlastní infrastruktury.
	4. Poskytovatel systematicky získává, eviduje, analyzuje a vyhodnocuje informace o incidentech.
	5. Poskytovatel zasílá provozovateli upozornění na incidenty, o kterých se dozvěděl z vlastní činnosti.
	6. Poskytovatel vytváří a zvyšuje bezpečnostní povědomí svých zaměstnanců podílejících se na plnění této smlouvy a/nebo majících přístup k informacím a údajům provozovatele.
	7. Poskytovatel zajistí průběžné monitorování zranitelností a udržení situačního povědomí o dění v rámci daného systému.
9. V rámci reakce na incidenty:
	1. Poskytovatel informuje provozovatele o incidentech s významným dopadem na předmět této smlouvy.
	2. Poskytovatel řeší incident koordinací řešení incidentu, odezvou nebo jinou reakcí na něj, ohraničením incidentu a jeho dopadů, nápravou následků incidentu, reakcí na incident a podporou reakcí na incident (dále též „***opatření k řešení incidentu***“). Při řešení incidentu je poskytovatel povinen na žádost provozovatele poskytnout informace provozovateli a příslušným orgánům České republiky a poskytnout součinnost v nezbytném rozsahu.
	3. Poskytovatel na vyzvání provozovatele oznamuje a prokazuje provedení opatření k řešení incidentu a jejich výsledek.
	4. Poskytovatel usiluje o zajištění informací o incidentu tak, aby bylo možno jejich použití v trestním řízení, bude-li ho provozovatel iniciovat.
	5. Poskytovatel předkládá na výzvu provozovatele po vyřešení incidentu návrh opatření k zabránění pokračování, šíření a opakovaného výskytu incidentu (dále jen „***ochranná opatření***“). Provozovatel ochranná opatření schvaluje, v případě nedostatečnosti navrhuje jejich úpravu.
	6. Poskytovatel provádí provozovatelem schválená ochranná opatření.
10. Pokud poskytovatel využívá při poskytování plnění poddodavatele, zavazuje se zajistit dodržování veškerých bezpečnostních opatření stanovených provozovatelem rovněž ve smluvních vztazích se svými poddodavateli. Tuto skutečnost se poskytovatel zavazuje doložit provozovateli na vyžádání předložením příslušného smluvního vztahu uzavřeného s tímto poddodavatelem, případně předložením čestného prohlášení o řádném naplňování této povinnosti.
11. Poskytovatel poskytuje provozovateli licenci nebo podlicenci, není-li oprávněn licenci poskytnout, na veškerý software, který má povahu autorského díla 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, poskytnutý podle této smlouvy, ke kterému je oprávněn licenci nebo podlicenci poskytnout (veškerý takový software dále souhrnně jen „vlastní software“), a zavazuje se zajistit, aby nejpozději k okamžiku instalace softwaru dodaného podle smlouvy, nebo nabytím účinnosti smlouvy byla provozovateli udělena licence nebo podlicence na software dodaný podle smlouvy, ke kterému poskytovatel není oprávněn licenci nebo podlicenci poskytnout (dále jen „cizí software“, licence a podlicence k vlastnímu a cizímu software se poskytuje, resp. musí být poskytnuta jako bezúplatná, nevýhradní, pro území České republiky, na dobu trvání majetkových práv k předmětu licence a bez omezení věcného či osobního rozsahu. Poskytovatelem udělená nebo zajištěná licence na software se vztahuje ve shora uvedeném rozsahu i na jakákoli rozšíření, upgrady, updaty, patche a další změny autorských děl poskytnutých podle smlouvy.
