# Smlouva na implementaci systému řízení bezpečnosti informací a poskytování služeb dohledového centra

## I.
## Smluvní strany

**1. Moravskoslezské datové centrum, příspěvková organizace**

se sídlem: Na Jízdárně 2824/2, 702 00 Ostrava - Moravská Ostrava

zastoupena: Ing. RNDr. Alois Slovák, ředitel organizace

IČO: 068 39 517

DIČ: CZ06839517

bankovní spojení: [redacted]

číslo účtu:

(dále jen ***„objednatel")***

a

**2. Společníci společnosti „KONSORCIUM VISITECH A DATASYS"**

společnost dle § 2716 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, jež tvoří:

**VISITECH a.s.**

se sídlem: Košinova 655/59, 612 00 Brno, Královo Pole

zastoupena: Pavel Kocour, předseda představenstva

IČO: 25543415

DIČ: CZ25543415

bankovní spojení: [redacted]

číslo účtu:

Zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně, sp. zn. B6323

jako vedoucí společník

a

**DATASYS s.r.o.**

se sídlem: Jeseniova 2829/20, 130 00 Praha 3

zastoupena: Pavel Kocour, na základě smlouvy o společnosti ze dne 5. 8. 2022

IČO: 61249157

DIČ: CZ61249157

Zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, sp. zn. C28862

(dále jen ***„poskytovatel")***

(objednatel a poskytovatel dále jednotlivě též jen ***„smluvní strana"*** nebo společně ***„smluvní strany")***

## II.
## Základní ustanovení

1. Tato smlouvaje uzavřena dle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen ***„občanský zákoník"),*** s přihlédnutím k § 2586 a násl. občan ho zákoníku; práva a povinnosti stran touto smlouvou neupravená se řídí příslušnými ustanoveními občanského zákoníku.
2. Smluvní strany prohlašují, že údaje uvedené v čl. I této smlouvy jsou v souladu se skutečností v době uzavření smlouvy. Smluvní strany se zavazují, že změny dotčených údajů oznámí bez prodlení písemně druhé smluvní straně. Při změně identifikačních údajů smluvních stran včetně změny účtu není nutné uzavírat ke smlouvě dodatek.
3. Je-li poskytovatel plátcem DPH, prohlašuje, že bankovní účet uvedený v čl. I odst. 2 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 účtu poskytovatele je poskytovatel povinen doložit vlastnictví k novému 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.
4. Smluvní strany prohlašují, že osoby podepisující tuto smlouvu jsou k tomuto jednání oprávněny.
5. Poskytovatel prohlašuje, že není obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (člen vlády nebo vedoucí jiného ústředního správního úřadu, v jehož čele není člen vlády), nebo jím ovládaná osoba vlastní podíl představující alespoň 25% účast společníka v obchodní společnosti. Poskytovatel bere na vědomí, že pokud je uvedené prohlášení nepravdivé, bude smlouva považována za neplatnou.
6. Smlouva se mezi výše uvedenými smluvními stranami uzavírá na základě výsledku zadávacího řízení na veřejnou zakázku s názvem *„Začlenění organizace Zdravotnická záchranná služba Moravskoslezského kraje do jednotného krajského řešení kybernetické bezpečnosti"* (dále jen ***„Veřejná zakázka"),*** zadávanou v jednacím řízení bez uveřejnění dle ust. § 67 zákona č. 134/2016 Sb., o zadávání veřejných zakázkách, ve znění pozdějších předpisů (dále jen ***„ZZVZj.*** Jednotlivá ujednání smlouvy tak budou vykládána v souladu se zadávacími podmínkami Veřejné zakázky uvedenými v zadávací dokumentaci včetně jejich příloh a v souladu s nabídkou poskytovatele podanou na Veřejnou zakázku, jež tvoří přílohu č. 5 Smlouvy.
7. Poskytovatel prohlašuje, že se detailně seznámil s rozsahem a povahou předmětu plnění smlouvy, že jsou mu známy veškeré relevantní technické, kvalitativní a jiné podmínky

nezbytné pro realizaci předmětu plnění smlouvy, a že disponuje takovými kapacitami (zejm. realizačním týmem dle přílohy č. 2) a odbornými znalostmi, které jsou nezbytné pro realizaci předmětu plnění smlouvy za dohodnuté maximální smluvní ceny uvedené ve smlouvě.

8. Poskytovatel dále prohlašuje, že jím poskytované plnění odpovídá všem požadavkům vyplývajícím z platných právních předpisů, které se na plnění vztahují.

9. Není-li výslovně ve smlouvě u lhůt či dob uvedeno, že příslušné dny jsou pracovní, jedná se o dny kalendářní.

10. Poskytovatel bere na vědomí, že u objednatele, resp. Zdravotnické záchranné služby Moravskoslezského kraje, příspěvkové organizace, se předpokládá, že bude dle nově připravovaného zákona o kybernetické bezpečnosti (ve vazbě na směrnici Evropského parlamentu a Rady (EU) 2022/2555 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (směrnice NIS2)) poskytovatelem regulované služby, a proto se poskytovatel uzavřením smlouvy stane jeho významným dodavatelem dle § 2 písm. n) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen ***„VKB"),*** resp. ve smyslu později účinného právního předpisu, který VKB nahradí. Objednatel je tudíž povinen dle relevantních právních předpisů v oblasti kybernetické bezpečnosti provádět pravidelnou analýzu rizik, identifikovat rizika a identifikovaná rizika řídit. Poskytovatel je při poskytování plnění rovněž povinen zohlednit analýzu bezpečnostních rizik ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících předpisů, ve znění pozdějších předpisů, potažmo ve smyslu nové legislativy, která uvedený zákon a VKB nahradí.

## III.
## Seznam zkratek a vymezení pojmů

1. Pro účely této smlouvy (a jejích příloh) se smluvní strany dohodly na následujícím vymezení pojmů a zkratek:

   a) Pod zkratkou **GDPR** se rozumí nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

   b) Pod pojmem **hmotné výstupy služeb** se rozumí písemně vypracovaná dokumentace poskytovatelem, která se vztahuje k poskytování služeb a která je specifikovaná příloze č. 1 této smlouvy.

   c) Pod zkratkou **IS** se rozumí informační systémy.

   d) Pod zkratkou **ISMS** se rozumí Information Security Management System - Systém řízení bezpečnosti informací.

   e) Pod zkratkou **MSDC** se rozumí objednatel, tj. Moravskoslezské datové centrum p. o.

f) Pod zkratkou **NDA** se rozumí Non-Disclosure Agreement, dohoda o mlčenlivosti ve znění dodatku č. 1, kterou mezi sebou smluvní strany uzavřely dne 6. 6. 2022 (v případě NDA mezi MSDC a VISITECH, a.s.) a dne 9. 6. 2022 (v případě NDA mezi MSDC a DATASYS s.r.o.). Dodatek č. 1 k NDA mezi sebou smluvní strany uzavřely dne 3. 1. 2024 (mezi MSDC a VISITECH, a.s.) a dne 9. 1. 2024 (mezi MSDC a DATASYS s.r.o.).

g) Pod zkratkou **SOC** se rozumí Security operation center - centrum kybernetické bezpečnosti.

h) Pod pojmem **ZZS MSK** se rozumí Zdravotnická záchranná služba Moravskoslezského kraje, příspěvková organizace.

Další pojmy a zkratky jsou definovány v textu a v přílohách této smlouvy, a to zejména v příloze č. 1 (technická specifikace).

## IV.
## Účel a předmět smlouvy

1. Účelem této smlouvy je:

   *V oblasti ISMS*

   - ustanovení a zavedení bezpečnostních zásad do praxe ZZS MSK v rozsahu poskytování služeb řešící korporátní úroveň systému řízení bezpečnosti informací (blíže viz příloha č. 1 této smlouvy).

   *V oblasti SOC*

   - komplexní zajištění aktivní kybernetické bezpečnosti jako výstupu poskytovaných služeb SOC s pomocí provozovaných nástrojů pro vyhodnocování kybernetických bezpečnostních událostí, provozních událostí ve výpočetních systémech a v komunikačních sítích u ZZS MSK (blíže viz příloha č. 1 této smlouvy).

2. Předmětem této smlouvy je implementace systému řízení bezpečnosti informací ISMS a poskytování služeb ISMS a komplexní zajištění služeb centra kybernetické bezpečnosti (SOC) k zajištění dohledu operátory, provozu nástrojů pro sběr a vyhodnocování kybernetických bezpečnostních událostí v provozovaných systémech a v komunikačních sítích objednatele (ZZS MSK) se zajištěním prevence a aktivní reakce na případné kybernetické incidenty. Podrobná specifikace služeb je uvedena v příloze č. 1 této smlouvy.

3. Poskytovatel se zavazuje poskytnout pro objednatele (ZZS MSK) služby na svůj náklad a nebezpečí. Poskytování služeb je rozplánováno do následujících etap:

   a) **Základní implementace ISMS -** zahrnuje základní implementaci systému řízení bezpečnosti informací ISMS v rámci ZZS MSK v rozsahu nutném pro zahájení poskytování služeb SOC; bližší specifikace je uvedena v příloze č. 1 této smlouvy.

   b) **Implementace ISMS a poskytování služeb ISMS -** zahrnuje implementaci ISMS včetně zaškolení zaměstnanců a následné poskytování služeb ISMS; bližší specifikace je uvedena v příloze č. 1 této smlouvy.

c) **Adaptační fáze SOC -** adaptační fáze dohledového centra zahrnuje zpracování prováděcího (implementačního) projektu v rozsahu dle přílohy č. 1 této smlouvy; návrh prováděcího (implementačního) projektu bude předán v elektronické podobě k vyjádření objednateli nejméně 10 pracovních dnů před uplynutím lhůty dle odst. V.3 této smlouvy, přičemž objednatel (příp. ZZS MSK) vznese případné připomínky do 4 pracovních dnů od předání návrhu projektu; poskytovatel bude povinen připomínky zapracovat a následně předloží projekt objednateli k akceptaci ve lhůtě do 5 pracovních dnů od přijetí připomínek; po akceptaci bude finální projekt doručen objednateli v listinné podobě, a dále činnosti poskytovatele dle specifikace uvedené v příloze č. 1 této smlouvy; návrhy výstupů z adaptační fáze SOC budou předány v elektronické podobě k vyjádření objednatele nejméně 10 pracovních dnů před uplynutím lhůty dle odst. V.3 této smlouvy, přičemž objednatel (příp. ZZS MSK) vznese případné připomínky do 4 pracovních dnů od předání návrhů výstupů; poskytovatel bude povinen připomínky zapracovat a následně předloží výstup objednateli k akceptaci ve lhůtě do 5 pracovních dnů od přijetí připomínek; po akceptaci bude finální výstup doručen objednateli v listinné podobě. Součástí adaptační fáze před spuštěním do rutinního provozu bude testování v rozsahu dle přílohy č. 1 této smlouvy.

d) **Provozní fáze SOC** - představuje rutinní provoz dohledového centra a souvisejících technologií pro ZZS MSK s podporou MSDC dle specifikace uvedené v příloze č. 1 této smlouvy.