12. Poskytovatel se zavazuje poskytnout provozovateli veškerou potřebnou součinnost pro likvidaci nepotřebných dat. Za tím účelem poskytovatel s provozovatelem dohodnou konkrétní rozsah a časové intervaly pro likvidaci dat. Nedojde-li k dohodě, je rozsah a podmínky likvidace dat oprávněn určit provozovatel. Podmínky likvidace musí být v souladu s přílohou č. 4 VoKB. Poskytovatel se zavazuje protokolárně vymazat nebo jinak zlikvidovat veškeré poskytovateli dostupné kopie dat či provozních údajů, které byly poskytovateli zpřístupněny nebo poskytovatelem či jeho poddodavateli vytvořeny na základě smlouvy nebo v souvislosti s plněním smlouvy. Poskytovatel je povinen před likvidací předat všechna taková data a provozní údaje provozovateli. Poskytovatel umožní provozovateli dohled nad průběhem likvidace kopií dat a provozních údajů.
13. Poskytovatel je povinen spolupracovat s provozovatelem na řízení změn. Poskytovatel se zavazuje poskytnout provozovateli veškerou nezbytnou součinnost při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testování a zajištění možnosti navrácení do původního stavu. Provozovatel má oprávnění zapojit poskytovatele do řízení kontinuity činností, a to zejména oprávnění k zahrnutí poskytovatele do plánu kontinuity činností, který souvisí s ISZS nebo s jeho HW komponentami a souvisejících služeb a/nebo zahrnutí poskytovatele do havarijního plánu provozovatele.
14. Pokud dojde k významné změně kontroly nad poskytovatelem, je provozovatel oprávněn odstoupit od smlouvy. Poskytovatel je povinen provozovatele o významné změně kontroly nad poskytovatelem bez zbytečného odkladu informovat. Kontrolou se rozumí zejména ovládání či řízení podle § 74 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů, či ekvivalentní postavení, nebo dojde ke změně vlastnictví či oprávnění nakládat s aktivy využívanými poskytovatelem k plnění této smlouvy a tato změna bude provozovatelem vyhodnocena jako nepřijatelné bezpečnostní riziko ve smyslu ZoKB a/nebo VoKB.
15. Poskytovatel se zavazuje pro případ skončení účinnosti smlouvy poskytnout provozovateli veškerou potřebnou součinnost, dokumentaci a informace za účelem plynulého a řádného převedení všech činností souvisejících s provozem, servisem a rozvojem předmětu smlouvy na jiné, nové řešení provozovatele či jiného poskytovatele.
16. Veškerá uživatelská a/nebo provozní data ISZS musí být provozovateli 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 provozovatel 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. Neurčí-li provozovatel jinak, je poskytovatel povinen data exportovat v kódování českého jazyka UTF-8. Soulad exportovaných dat s těmito požadavky, jakož i jejich úplnost, podléhá akceptaci provozovatele.
17. Smlouva mezi poskytovatelem a provozovatelem je uzavřena podle právních předpisů upravujících kybernetickou bezpečnost, jakož i v souladu s obecně závaznými právními předpisy platnými a účinnými k okamžiku uzavření této smlouvy, a dopadajícími na poskytované plnění. Poskytovatel je povinen v průběhu plnění této smlouvy monitorovat změny těchto právních předpisů a poskytovat plnění v souladu s aktuálním zněním těchto právních předpisů. Z uvedených důvodů se pod výše použitými zkratkami ZoKB a VoKB rozumí i právní předpisy, které se platnými a účinnými stanou v době plnění této smlouvy a které nahradí právní předpisy uvedené v této příloze smlouvy, které jsou platné a účinné ke dni uzavření této smlouvy.
18. Není-li stanoveno v této smlouvě jinak, je poskytovatel povinen se řídit vnitřními bezpečnostními pravidly pro dodavatele dostupnými na <https://www.nem-tr.cz/bezpecnostni-pravidla-pro-dodavatele/>

**Příloha č. 3 smlouvy – Realizační tým**

***Pokyn pro dodavatele:*** *V této příloze dodavatel před uzavřením smlouvy uvede seznam členů realizačního týmu dle přílohy č. 2 Výzvy k podání nabídek.*