## V.
## Místo předání a doba plnění

1. Poskytovatel je povinen předat objednateli hmotné výstupy služeb v místě předání, kterým je budova MSDC na adrese Na Jízdárně 2824/2, 702 00 Ostrava - Moravská Ostrava.

2. Služby je poskytovatel oprávněn poskytovat vzdáleně ze svých vlastních prostor na svém vlastním technickém vybavení. Místem poskytování služeb z vlastních prostor poskytovatele je Řipská 1321/11c, 627 00 Brno. Bližší podmínky poskytovaní služeb budou specifikovány na úvodní schůzce dle čl. IX odst. 4 této smlouvy a dále v prováděcím (implementačním) projektu.

3. Poskytovatel je povinen poskytnout služby dle etap podle čl. IV odst. 3 této smlouvy bez vad v těchto termínech:

   a) **Základní implementace ISMS -** do **3 měsíců** od nabytí účinnosti této smlouvy v rozsahu nutném pro zahájení poskytování služeb SOC,

   b) **Implementace ISMS a poskytování služeb ISMS -** po dokončení základní implementace ISMS bude provedena implementace ISMS včetně zaškolení ve lhůtě stanovené v prováděcím projektu (nejpozději však do 2 let od nabytí účinnosti této smlouvy) a následně budou poskytovány služby ISMS po **dobu neurčitou,**

c) **Adaptační fáze SOC, vč. prováděcího (implementačního) projektu -** do **4 měsíců** od nabytí účinnosti této smlouvy, a to včetně zapracování připomínek objednatele a akceptace,

d) **Provozní fáze SOC -** po **dobu neurčitou** od akceptace výstupů z adaptační fáze SOC.

## VI.
## Cena

1. Cena za služby činí:

| Poskytované služby | Cena bez DPH v Kč | Sazba DPH v % | Cena s DPH v Kč |
|---|---|---|---|
| **Cena za implementaci ISMS včetně zaškolení (zahrnuje také základní implementaci)** | **207 000,-** | **21** | **250 470,-** |
| **Cena za 3 měsíce poskytování služeb ISMS** | **22 200,-** | **21** | **26 862,-** |
| **Cena za poskytování služeb adaptační fáze SOC, vč. prováděcího (implementačního) projektu** | **492 000,-** | **21** | **595 320,-** |
| **Cena za 3 měsíce poskytování služeb provozní fáze SOC** | **508 500,-** | **21** | **615 285,-** |

2. Cena za služby zahrnuje veškeré náklady poskytovatele spojené se splněním jeho závazku z této smlouvy, tj. cenu služeb včetně dopravného, odměnu za poskytnutí licence, veškeré instalační práce apod. Cena za služby je stanovena jako nejvýše přípustná a není ji možno překročit s výjimkou navýšení dle odst. 4 tohoto článku.

3. 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 služeb bez DPH povinen účtovat DPH v platné výši. Smluvní strany se dohodly, že v případě změny ceny služeb v důsledku změny sazby DPH není nutno k smlouvě uzavírat dodatek. 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.

4. Cenu za služby provozní fáze ISMS a SOC lze v souvislosti s uplynutím druhého výročí poskytování služeb provozní fáze upravit z důvodu inflace za podmínek dále uvedených:
   - Inflací se rozumí meziroční inflace měřená vzrůstem úhrnného indexu spotřebitelských cen zboží a služeb, kterou udává každým kalendářním rokem Český statistický úřad za rok předcházející vyjádřená v procentech.
   - Počínaje třetím rokem zahájení poskytování služeb provozní fáze a dále do budoucna je poskytovatel oprávněn zvýšit cenu služeb provozní fáze nejčastěji

jednou ročně z důvodů inflace, a to o tolik procent, kolik procent činil součet inflace v letech předcházejících, ve kterých nedošlo ke zvýšení ceny dle tohoto odst. smlouvy; součástí (např. přílohou) daňového dokladu dle čl. VIII. odst. 4 smlouvy bude vymezení údajů o inflaci dle smlouvy, přičemž objednatel je oprávněn tuto fakturu před uplynutím lhůty splatnosti vrátit, pokud inflace nebude vyjádřena správně (vrácením vadné faktury poskytovateli přestává běžet původní lhůta splatnosti, nová lhůta splatnosti běží ode dne vystavení nové faktury).

- Cena služeb provozní fáze upravená z důvodu inflace se považuje za sjednanou cenu, která nevyžaduje uzavření dodatku ke smlouvě.

## VII.
## Předání hmotných výstupů služeb a nebezpečí škody

1. Objednatel se zavazuje převzít hmotné výstupy služeb specifikovaných v příloze č. 1 této smlouvy v případě, že tyto budou předány bez vad a nedodělků. O předání a převzetí hmotných výstupů služeb poskytovatel sepíše bezodkladně předávací protokol, ve kterém objednatel prohlásí, zda hmotné výstupy služeb přejímá (akceptuje), či nikoli (dále jen ***„předávací protokol“).*** Budou-li hmotné výstupy služeb vykazovat jakékoli vady či nedodělky, nebudou objednatelem převzaty (akceptovány) a tyto vady či nedodělky budou uvedeny v předávacím protokolu spolu se lhůtou k jejich odstranění. Po odstranění vad bude poskytovatelem opětovně sepsán předávací protokol ve smyslu tohoto článku smlouvy.
2. Poskytovatel a objednatel jsou oprávněni uvést v předávacím protokolu cokoliv, co budou považovat za nutné.
3. Předávací protokol musí obsahovat minimálně tyto náležitosti:
   a) číslo předávacího protokolu a datum jeho vyhotovení,
   b) číslo smlouvy a datum jejího uzavření, číslo veřejné zakázky (tj. N006/24/V00001302),
   c) označení hmotných výstupů služeb vč. soupisu dodaných jednotlivých položek a provedených prací, odpovídající jednoznačně jak obsahem, tak formátem technickým podmínkám a specifikacím dle členění této smlouvy,
   d) název, sídlo, IČO a DIČ objednatele a poskytovatele,
   e) prohlášení objednatele, že hmotné výstupy služeb přejímá (akceptuje) či nikoliv, pokud hmotné výstupy služeb nebudou objednatelem převzaty (akceptovány), bude protokol obsahovat specifikaci vad hmotných výstupů služeb včetně navrhovaného termínu jejich odstranění,
   f) jméno, vlastnoruční podpis, kontaktní telefon a e-mail zástupců objednatele a zástupců poskytovatele,

g) datum předání a převzetí hmotných výstupů služeb vč. označení doby začátku a konce prací.

4. V případě, že při plnění této smlouvy vznikne autorské dílo, které je chráněno předpisy upravující práva duševního vlastnictví (např. dokumentace jako dílo autorské apod.), vzniká objednateli právo toto autorské dílo užívat v rozsahu nezbytném pro naplnění účelu, ke kterému bylo vytvořeno.

## VIII.
## Platební a fakturační podmínky

1. Zálohové platby nebudou poskytovány.
2. Úhrada ceny za plnění předmětu této smlouvy bude objednatelem provedena takto:
   a) po dokončení implementace ISMS včetně zaškolení poskytovatel vystaví fakturu na částku odpovídající ceně za implementaci ISMS včetně zaškolení dle čl. VI. odst. 1 této smlouvy,
   b) po dokončení (akceptaci na základě úspěšného výsledku testování) adaptační fáze SOC vystaví fakturu na částku odpovídající ceně za adaptační fázi SOC dle čl. VI odst. 1 této smlouvy,
   c) vždy po uplynutí tří měsíců poskytování služeb ISMS poskytovatel vystaví fakturu na částku odpovídající ceně za 3 měsíce poskytování služeb ISMS dle čl. VI odst. 1 této smlouvy, s výjimkou závěrečné faktury po ukončení poskytování služeb dle písm. e) tohoto odstavce,
   d) vždy po uplynutí tří měsíců poskytování služeb provozní fáze SOC poskytovatel vystaví fakturu na částku odpovídající ceně za 3 měsíce poskytování služeb provozní fáze SOC dle čl. VI odst. 1 této smlouvy, s výjimkou závěrečné faktury po ukončení poskytování služeb dle písm. e) tohoto odstavce,
   e) po ukončení poskytování služeb a podpisu akceptačního protokolu podle čl. XVII odst. 5 této smlouvy poskytovatel vystaví závěrečnou fakturu na částku odpovídající doposud neuhrazené ceně poskytovaných služeb; v případě ukončení smlouvy v průběhu provozní fáze na částku odpovídající poměrné výši ceny uvedené v čl. VI odst. 1 této smlouvy přepočtené na kalendářní dny, po které poskytovatel poskytoval služby v souladu s touto smlouvou objednateli a které nebyly poskytovateli doposud uhrazeny.
3. Je-li poskytovatel plátcem DPH, podkladem pro úhradu ceny za služby bude faktura, která bude mít náležitosti daňového dokladu dle zákona o DPH a náležitosti stanovené dalšími obecně závaznými právními předpisy. Není-li poskytovatel plátcem DPH, podkladem pro úhradu ceny za služby bude faktura, která bude mít náležitosti účetního dokladu dle zákona č. 563/1991 Sb., o účetnictví, věznění pozdějších předpisů, a náležitosti stanovené dalšími obecně závaznými právními předpisy.
4. Faktura musí dále obsahovat:

a) číslo smlouvy objednatele, číslo veřejné zakázky (tj. N006/24/V00001302), IČO objednatele,

b) označení fakturovaných služeb dle odst. 2 tohoto článku smlouvy,

c) označení banky a číslo účtu, na který musí být zaplaceno (pokud je číslo účtu odlišné od čísla uvedeného v čl. I odst. 2, je poskytovatel povinen o této skutečnosti v souladu s čl. II odst. 2 a 3 této smlouvy informovat objednatele),

d) lhůtu splatnosti faktury,

e) označení osoby, která fakturu vyhotovila, včetně jejího podpisu a kontaktního telefonu a e-mailu,

f) číslo a datum předávacího protokolu dle čl. VII odst. 1 této smlouvy podepsaného oběma smluvními stranami po dokončení prováděcího (implementačního) projektu, implementace ISMS včetně zaškolení či adaptační fáze SOC, přičemž předávací protokol obsahující prohlášení objednatele, že plnění přejímá (akceptuje), bude přílohou příslušné faktury,

g) číslo a datum akceptačního protokolu dle čl. XVII odst. 5 této smlouvy podepsaného oběma stranami po ukončení smlouvy, který bude přílohou závěrečné faktury.

5. Povinnost zaplatit cenu za služby je splněna dnem odepsání příslušné částky z účtu objednatele.

6. Lhůta splatnosti faktury je dohodou stanovena na 30 kalendářních dnů ode dne jejího doručení objednateli. Doručení faktury se provede prostřednictvím provozovatele poštovních služeb, elektronicky na e-mail: info@msdc.cz nebo prostřednictvím datové schránky objednatele.

7. 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. Poskytovatel provede opravu vystavením nové faktury. Vrácením vadné faktury poskytovateli přestává běžet původní lhůta splatnosti. Nová lhůta splatnosti běží ode dne doručení nové faktury objednateli.

8. Je-li poskytovatel plátcem DPH, objednatel uplatní institut zvláštního způsobu zajištění daně dle § 109a zákona o DPH a hodnotu plnění odpovídající dani z přidané hodnoty uvedené na faktuře uhradí v termínu splatnosti této faktury stanoveném dle smlouvy přímo na osobní depozitní účet poskytovatele vedený u místně příslušného správce daně v případě, že:

   a) poskytovatel bude ke dni poskytnutí úplaty nebo ke dni uskutečnění zdanitelného plnění zveřejněn v aplikaci „Registr DPH" jako nespolehlivý plátce, nebo

   b) poskytovatel bude ke dni uskutečnění úplaty nebo ke dni zdanitelného plnění v insolvenčním řízení, nebo

c) bankovní účet poskytovatele určený k úhradě plnění uvedený na faktuře nebude správcem daně zveřejněn v aplikaci „Registr DPH".

9. Tato úhrada bude považována za splnění části závazku odpovídající příslušné výši DPH sjednané jako součást smluvní ceny za předmětné plnění. Objednatel nenese odpovědnost za případné penále a jiné postihy vyměřené či stanovené správcem daně poskytovateli v souvislosti s potenciálně pozdní úhradou DPH, tj. po datu splatnosti této daně.

## IX.
## Práva a povinnosti smluvních stran

1. Není-li stanoveno touto smlouvou výslovně jinak, řídí se vzájemná práva a povinnosti smluvních stran ustanoveními § 2586 a následujícími občanského zákoníku.

2. Poskytovatel je zejména povinen:

   a) Poskytnout služby řádně a včas za použití materiálu a postupů odpovídajících právním předpisům a technickým normám ČR. Služby musí odpovídat příslušným právním předpisům, normám nebo jiné dokumentaci vztahující se kjejich poskytování.

   b) Informovat objednatele o jakýchkoliv skutečnostech, které mohou mít zejména vliv na plnění této smlouvy nebo na bezpečnost informací či vznik škody objednateli, neprodleně poté co se o nich dozví.

   c) Umožnit objednateli kontrolu poskytování služeb kdykoliv v průběhu plnění smlouvy. Pokud objednatel zjistí, že poskytovatel neposkytuje služby řádně či jinak porušuje svou povinnost, poskytne poskytovateli lhůtu k nápravě; neučiní-li tak poskytovatel ve stanovené lhůtě, je objednatel oprávněn od smlouvy odstoupit.

   d) Dbát při poskytování služeb dle této smlouvy na ochranu životního prostředí a dodržovat platné technické, bezpečnostní, zdravotní, hygienické a jiné předpisy, včetně předpisů týkajících se ochrany životního prostředí.

   e) Postupovat při poskytování služeb s odbornou péčí.

   f) Ochraňovat veškeré informace získané v průběhu poskytování služeb. Poskytovatel se současně zavazuje, pokud není v této smlouvě výslovně stanoveno jinak, že informace získané v průběhu poskytování služeb nebude dále rozšiřovat nebo reprodukovat a nezpřístupní je třetí straně.

   g) Umožnit objednateli provést audit procesů a bezpečnostních opatření souvisejících s poskytovanými službami. Podrobná pravidla auditu jsou upravena v příloze č. 4 této smlouvy.

   h) Respektovat závěry a doporučení bezpečnostních výborů objednatele.

3. Objednatel je zejména povinen poskytnout poskytovateli nezbytnou součinnost nutnou k poskytnutí služeb.

4. Objednatel se zavazuje po uzavření této smlouvy svolat do svého sídla úvodní informační schůzku, kde bude dohodnut zejména postup přípravy prováděcího (implementačního) projektu, implementace ISMS a adaptační fáze SOC a dále poskytnuty nezbytné informace pro poskytování služeb. Schůzka bude realizována nejpozději do 1 týdne od nabytí

účinnosti této smlouvy a poskytovatel je povinen se této schůzky zúčastnit; po dohodě stran může být schůzka realizována rovněž distančně prostřednictvím videokonference. Smluvní strany se zavazují pořídit z úvodní schůzky zápis, ve kterém budou uvedeny všechny podstatné informace zejména související s poskytováním služeb, včetně rámcového časového harmonogramu jejich poskytování, a který bude opatřen podpisy zástupců smluvních stran.

5. Poskytovatel je povinen účastnit se na základě pozvánky objednatele všech jednání týkajících se předmětu smlouvy. Účast na těchto jednáních není považována za technickou podporu, údržbu, poradenství ani konzultaci a poskytovateli za takové jednání nenáleží odměna.

6. Poskytovatel je povinen z každého jednání dle předchozího odstavce vyhotovit zápis o průběhu a závěrech jednání, který bude v případě odsouhlasení podepsán zástupci objednatele i poskytovatele, a to bezprostředně po takovémto jednání a současně odeslán na e-mail objednatele nebo bude objednateli předán jinou obdobnou formou. Zápis bude obsahovat minimálně tyto náležitosti: pořadové číslo zápisu, datum konání, místo konání, seznam přítomných a omluvených účastníků, program jednání, popis sjednaných úkolů a závěrů jednání; popis splnění úkolů ujednaných na předchozím jednání; číslo smlouvy a datum jejího uzavření, číslo veřejné zakázky. Objednatel si vyhrazuje právo zápis nepřevzít, nepodepsat a prohlásit jej vadným, nebude-li obsahovat některý z výše uvedených údajů.

## X.
## Zaměstnanci a poddodavatelé poskytovatele a osoby zúčastněné na plnění předmětu smlouvy v jiném právním vztahu k poskytovateli (dále také *„pracovníci")*

1. Poskytovatel se zavazuje poskytovat služby prostřednictvím osob (realizačního týmu), jejichž seznam a popis rolí je uveden v příloze č. 2 této smlouvy. V případě, že poskytovatel hodlá nahradit člena realizačního týmu dle přílohy č. 2 této smlouvy jinou osobou, je povinen o tomto písemně informovat objednatele minimálně 3 pracovní dny předem a současně objednateli doručit doklady svědčící o tom, že tato nová osoba disponuje minimálně stejnou kvalifikací a zkušeností. Výměna osoby dle tohoto odstavce podléhá schválení objednatelem, přičemž objednatel není bez vážného důvodu oprávněn odmítnout udělení takového souhlasu. Poskytovatel je dále povinen do 3 pracovních dnů objednatele písemně informovat o jakýchkoli změnách pracovníků podílejících se přímo na realizaci služeb, či poskytování technické podpory, např. ukončení pracovního poměru zaměstnance poskytovatele, který má plnou vzdálenou správu k systému zálohování apod. Poskytovatel je současně povinen dodržovat v průběhu plnění personální rozdělení kompetencí dle přílohy č. 2 této smlouvy.

2. Poskytovatel před uzavřením této smlouvy poskytl a dále je povinen objednateli na úvodní schůzce dle čl. IX odst. 4 této smlouvy předat aktuální seznam poddodavatelů (včetně jejich identifikačních a kontaktních údajů a o tom, které činnosti pro něj v rámci předmětu plnění každý z poddodavatelů poskytuje) a tyto smluvně zavázat tak, aby plnili veškeré povinnosti poskytovatele uvedené v této smlouvě, ve stejném rozsahu jako je

zavázán sám poskytovatel. Poskytovatel je povinen kdykoliv na vyžádání objednatele předložit smlouvu uzavřenou mezi ním a poddodavatelem, ze které vyplývá tento závazek. Tímto ustanovením není dotčena odpovědnost poskytovatele za služby poskytnuté jeho poddodavateli, které si k provádění služeb zvolil. Poddodavatel poskytovatele může poskytovat část plnění prostřednictvím poddodavatele, avšak tento již nemůže využít dalšího poddodavatele (tzv. řetězec poddodavatelů je tedy omezen nejvýše na 2 vrstvy). Poddodavatel poskytovatele se zavazuje své poddodavatele smluvně zavázat tak, aby plnili veškeré povinnosti poskytovatele uvedené v této smlouvě, ve stejném rozsahu jako je zavázán sám poskytovatel. Poskytovatel je povinen kdykoliv na vyžádání objednatele předložit smlouvu uzavřenou mezi jeho poddodavatelem a dalším poddodavatelem, ze které vyplývá tento závazek.

3. Poskytovatel bere na vědomí, že jeho aktivity, které provádí na zařízeních objednatele prostřednictvím vzdáleného přístupu, budou monitorovány a zaznamenávány.

4. Poskytovatel je povinen písemně informovat objednatele o všech případných dalších (nových) poddodavatelích a o jejich změně, a to nejpozději do 7 kalendářních dnů ode dne, kdy poskytovatel vstoupil s poddodavatelem ve smluvní vztah či ode dne, kdy nastala změna, avšak nejpozději před zahájením plnění poddodavatele. Poskytovatel je oprávněn změnit poddodavatele, jehož pracovník je člen realizačního týmu dle přílohy č. 2 této smlouvy, jen z vážných objektivních důvodů a s předchozím písemným souhlasem objednatele, přičemž podmínky pro nahrazení pracovníka (člena realizačního týmu) jsou uvedeny v odst. 1 tohoto článku smlouvy.

5. Poskytovatel bere na vědomí, že objednatel si v souladu s ust. § 105 odst. 2 ZZVZ vyhradil, aby významné části plnění předmětu této smlouvy byly plněny přímo poskytovatelem, tedy nikoliv jinou osobou (poddodavatelem). Za významné části plnění předmětu této smlouvy objednatel považuje níže uvedené služby aktivní kybernetické bezpečnosti prostřednictvím SOC:

    - poskytování služeb dohledového centra nad bezpečnostními událostmi a incidenty;
    - zpracování prvotního hlášení o kybernetických bezpečnostních incidentech,
    - postoupení řešení běžných kybernetických bezpečnostních incidentů odpovědným osobám a je-li to žádoucí, provedení nezbytných opatření vedoucích k jejich řešení nebo alespoň zastavení šíření,
    - obsluha a administrace nástroje pro detekci kybernetických bezpečnostních událostí a vyhodnocování jeho výstupů,
    - obsluha a administrace nástroje pro vyhodnocení kybernetických bezpečnostních událostí (SIEM),
    - informování manažera kybernetické bezpečnosti o rozsahu činností, na které může mít kybernetický bezpečnostní událost dopad,
    - vyhodnocení závažnosti kybernetických bezpečnostních události (méně významné, významné a velmi významné události, či incidenty),

- informování manažera kybernetické bezpečnosti o závažné kybernetické bezpečnostní události, či incidentu,
- postoupení řešení odpovědným osobám a je-li to žádoucí, provedení také nezbytných opatření vedoucích k řešení (či alespoň snížení stupně klasifikace bezpečnostního incidentu),
- administrace a konfigurace specifických technologií v rámci zásahů při aktivním řešení incidentů v rámci kybernetické bezpečnosti (rozsah bude upřesněn v Prováděcím projektu ve vztahu k ZZS MSK,
- spolupráce s analytikem v úzce specializovaných oblastech vztažených k technologiím jednotlivých výrobců,
- pokud je to vzhledem k závažnosti incidentu žádoucí, pak realizování nezbytných opatření vedoucích k řešení (či alespoň snížení stupně klasifikace bezpečnostního incidentu),
- postoupení dalšího, následného řešení incidentu odpovědným osobám na straně ZZS MSK,
- obsluha a administrace nástrojů nejpokročilejších technologických řešení pro načítání, prohledávání, analýzy a vizualizaci velkých a složitých datových souborů,
- shromažďování relevantních informací, které jsou nezbytné při řešení případných soudních sporů, vyšetřování a řešení regulatorních otázek, finanční a jiné trestné činnosti,
- využití techniky ke shromažďování a uchovávání důkazního materiálu, zajištění důvěryhodnosti získaných údajů z konkrétního výpočetního celku a to způsobem, který je vhodný pro následné právní úkony,
- identifikace dalších systémů z forenzního pohledu, které mohou být s jistou pravděpodobnosti ohroženy kybernetickými útoky,
- poskytování znaleckého svědectví v soudním řízení,
- postoupení informací a řešení odpovědným osobám,
- vytváření a aktualizace hardeningových bezpečnostních politik,
- stanovení strategií postupů k přístupu a stanovení priorit, okamžitých oprav a oprav vedoucích k posílení zabezpečení a ochrany systémů v oblasti software, firmware, BIOS (serverů, sítí a jejich prvků, aplikací, databází, operačních systémů a nepotřebných účtů a oprávnění),
- odpovědnost za (činnosti v oblasti) řízení procesu zabezpečení konfigurace systémů vedoucí k omezení výskytu zranitelnosti,
- odpovědnost za (činnosti v oblasti) návrhy hardeningu zabezpečení a ochrany systémů,

- odpovědnost za (činnosti v oblasti) hardening aplikací s kontrolou vzájemných integrací s jinými aplikacemi a systémy s odstraněním nebo omezením nepotřebných integračních komponent a oprávnění.

Pro účely kontroly plnění této povinnosti je v příloze č. 2 této smlouvy uveden organigram a rozdělení kompetencí jednotlivých pracovníků poskytovatele.

6. Část plnění týkající se ISMS (ISO/IEC 27001) je povinen zajišťovat poskytovatel, který k tomu má příslušné osvědčení/certifikát ISO/IEC 27001:2014 (nebo aktuálnější), který je za tuto část plnění odpovědný.

***Sankce vůči Rusku a Bělorusku***

7. Poskytovatel odpovídá za to, že platby poskytované objednatelem dle této smlouvy nebudou přímo nebo nepřímo ani jen zčásti zpřístupněny osobám, vůči kterým platí tzv. individuální finanční sankce ve smyslu čl. 2 odst. 2 Nařízení Rady (EU) č. 208/2014 ze dne 5. 3. 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině a Nařízení Rady (ES) č. 765/2006 ze dne 18. 5. 2006 o omezujících opatřeních vůči prezidentu Lukašenkovi a některým představitelům Běloruska a které jsou uvedeny na tzv. sankčních seznamech (dle příloh č. 1 obou nařízení).

8. Bude-li kterékoliv z nařízení v budoucnu doplněno či nahrazeno jinou legislativou obdobného významu, uvedená povinnost se uplatní obdobně.

9. Poskytovatel odpovídá za to, že po dobu trvání smlouvy nejsou naplněny podmínky uvedené v nařízení Rady (EU) 2022/576 ze dne 8. dubna 2022, kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, tedy zejména, že poskytovatel není:

    - ruským státním příslušníkem, fyzickou nebo právnickou osobou se sídlem v Rusku,
    - právnickou osobou, která je z více než 50 % přímo či nepřímo vlastněna některou z osob dle předešlé odrážky, nebo
    - fyzickou nebo právnickou osobou, která jedná jménem nebo na pokyn některé z osob uvedených v předešlých odrážkách.

    Poskytovatel odpovídá za to, že po dobu trvání smlouvy žádná z výše uvedených podmínek není naplněna ani u jeho poddodavatele (nebo jiné osoby prokazující za poskytovatele kvalifikaci), který se bude na plnění této smlouvy podílet z více jak 10 % hodnoty plnění.

10. Poskytovatel je povinen objednatele bezodkladně informovat o jakýchkoliv skutečnostech, které mohou mít vliv na odpovědnost poskytovatele dle odst. 7 nebo 9 tohoto článku smlouvy. Poskytovatel je současně povinen kdykoliv poskytnout objednateli bezodkladnou součinnost pro případné ověření pravdivosti těchto informací.

11. Dojde-li k porušení pravidel dle odst. 7 nebo 9 tohoto článku smlouvy, je objednatel oprávněn odstoupit od této smlouvy; odstoupení se však nedotýká povinností poskytovatele vyplývajících ze záruky za jakost, odpovědnosti za vady, povinnosti zaplatit smluvní pokutu, povinnosti nahradit škodu a povinnosti zachovat důvěrnost informací souvisejících s plněním dle této smlouvy.

12. Dojde-li k porušení pravidel dle odst. 7 nebo 9 tohoto článku smlouvy, je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 250.000 Kč, a to za každý jednotlivý případ porušení. Smluvní pokuty se nezapočítávají na náhradu případně vzniklé škody, kterou lze vymáhat samostatně vedle smluvní pokuty, a to v plné výši.

## XI.
## Oznámení a komunikace

1. Veškerá komunikace na základě této smlouvy bude probíhat v souladu s tímto článkem a v českém jazyce. Kromě jiných způsobů komunikace dohodnutých mezi stranami se za účinné považují osobní doručování, doručování doporučenou poštou, datovou schránkou či elektronickou poštou, a to na adresy smluvních stran, nebo na takové adresy, které si strany vzájemně písemně oznámí. Kontaktní údaje jednotlivých zástupců smluvních stran jsou uvedeny v příloze č. 2 této smlouvy. V případě změn jednotlivých zástupců smluvních stran dojde k úpravě příslušných kontaktů v příloze č. 2 této smlouvy; při takovéto změně není nutné uzavírat ke smlouvě dodatek.
2. Oznámení správně adresovaná se považují za uskutečněná v případě osobního doručování anebo doručování doporučenou poštou okamžikem doručení, v případě zasílání elektronickou poštou okamžikem obdržení potvrzení druhé smluvní stran o doručení, provedeného stejným komunikačním kanálem.
3. Informace a materiály, které obsahují osobní údaje a důvěrné informace budou doručovány buď osobně, nebo zasílány elektronickou poštou a šifrovány minimálně na úrovni dle čl. XV odst. 10 této smlouvy. Další možností je předávání těchto údajů prostřednictvím nástroje / platformy pro zabezpečenou komunikaci a sdílení dokumentů (např. MS Teams či jiné).
4. V případě, kdy dojde k mimořádné situaci (či bezpečnostnímu incidentu), která může mít vliv na integritu a bezpečnost informací, osobních údajů či jiných dat, které lze považovat za citlivé, jež jsou spravovány objednatelem, je poskytovatel povinen o nich informovat též osoby určené k řešení těchto situací, jejichž kontakty jsou uvedeny v příloze č. 2 této smlouvy.

## XII.
## Licenční ujednání

1. Je-li relevantní, poskytovatel poskytuje touto smlouvou objednateli a objednatel touto smlouvou přijímá nevýhradní oprávnění k užití software dodávaného či jakkoliv zpřístupněného při poskytování služeb, a to všemi způsoby uvedenými v § 12 odst. 4 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.
2. Pokud jsou licence nezbytné a je-li to dáno charakterem služeb, poskytovatel poskytne (v případě proprietárního SW zajistí) objednateli veškeré potřebné licence či podlicence pro řádné poskytování všech služeb a provoz dohledového centra. Veškeré potřebné licence jsou zahrnuty v ceně plnění.

3. Poskytovatel výslovně prohlašuje, že je oprávněn disponovat právy k duševnímu vlastnictví, včetně práv autorských zahrnutých v předmětu poskytovaných služeb v rozsahu nezbytném k řádnému plnění předmětu této smlouvy.
4. Územní rozsah a časový rozsah licencí je neomezený.
5. Licence se vztahuje automaticky i na všechny nové verze, úpravy a překlady příslušného autorského díla.
6. Poskytovatel se zavazuje, že poskytováním služeb nezasáhne neoprávněně do autorských práv třetí osoby. Jestliže se prohlášení poskytovatele v tomto článku ukáže nepravdivým nebo poskytovatel poruší jiné povinnosti podle tohoto článku smlouvy, jde o podstatné porušení této smlouvy a poskytovatel uhradí ve prospěch objednatele smluvní pokutu ve výši 50.000,- Kč za každé jednotlivé porušení povinnosti. Zaplacením smluvní pokuty není nijak dotčeno ani omezeno právo objednatele na náhradu škody, kterou lze vymáhat vedle smluvní pokuty v plné výši. S nositeli chráněných práv duševního vlastnictví vzniklých v souvislosti s realizací služeb dle této smlouvyje poskytovatel povinen vždy smluvně zajistit možnost volného nakládání s těmito právy objednatelem.
7. Udělení veškerých práv uvedených v tomto článku smlouvy nelze ze strany poskytovatele vypovědět a na jejich udělení nemá vliv ukončení této smlouvy.
8. Poskytovatel výslovně prohlašuje, že odměna za veškerá oprávnění poskytnutá objednateli dle tohoto článku smlouvyje již zahrnuta v ceně služeb.
9. Poskytovatel odpovídá za splnění povinností týkající se poskytnutí licencí objednateli dle tohoto článku smlouvy i v případě plnění předmětné části smlouvy prostřednictvím poddodavatele.

## XIII.
## Práva z vadného plnění

1. Služby mají vady, jestliže jejich poskytnutí neodpovídá požadavkům uvedeným v této smlouvě, příslušným právním předpisům, normám nebo jiné dokumentaci vztahující se k jejich poskytování.
2. Za vadu služeb se považuje zejména nezajištění dostupnosti služeb dle přílohy č. 1 této smlouvy ze strany poskytovatele, tj. **99,9 % za měsíc.**
3. Objednatel má právo z vadného plnění z vad poskytnutých služeb. Objednatel má právo z vadného plnění také z vad hmotných výstupů služeb.
4. Není-li v oznámení vady uvedeno jinak, požaduje objednatel bezplatné odstranění vady.
5. Veškeré vady je objednatel povinen uplatnit u poskytovatele bez zbytečného odkladu poté, kdy vadu zjistil, a to formou písemného oznámení (za písemnou formu je považováno i oznámení e-mailem), obsahujícím co nejpodrobnější specifikaci zjištěné vady. Objednatel bude vady díla oznamovat:
    - prostřednictvím rozhraní Service desk využívaného Krajským úřadem Moravskoslezského kraje, ke kterému má objednatel přístup, kdy tento přístup

objednatel pro poskytovatele zajistí

6. Kategorizace vad:

**Vada kategorie A**

- Popis vady: Vážné vady s nejvyšší prioritou, které mají kritický dopad do funkčnosti SOC nebo jeho části a dále vady, které znemožňují činnost SOC nebo jeho části nebo způsobují vážné provozní problémy.

**Vada kategorie B**

- Popis vady: Vada, která svým charakterem nespadá do kategorie A. Znamená vážné vady způsobující zhoršení výkonnosti a funkčnosti SOC nebo jeho části. SOC nebo jeho část má omezení nebo je částečně nefunkční. Jedná se o odstranitelné vady, které způsobují problémy při užívání a provozování SOC nebo jeho části, ale umožňují provoz.

**Vada kategorie C**

- Popis vady: Vada, která svým charakterem nespadá do kategorie A nebo kategorie B. Znamená snadno odstranitelné vady s minimálním dopadem na funkcionality či funkčnost SOC nebo jeho části.

Kategorizaci vad stanovuje při nahlášení vady výhradně objednatel. V případě změny, částečného řešení nebo vyřešení vady objednatel může kategorii vady změnit dle závažnosti jejích dopadů.

7. Nahlášenou vadu služeb je poskytovatel povinen odstranit neprodleně po jejím oznámení ze strany objednatele, a to v následujících lhůtách:

| VADA | RESPONSE TIME<br>REAKČNÍ DOBA, DOBA ODEZVY | REPAIR TIME<br>DOBA ŘEŠENÍ, DOBA ODSTRANĚNÍ VAD, CHYB, INCIDENTŮ DO |
|---|---|---|
| A (kritická) | 1 hodina | 2 hodiny |
| B (závažná) | 1 hodina | 8 hodin |
| C (běžná) | následující den | 3 dny |

## XIV.
## Odpovědnost za škodu

1. Poskytovatel je povinen uhradit objednateli (ZZS MSK) škodu, která mu vznikla vadným plněním (tj. vadným poskytováním služeb), a to v plné výši. Poskytovatel rovněž objednateli uhradí náklady vzniklé při uplatňování práv z vadného plnění.

2. Poskytovatel prohlašuje, že po celou dobu plnění svého závazku z této smlouvy bude mít sjednáno pojištění odpovědnosti za škodu způsobenou třetím osobám vyplývající z dodávaného předmětu plnění s limitním plněním na jednu pojistnou událost minimálně 15 mil. Kč, s maximální výši spoluúčasti 50 tis. Kč.

3. V případě, že při činnosti prováděné poskytovatelem dojde ke způsobení prokazatelné škody objednateli, ZZS MSK nebo třetím osobám, která nebude kryta pojištěním sjednaným ve smyslu odstavce 2 tohoto článku, bude poskytovatel povinen tyto škody uhradit zvláštních prostředků.

4. Poskytovatel předložil před podpisem této smlouvy kopie pojistných smluv na požadované pojištění dle odst. 2 tohoto článku smlouvy včetně všech dodatků nebo certifikáty příslušných pojišťoven prokazující existenci pojištění dle této smlouvy (dobu trvání pojištění, jeho rozsah, pojištěná rizika, pojistné částky, roční limity a sublimity plnění a výši spoluúčasti). Certifikát dle předchozí věty nesmí být starší 1 měsíce. Poskytovatel je dále povinen předložit, po celou dobu plnění této smlouvy, do 5 pracovních dnů od vyžádání objednatelem, kopie pojistných smluv či certifikát prokazující existenci pojištění dle tohoto odstavce, a to i opakovaně.

## XV.
## Úprava vztahů související s bezpečností a zpracováním osobních údajů

1. Není-li stanoveno touto smlouvou výslovně jinak, je ustanoveními tohoto článku smlouvy a dále přílohou č. 3a této smlouvy (Směrnice ZZS MSK, která je chráněná dle NDA) a přílohou č. 3b této smlouvy (Bezpečnostní politiky místních nesdílených aplikací, která je chráněná dle NDA) mezi smluvními stranami upravena zejména bezpečnost informací, ochrana a zpracování osobních údajů a bezpečnostní procesy a postupy objednatele, které souvisejí s plněním této smlouvy. Přílohy č. 3a a 3b této smlouvy jsou závazné ve vztahu kZZS MSK do okamžiku, než bude implementována nová bezpečnostní politika v rámci plnění poskytovatele.

2. Poskytovatel je zejména povinen:

   a) Zajistit seznámení všech pracovníků (vlastních zaměstnanců i poddodavatelů), kteří se budou podílet na plnění služeb (ať už osobně v místě plnění nebo vzdáleným přístupem) s pravidly a postupy bezpečnosti informací MSDC a ZZS MSK a s pravidly pro vzdálený přístup. Toto seznámení bude provedeno bezprostředně po nabytí účinnosti této smlouvy, a to formou vstupního školení, které provede zaměstnanec objednatele a poskytovatel je povinen zajistit účast svých pracovníků na tomto školení.

   b) Řídit se při poskytování služeb pokyny objednatele a aktuálními interními pravidly objednatele a ZZS MSK, definovanými zejména v příloze č. 3a a příloze č. 3b této smlouvy, a v oblasti bezpečnosti práce a ochrany zdraví a požární ochrany, k nimž bude poskytovatel proškolen objednatelem bezprostředně po nabytí účinnosti této smlouvy.

c) Zajistit, aby jeho pracovníci (včetně poddodavatelů), kteří budou přítomni v prostorách objednatele či ZZS MSK, dodržovali všechny bezpečnostní předpisy tak, jak s nimi byli seznámeni objednatelem, zejména co se týče fyzických přístupů do zabezpečených prostor MSDC či ZZS MSK.

d) Písemně nahlásit objednateli plánované zásahy (tzv. servisní okna) do systému prostřednictvím dohodnutého komunikačního kanálu dle čl. XI této smlouvy s výjimkou nahlášených vad dle čl. XIII této smlouvy (neplánované, akutní zásahy), a to nejméně 3 pracovní dny předem a provádět je pokud možno mimo frekventované časy, tj. o víkendech a ve dnech pracovního volna v době od půlnoci do 9:00 h, případně v pracovní dny v době od 22:00 h do 05:00 h.

3. Poskytovatel objednateli odpovídá za to, že dokumenty a soubory dat, které mu v poskytování služeb předá:

   a) jsou kopiemi originálů příslušných dokumentů a souborů dat poskytovatele,

   b) neobsahují žádné infiltrační prostředky,

   c) že k nim má práva na jejich šíření, instalaci, konfiguraci a správu, která mu umožňují s nimi nakládat a dále je poskytovat tak, jak je sjednáno v této smlouvě.

4. Objednatel se zavazuje vždy bez zbytečného odkladu informovat poskytovatele o změně interních pravidel bezpečnostní politiky objednatele. Poskytovatel je následně povinen ihned seznámit s touto změnou pracovníky (vlastní zaměstnance i poddodavatele) podílející se na realizaci předmětu této smlouvy.

5. Pro zajištění dostatečné ochrany informačních aktiv, kterými objednatel disponuje, klasifikuje objednatel data do klasifikačních skupin:

   - veřejné, které jsou označeny písmenem "V/W",
   - neveřejné, které jsou označeny písmenem "N",
   - chráněné, které jsou označeny písmenem "CH".

6. Veškeré skutečnosti obchodní, ekonomické a technické povahy související se smluvními stranami, které nejsou běžně dostupné v obchodních kruzích a se kterými se smluvní strany seznámí při realizaci předmětu smlouvy nebo v souvislosti s touto smlouvou, jsou klasifikovány jako neveřejné. V případě, že budou poskytovateli zpřístupněny osobní údaje, jsou pro účely této smlouvy považovány za neveřejné či chráněné informace.

7. Poskytovatel se zavazuje, že neveřejné či chráněné informace jiným subjektům nesdělí, nezpřístupní, nezkopíruje a neumožní jejich zkopírování ani nevyužije pro sebe nebo pro jinou osobu. Zavazuje se zachovat je v přísné tajnosti a sdělit je výlučně těm svým zaměstnancům nebo poddodavatelům, kteří jsou pověřeni plněním smlouvy a za tímto účelem jsou oprávněni se s těmito informacemi v nezbytném rozsahu seznámit. Poskytovatel se zavazuje zabezpečit, aby i tyto osoby považovaly uvedené informace za důvěrné a zachovávaly o nich mlčenlivost.

8. Povinnost plnit ustanovení tohoto článku smlouvy ohledně neveřejných či chráněných informací se nevztahuje na informace, které:
   a) mohou být zveřejněny bez porušení této smlouvy,
   b) byly písemným souhlasem obou smluvních stran zproštěny těchto omezení,
   c) jsou známé nebo byly zveřejněny jinak než následkem porušení povinnosti jedné ze smluvních stran,
   d) příjemce je zná dříve, než je sdělí smluvní strana,
   e) jsou vyžádány soudem, státním zastupitelstvím nebo příslušným správním orgánem na základě zákona, popřípadě, jejichž uveřejnění je stanoveno zákonem,
   f) smluvní strana sdělí osobě vázané zákonnou povinností mlčenlivosti (např. advokátovi nebo daňovému poradci) za účelem uplatňování svých práv.

9. Poskytovatel je povinen zlikvidovat veškeré neveřejné či chráněné informace, které se dověděl v průběhu plnění této smlouvy poté, co bude plnění z této smlouvy ukončeno, ať už splněním anebo jiným způsobem zániku této smlouvy.

10. Poskytovatel je povinen veškeré neveřejné nebo chráněné informace získané v průběhu plnění této smlouvy přenášet přes veřejné přenosové linky zabezpečené šifrováním, přičemž musí být použitý silný šifrovací algoritmus (šifrování AES-256, heslo min. 17 znaků a kombinace znaků ze všech kategorií - velká písmena, malá písmena, číslice a speciální znaky).

11. Poskytovatel je povinen přijmout veškerá potřebná opatření, která jsou nutná k zajištění plnění předmětu této smlouvy a která vyplývají z této smlouvy anebo z interních předpisů a postupů objednatele, se kterými bude poskytovatel seznámen.

12. Poskytovatel je povinen v souladu s touto smlouvou písemně (např. e-mailem) informovat kontaktní osobu objednatele dle přílohy č. 2 této smlouvy o kybernetických bezpečnostních incidentech dle ZoKB souvisejících s plněním této smlouvy, a to neprodleně, nejpozději do konce dne, kdy byl kybernetický bezpečnostní incident zjištěn. O kybernetický bezpečnostní incident se jedná zejména, dojde-li k nefunkčnosti aplikace, která souvisí s dílem, ztrátě dat nebo neoprávněnému přístupu do takové aplikace nebo k datům. Poskytovatel je zároveň povinen ve lhůtě do 48 hodin od zjištění kybernetického bezpečnostního incidentu písemně (např. e-mailem) informovat o způsobu nápravy takovéto incidentu, a není-li možné v dané lhůtě nápravu zajistit, informovat rovněž o nejbližším možném termínu nápravy, který musí být objednatelem odsouhlasen. Stejnou informační povinnost dle tohoto odstavce smlouvy má poskytovatel v případě, kdy dojde při plnění této smlouvy k situaci, která může mít pro objednatele významné dopady, které by mohly být srovnatelné s kybernetickým bezpečnostním incidentem.

13. Povinnost ochrany neveřejných a chráněných informací trvá bez ohledu na ukončení účinnosti této smlouvy. Neveřejné a chráněné informace jsou považovány za důvěrné údaje ve smyslu § 1730 odst. 2 občanského zákoníku. Za důvěrné objednatel označuje rovněž veškeré informace vymezené v NDA uzavřené před podpisem této smlouvy.

14. Poskytovatel bere na vědomí, že v průběhu plnění bude nakládat s neveřejnými informacemi ZZS MSK a bude povinen zajistit ochranu nejen z hlediska důvěrnosti, ale také z hlediska integrity.

15. Smluvní strany prohlašují, že pokud by při plnění této smlouvy mělo docházet ke zpracování osobních údajů ve smyslu zákona č. 110/2019 Sb., o zpracování osobních údajů (dále jen ***„ZoZOÚ")*** a ve smyslu GDPR, kdy by se objednatel měl stát správcem osobních údajů dle čl. 4 odst. 7 GDPR a poskytovatel zpracovatelem osobních údajů dle čl. 4 odst. 8 GDPR, uzavřou strany bezodkladně samostatnou smlouvu o zpracování osobních údajů, ve které upraví práva a povinnosti vyplývající z GDPR a ZoZOÚ.

16. Přihlášení poskytovatele do sítě MSDC musí podléhat kontrole přístupu na základě autorizace po předchozí autentizaci. Poskytovatel se zavazuje, že před připojením koncového zařízení, mobilní koncového zařízení nebo aktivního síťového prvku do počítačové sítě zažádá o schválení připojení kontaktní osobu na straně objednatele.

17. Poskytovatel se zavazuje, že vzdálený přístup do systému bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení VPN.

18. Poskytovatel se zavazuje, že bez zbytečného odkladu deaktivuje všechny nevyužívané zakončení sítě anebo nepoužívané porty aktivního síťového prvku.

19. Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění, které přistupují do interní sítě nebo informačního systému, měly v externím zařízení např. notebook aplikovány bezpečnostní záplaty a nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu.

20. Poskytovatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci poskytovatele nebo poddodavatele.

21. Poskytovatel se zavazuje, že nebude konat v rozporu s bezpečnostními politikami objednatele.

22. Objednatel v rámci řízení změn v systému řízení kybernetické bezpečnosti přezkoumává možné dopady změn a určuje významné změny dle VKB.

23. Poskytovatel 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.

24. Při realizaci penetračního testování nebo testování zranitelnosti řešení poskytne poskytovatel objednateli veškerou potřebnou součinnost dle odst. 5.2. přílohy č. 1 této smlouvy. Poskytovatel je povinen přijmout dodatečná, účinná nápravná opatření k odstranění zranitelností.

25. Objednatel má oprávnění zapojit poskytovatele do řízení kontinuity činností, zejména havarijních plánů, které souvisí se službou SOC.

26. Poskytovatel předloží objednateli metodiku zálohování a obnovy dat, systém evidence a zajištění integrity šifrováním záloh.

27. Poskytovatel bere na vědomí, že veškerý přenos dat a informací musí být dostatečně zabezpečen pomocí aktuálně odolných kryptografických algoritmů a kryptografických klíčů. Pro online webové technologie budou chráněny SSL certifikáty.

28. Pokud není určena kvalifikace informace, bude použit způsob likvidace pro důležitost aktiva kritickou. Přípustný způsob likvidace nosičů informace dle úrovně důležitosti aktiva je definován v příloze č. 5 VKB. O likvidaci dat bude proveden záznam.

## XVI.
## Sankce

1. V případě, že poskytovatel neprovede služby spočívající v implementaci ISMS a dokončení adaptační fáze SOC včas, je povinen zaplatit objednateli smluvní pokutu ve výši 0,2 % z ceny za poskytování příslušné části služeb bez DPH dle čl. VI odst. 1 této smlouvy, a to za každý započatý den prodlení.

2. Pokud budou mít poskytované služby vadu spočívající v nezajištění dostupnosti služeb v 99,9 % za měsíc poskytování služeb ze strany poskytovatele, dle čl. XIII odst. 2 a přílohy č. 1 této smlouvy, je poskytovatel povinen uhradit objednateli smluvní pokutu ve výši 750 Kč, za každou započatou hodinu, která překročí 0,1 % z časové nedostupnosti služeb.

3. Pokud poskytovatel neprovede vůči objednateli notifikace dle závažnosti a ve lhůtách dle přílohy č. 1 této smlouvy, je povinen objednateli uhradit smluvní pokutu za každou započatou hodinu porušení této povinnosti ve výši 750 Kč. Smluvní pokuta dle tohoto odstavce smlouvy nepřesáhne cenu za poskytování služeb provozní fáze SOC za 3 měsíce dle čl. VI odst. 1 této smlouvy.

4. V případě nedodržení lhůt pro odezvu a/nebo odstranění vad dle odst. XIII.7 této smlouvy, je poskytovatel povinen uhradit objednateli následující smluvní pokuty:
    - nedodržení lhůty odezvy u vady kategorie A: 1.000,- Kč za každých i započatých 60 minut prodlení a jednotlivou vadu;
    - nedodržení lhůty odezvy u vady kategorie B: 500,- Kč za každých i započatých 60 minut prodlení a jednotlivou vadu;
    - nedodržení lhůty odezvy u vady kategorie C: 1.000,- Kč za každý i započatý den prodlení a jednotlivou vadu;
    - nedodržení lhůty řešení u vady kategorie A: 1.000,- Kč za každých i započatých 60 minut prodlení a jednotlivou vadu;
    - nedodržení lhůty řešení u vady kategorie B: 1.000,- Kč za každých i započatých 60 minut prodlení a jednotlivou vadu;
    - nedodržení lhůty řešení u vady kategorie C: 500,- Kč za každý i započatý den prodlení a jednotlivou vadu.

5. V případě porušení jakékoliv povinnosti poskytovatele uvedené v čl. XV této smlouvy je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 10.000 Kč za každý jednotlivý případ takového porušení, není-li v NDA sjednáno pro konkrétní případ jinak.

6. V případě nesplnění povinnosti dle čl. X odst. 1, 2, 4, 5 a 6 této smlouvy je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 25.000 Kč, a to za každý jednotlivý případ takového porušení a i každý započatý den prodlení s oznámením příslušné změny.
7. Nezúčastní-li se poskytovatel jednání týkajícího se předmětu smlouvy na základě pozvánky objednatele dle čl. IX odst. 4 nebo 5 této smlouvy bez dřívějšího písemného souhlasu objednatele s absencí poskytovatele, je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 2.000 Kč za každý jednotlivý takto zmařený průběh jednání týkajícího se předmětu smlouvy na základě pozvánky.
8. V případě nepředá-li či nedoručí-li poskytovatel zápis o průběhu a závěrech jednání týkajícího se předmětu smlouvy dle čl. IX odst. 6 této smlouvy objednateli ani do pěti pracovních dní ode dne konání jednání, je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 2.000 Kč, a to za každý i započatý den prodlení s předáním či doručením každého takovéhoto zápisu.
9. V případě porušení povinnosti dle čl. XIV odst. 2 této smlouvy, tj. povinnosti mít po celou dobu platnosti této smlouvy sjednanou pojistnou smlouvu pro případ způsobení škody třetí osobě, je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 30.000 Kč za každý i započatý měsíc, v němž nebude mít sjednanou pojistnou smlouvu dle čl. XIV odst. 2 této smlouvy.
10. Smluvní pokuta a úrok z prodlení jsou splatné do 30 dní ode dne doručení písemného vyúčtování příslušné výše povinné straně.
11. Zaplacením jakékoli smluvní pokuty není dotčen nárok objednatele na náhradu škody, objednatel má nárok na náhradu škody vedle smluvní pokuty v plné výši. Zaplacením smluvní pokuty není dotčena povinnost splnění povinnosti, která je prostřednictvím smluvní pokuty zajištěna.

## XVII.
## Zánik smlouvy

1. Smluvní strany se dohodly, že smlouva zaniká:
   a) Písemnou výpovědí kterékoliv smluvní strany s **výpovědní dobou 6 měsíců,** která započne běžet od prvního dne měsíce následujícího po doručení výpovědi. Poskytovatel je oprávněn vypovědět smlouvu nejdříve po uplynutí tří let a 6 měsíců poskytování služeb provozní fáze.
   b) Dohodou smluvních stran.
   c) Jednostranným odstoupením od smlouvy pro její podstatné porušení druhou smluvní stranou, přičemž podstatným porušením smlouvy se rozumí zejména:
      - Neposkytnutím služeb v termínu plnění dle čl. V odst. 3 této smlouvy prodlouženém o 10 dní,
      - opakované (nejméně dvakrát) nedodržení pokynů objednatele, právních předpisů nebo technických norem, které se týkají poskytování služeb,

- opakované (nejméně dvakrát) nedodržení smluvních ujednání o právech z vadného plnění,
- opakovaná (nejméně dvakrát) neúčast poskytovatele na úvodní informační schůzce dle čl. IX odst. 4 této smlouvy,
- porušení povinností poskytovatele dle čl. X odst. 1 nebo 2 této smlouvy,
- neshoda smluvních stran na hmotných výstupech adaptační fáze, zejména prováděcí (implementační) projekt,
- neuhrazení ceny za služby objednatelem po druhé výzvě poskytovatele k uhrazení dlužné částky, přičemž druhá výzva nesmí následovat dříve než 30 dnů po doručení první výzvy,
- opakované (nejméně dvakrát) nedodržení smluvních ujednání o nutné součinnosti objednatele.

2. Objednatel je dále oprávněn od této smlouvy odstoupit v těchto případech:
   - bylo-li příslušným soudem rozhodnuto o tom, že poskytovatel je v úpadku ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů (a to bez ohledu na právní moc tohoto rozhodnutí);
   - podá-li poskytovatel sám na sebe insolvenční návrh,
   - dojde k významné změně kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými Poskytovatelem k plnění dle této smlouvy ve smyslu písm. n) přílohy č. 7 VKB
3. Pro účely této smlouvy se pod pojmem „bez zbytečného odkladu" dle § 2002 občanského zákoníku rozumí „nejpozději do 3 týdnů".
4. Odstoupením či výpovědí této smlouvy nezaniká nárok oprávněné strany na zaplacení smluvních pokut a náhradu škody.
5. V případě jakéhokoliv ukončení smlouvy se poskytovatel zavazuje splnit tyto povinnosti:
   - poskytnutí požadovaných součinností v souvislosti s předáním podpory a poskytování služeb novému poskytovateli nebo objednateli, a to v souladu s exit plánem vytvořeným v rámci prováděcího (implementačního) projektu (náklady na vytvoření exit plánu a poskytování součinnosti při exitu jsou součástí ceny plnění),
   - poskytnutí informací nezbytných k převzetí systému novým poskytovatelem nebo objednatelem,
   - poskytnutí veškeré relevantní dokumentace v aktuálním stavu, která byla vytvořena v rámci plnění předmětu této smlouvy,

   O řádné splnění povinností poskytovatele dle tohoto odstavce bude sepsán akceptační protokol, který bude podepsán oběma smluvními stranami a bude přiložen k závěrečné faktuře.

## XVIII.
## Závěrečná ustanovení

1. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem, uveřejnění smlouvy 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"").***
2. Smluvní strany se dohodly, že objednatel provede uveřejnění této smlouvy v souladu se zákonem o registru smluv.
3. Doplňování nebo změnu této smlouvy lze provádět jen se souhlasem obou smluvních stran, a to pouze formou písemných, vzestupně číslovaných a takto označených dodatků.
4. Poskytovatel nemůže bez souhlasu objednatele postoupit svá práva a povinnosti plynoucí z této smlouvy třetí straně.
5. Tato smlouvaje podepsána elektronickým podpisem zástupců smluvních stran.
6. Osobní údaje obsažené v této smlouvě budou MSDC zpracovávány pouze pro účely plnění práv a povinností vyplývajících z této smlouvy; k jiným účelům nebudou tyto osobní údaje MSDC použity. Podrobné informace o ochraně osobních údajů jsou uvedeny na oficiálních webových stránkách MSDC https://www.msdc.cz/gdpr/.
7. Nedílnou součástí této smlouvy jsou následující přílohy:

   *Příloha č. 1: Technická specifikace (důvěrná příloha v rozsahu dle NDA)*

   *Příloha č. 2: Zástupci smluvních stran a realizační tým*

   *Příloha č. 3a: Směrnice ZZS MSK: Používání informačních a komunikačních technologií (důvěrná příloha)*

   *Příloha č. 3b: Bezpečnostní politika místních nesdílených aplikací (důvěrná příloha)*

   *Příloha č. 4: Pravidla auditu*

   *Příloha č. 5: Nabídka poskytovatele (technický popis nabízeného řešení)*

| V Ostravě dne | V Brně dne |
|---|---|
| [redacted] | |
| **centrum, p.o.**<br>Ing. RNDr. Alois Slovák, ředitel organizace | Pavel Kocour, předseda představenstva vedoucího společníka |

# II. TECHNICKÁ SPECIFIKACE VEŘEJNÉ ZAKÁZKY

## *Začlenění organizace Zdravotnická záchranná služba Moravskoslezského kraje do jednotného krajského řešení kybernetické bezpečnosti*

## OBSAH


1. Popis výchozího stavu....4
2. Cíle veřejné zakázky.... 4
3. Kompetenční a odpovědnostní model.... 5
3.1. Subjekty.... 7
3.2. Zastoupené personální role v jednotlivých subjektech při řešení aktivní kybernetické bezpečnosti....7
3.2.1 Centrum kybernetické bezpečnosti - SOC.... 7
3.2.2 Moravskoslezské datové centrum, p. o.... 10
3.2.3 Zdravotnická záchranná služba Moravskoslezského kraje, p.o....13
3.3. Krajský úřad.... 14
4. Organizační model.... 15
5. Provozní/procesní model....18
5.1. Procesní část modelu ....19
5.2. Prevence a predikce kybernetických hrozeb.... 21
5.3. Provozní část modelu pro řízení kybernetických bezpečnostních incidentů 21
5.3.1 Typy kybernetických bezpečnostních incidentů.... 21
5.3.2 Kategorizace kybernetických bezpečnostních incidentů....22
5.3.3 Fáze analýzy, rozhodnutí a zvládání.... 22
5.3.4 Dokumentace kybernetického bezpečnostního incidentu ....23
5.4. Stavy kybernetického bezpečnostního incidentu.... 23
6. Předmět plnění veřejné zakázky....24
6.1. Služby ISMS.... 25
6.2. Poskytování služeb SOC ....27
6.2.1 Adaptační fáze.... 27
6.2.2 Provozní fáze.... 28
7. Detailní specifikace zadání - definice požadovaných parametrů.... 28
7.1. ISMS - detailní požadavky....29
7.2. Služby centra kybernetické bezpečnosti - detailní požadavky....31
8. Přílohy.... 50
Příloha č. 1 - Přehled infrastrukturních a aplikačních prvků/systémů.... 50

**Příloha č. 2 - Dokumentace IT systémů a sítí ZZ..... 51**
**Příloha č. 3 - Rozsah penetračního testování (1. sada penetračních testů)..... 51**

# Seznam zkratek

| Zkratka | Význam zkratky |
|---|---|
| ACL | *Access Control List, doslova seznam pro řízení přístupu* |
| APT | *Advanced Persistent Threat, pokročilé trvalé hrozby* |
| CSIRT | *Computer Security Incident Response Team - „Skupina pro reakci na bezpečnostní události “* |
| DB | *Databáze* |
| GDPR | *Právní rámec ochrany osobních údajů v evropském prostoru* |
| HW | *Hardware* |
| http | *Hypertext Transfer Protocol - protokol umožňující komunikaci* |
| https | *Hypertext Transfer Protocol Secure - protokol umožňující zabezpečenou komunikaci* |
| ICT | *Informační a komunikační technologie* |
| IDM | *Identity management* |
| Incident | *Taková událost vyhodnocená SOC, na kterou je potřeba neprodleně reagovat* |
| IPAM | *IP address management* |
| IPS/IDS | *Intrusion Prevention/Detection System - obranný systém, který monitoruje síťový provoz a snaží se odhalit podezřelé aktivity* |
| IS | *Informační systémy* |
| ISMS | *Information Security Management System - Systém řízení bezpečnosti informací* |
| ISZS | *Informační systém základní služby* |
| IT | *Informační technologie* |
| IT/OT | *Konvergované prostředí IT technologií a provozovaných zdravotnických prostředků* |
| KB | *Kybernetická bezpečnost* |
| Kil, KI | *Kritická informační infrastruktura, Kritická infrastruktura* |
| KS | *Komunikační systém* |
| LAN | *Local Area Network, Lokální síť* |
| MSDC | *Moravskoslezské datové centrum p. o.* |
| NDA | *Non-Disclosure Agreement, dohoda o mlčenlivosti* |
| NÚKIB | *Ústřední správní orgán pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany ve věcech kybernetické bezpečnosti* |
| PIN | *Personál Identification Number, identifikační číslo* |
| RDP | *Remote Desktop Protocol, proprietární síťový protokol, který umožňuje uživateli využívat (ovládat) vzdálený počítač* |
| SIEM | *Security Information and Event Management, management bezpečnostních informací a událostí* |
| SLA | *Service Level Agreement, úroveň poskytovaných služeb* |
| Snmp | *Simple Network Management Protocol - protokol využívaný pro management sítí* |

| | |
|---|---|
| SOC | *Security operation center - centrum kybernetické bezpečnosti* |
| SSH | *Secure Shell, protokol pro šifrovanou komunikaci* |
| SSL VPN | *Secure Sockets Layer Virtual Private Network, bezpečnostní technologie používaná pro šifrování síťové komunikace* |
| SW | *Software* |
| TCK KÚ MSK | *Krajské Technologické Centrum Moravskoslezského kraje* |
| TO | *Technické opatření* |
| URL | *Uniform Resource Locator, webová adresa* |
| VIS | *Významný informační systém* |
| VLÁN | *Virtuální LAN - jedna logická síť* |
| VNC | *Virtual Network Computing, grafický program, který umožňuje vzdálené připojení ke grafickému uživatelskému rozhraní* |
| VPN | *Virtual private network, virtuální privátní síť* |
| VŘ | *Výběrové řízení* |
| VZ | *Veřejná zakázka* |
| WiFi | *Označení pro několik standardů IEEE 802.11 popisujících bezdrátovou komunikaci* |
| WMI | *Windows Management Instrumentation* |
| ZoKB | *Zákon o kybernetické bezpečnosti* |
| ZZ | *zdravotnické zařízení* |

# Vymezení pojmů

| Pojem | pod pojmem se rozumí |
|---|---|
| **zdravotnické zařízení** | *Zdravotnická záchranná služba MSK, p. o.* |
| **organizace** | *Zřízená nebo založená registrovaná organizace sloužící jako prostředek k dosažení definovaných cílů s jasnou strukturou a řídící hierarchií. Pokud z kontextu nevyplývá, že se jedná o „organizaci“, kterou se také označuje vlastní činnost (tj. organizování).* |
| **řízená organizace** | *Jedná se o organizace, které jsou, nebo mohou být v oblasti kybernetické bezpečnosti řízeny z korporátní úrovně Krajského úřadu Moravskoslezského kraje. Jedná se o všechny organizace zřízené nebo založené MSK* |
| **zapojené subjekty** | *Moravskoslezské datové centrum p. o. a Nemocnice Havířov, p. o., Nemocnice Karviná-Ráj, p. o., Sdružené zdravotnické zařízení Krnov, p. o., Nemocnice Třinec p. o., Slezská nemocnice v Opavě, p. o., Nemocnice ve Frýdku-Místku p. o. a Bílovecká nemocnice, a.s., Zdravotnická záchranná služba MSK* |

# 1. Popis výchozího stavu

Současný stav ZZ je popsán v přílohách (kapitola 8) této technické specifikace:
Příloha č. 1 - Přehled infrastrukturních a aplikačních prvků/systémů
Příloha č. 2 - Dokumentace IT systémů a sítí ZZ

# 2. Cíle veřejné zakázky

Cíle veřejné zakázky jsou sledovány v těchto oblastech:

**a)** V oblasti ISMS jsou sledovány tyto cíle:

- Ustanovení a zavedení bezpečnostních zásad prostřednictvím ISMS v reflexi na dané modely popsané touto zadávací dokumentaci do praxe ZZ, kdy bude dosaženo:
  - zajištění přiměřené a dostatečné ochrany důvěrnosti, dostupnosti a integrity aktiv,
  - vytvoření takového bezpečnostního povědomí, aby se bezpečnost stala neoddělitelnou součástí každodenního chodu ZZ,
  - stanovení a prosazování odpovědnosti za řízení, naplňování a dodržování bezpečnostních zásad a opatření v modelu organizací s přesně vymezenou odpovědností,
  - zavedení v souladu s relevantní legislativou.

- Monitorování a přezkoumání:
  - účinnosti ISMS v rámci provozní fáze,
  - udržení v souladu s relevantní legislativou.

**b)** V oblasti poskytování služeb centra kybernetické bezpečnosti (SOC) jsou sledovány tyto cíle:

- Komplexní zajištění aktivní kybernetické bezpečnosti jako výstupu poskytovaných služeb SOC s pomocí provozovaných nástrojů pro vyhodnocování kybernetických bezpečnostních událostí, provozních událostí ve výpočetních systémech a v komunikačních sítích u ZZ.
- Udržováni kybernetické bezpečnosti minimálně na takovém stupni, který umožní snížit identifikovaná rizika na akceptovatelnou úroveň.

# 3. Kompetenční a odpovědnostní model

Vztahy v tomto modelu je nutno chápat jako komplikované, jelikož je nutno realizovat aktivní kybernetickou bezpečnost formou spolupráce, dodávkou služeb a činností se zapojením více subjektů dle dále uvedené specifikace.

Kompetenční a odpovědnostní model předpokládá existenci jednotlivých rolí pro systém řízení bezpečnosti informací. **Zde jsou popsány pouze role, které mají v jednotlivých modelech specifické vztahy v rámci organizace kybernetické bezpečnosti vykonávané jednotlivými subjekty.** Činnosti těchto rolí jsou organizovány v rámci kompetenčního modelu.

Jednotlivé role jsou buď zajišťovány vlastními zaměstnanci zapojených subjektů, nebo jsou zajišťovány formou služeb, které jsou předmětem této veřejné zakázky. Nedílnou součástí je Organizační model, ve kterém je popsána činnost kolektivních orgánů. Zde jsou popsány nezastupitelné specifické funkce jednotlivých rolí.

Oporou tohoto kompetenčního a odpovědnostního modelu je řídící dokumentace zahrnující principy, pravidla a požadavky plynoucí ze systému řízení bezpečnosti informací. Tato dokumentace je vydávána formou politik, metodik, příruček, směrnic nebo jiných řídících aktů. *(pozn: tato část je předmětem veřejné zakázky v části implementace ISMS v reflexi na popisované modely)*

Grafické vyjádření komunikačních vztahů v modelu je schématický znázorněno:

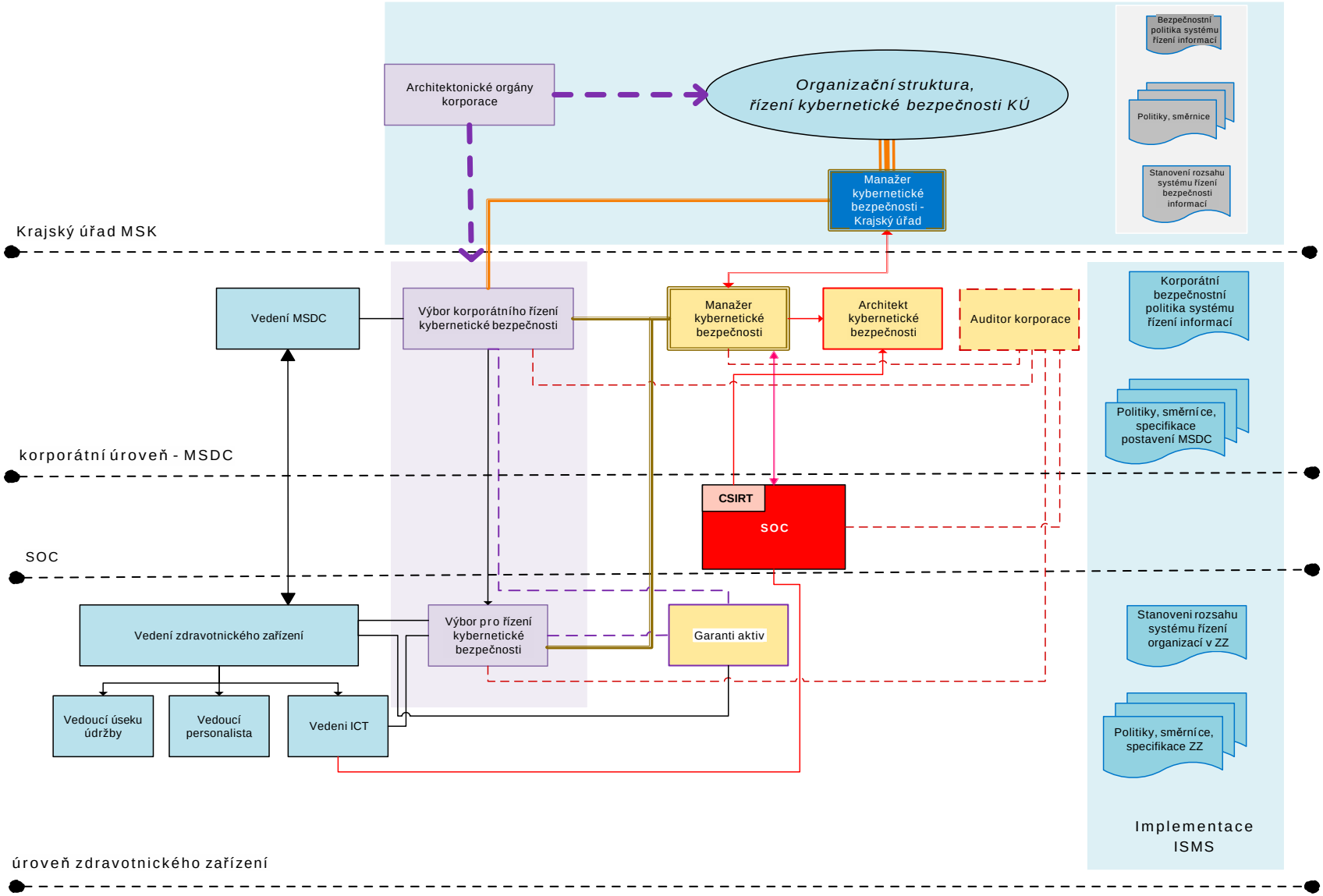


Schéma č. 1 Grafické vyjádření komunikačních vztahů v rámci modelů

## 3.1. Subjekty

Zastoupení subjektů v kompetenčním modelu aktivní kybernetické bezpečnosti a definice jejich specifických postavení v rámci předmětu veřejné zakázky.

| | |
|---|---|
| Zdravotnická záchranná služba MSK - | je spolupracující uživatel poskytovaných služeb. V definovaném rozsahu a hranicích ochrany je realizována aktivní kybernetická bezpečnost. Je anebo bude povinnou osobou[1]. Statutární orgán nese plnou zodpovědnost za oblast KB. |
| Moravskoslezské datové centrum, p. o. - | vykonává a odpovídá za realizaci modelu technických a organizačních opatření na základě výstupů z poskytovaných služeb SOC dodavatele. Organizace zajišťující činnosti plynoucí z náplní práce **manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti a auditora kybernetické bezpečnosti** definovaných v platné a účinné legislativně (obsazení těchto rolí tedy není předmětem plnění veřejné zakázky). |
| SOC *(Security Operations Center)* - | předmět plnění poskytovaných služeb dle této veřejné zakázky. |

## 3.2. Zastoupené personální role v jednotlivých subjektech při řešení aktivní kybernetické bezpečnosti

### 3.2.1 Centrum kybernetické bezpečnosti - SOC

Centrum kybernetické bezpečnosti provozuje nástroje pro sběr a analýzu informací (např. systémy SIEM, provozní monitoring, log-management, Netflow management, Vulnerability management apod.). Minimální množinou bezpečnostních logů je na úrovni subjektu perimetrovýfirewall, webový firewall, loadbalancer, centrální konzole ochrany koncových bodů, agenti na klíčových Windows serverech a technické prostředky (sondy) umístěné v páteři LAN vZZ. Pokud je ZZ příslušnou technologií vybaveno je možno při řešení využít současně provozovaných technologií. Zadavatel

[1] Zadavatel požaduje, aby k ZZ v rámci plnění veřejné zakázky bylo přistupováno, jako k povinné osobě v oblasti kybernetické bezpečnosti, a to i pokud tyto povinnosti plynoucí z platné a účinné legislativy prozatím nemá Národním úřadem pro kybernetickou a informační bezpečnost stanovené.

předpokládá, že sondy pro sběr vstupních informací budou umístěny v technologickém prostředí ZZ, pro které jsou poskytovány služby aktivní kybernetické bezpečnosti, případně bude využito stávajících provozovaných nástrojů.

Z pohledu garance funkčnosti využití současně provozovaných technologií bude zadavatelem zprostředkována sekundárně, na základě potřeb plynoucích z provozu jednotlivých technologických prvků ZZ. To například znamená, že pokud se firewall dostane do provozního stavu *"porucha",* bude především zájmem zadavatele (provozovatele) tuto závadu na tomto technologickém prvku odstranit. Tedy takto bude zprostředkovaně garantována funkčnost bez vlivu na SLA směrem k dodavateli. Pokud se bude jednat o provoz a využití technologických prvků a nástrojů plnící specifické funkce využívané "pouze" pro potřeby SOC, tak v tomto případě garance musí nést dodavatel v rámci plnění SLA dodávaných služeb.

SOC centralizuje aktivní činnosti, správu události a incidentů, koordinuje analýzu anomálií a řízení krizových úkonů při zvládání následků incidentů. Z hlediska provozních procesů SOC **monitoruje a vyhodnocuje bezpečnostní incidenty při provozu vybraných systémů** (především základní služba v oblasti zdravotnictví a informační systémy základní služby (dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů; dále jen „zákon 181/2014 Sb.“ nebo „ZoKB“), kritická infrastruktura, systémy bezpečnostního a provozního dohledu, systémy zařazené do režimu vyšší dostupnosti a související technologie jako je prostředí sítě, ochrany perimetru a síťových aktiv připojených do sítě a v případě jejich výpadku nebo nestandardních stavů aktivuje příslušný eskalační proces pro řešení incidentu.

Základním principem je poskytování služeb SOC formou aktivní kybernetické bezpečnosti. Uvedeným se rozumí **aktivní reakce na bezpečnostní incident** bezprostředním opatřením snižující stupeň klasifikace incidentu. **Před vlastním aktivním zásahem je vyžadován buď souhlas od příslušné role, a to systémového administrátora IT dotčeného zdravotnického zařízení, nebo v případě incidentů nesoucí vysoké riziko dopadu, realizace aktivního zásahu a současné kontaktování IT administrátora dotčeného zdravotnického zařízení.** Je požadováno, aby v rámci implementace ISMS byl stanoven postup (kategorizace) pro řešení aktivního zásahu ve vztahu k jednotlivým aktivům. V rámci poskytnuté součinnosti bude administrátor zdravotnického zařízení dosažitelný v režimu 24x7.

**V rámci SOC jsou zastoupeny tyto role s následujícími kompetencemi a příslušnou zodpovědností:**

**<u>Operátor SOC:</u>**

Je pracovní pozice, která je odpovědná za přijímání hlášení o kybernetických bezpečnostních událostech a incidentech od uživatelů, třetích stran a dalších osob a jejich zavedení do systému pro vyhodnocení kybernetických bezpečnostních událostí a incidentů, který je provozován u dodavatele služeb SOC. Mezi jeho odpovědnosti a příslušné kompetence v rámci procesu patří zejména následující:

- zpracování prvotního hlášení o kybernetických bezpečnostních incidentech,
- postoupení řešení běžných kybernetických bezpečnostních incidentů odpovědným osobám a je-li to žádoucí, provedení nezbytných opatření vedoucích k jejich řešení nebo alespoň zastavení šíření.

**Analytik kybernetické bezpečnosti**

Je pracovní pozice, která je odpovědná za zpracování informací o kybernetických bezpečnostních událostech a incidentech z nástrojů pro detekci, jejich vyhodnocení a zavedení do systému pro vyhodnocení kybernetických bezpečnostních událostí a incidentů. Mezi jeho odpovědnosti a příslušné kompetence v rámci procesu patří zejména následující:

- obsluha a administrace nástroje pro detekci kybernetických bezpečnostních událostí a vyhodnocování jeho výstupů,
- obsluha a administrace nástroje pro vyhodnocení kybernetických bezpečnostních událostí (SIEM),
- informování manažera kybernetické bezpečnosti o rozsahu činností, na které může mít kybernetický bezpečnostní událost dopad,
- vyhodnocení závažnosti kybernetických bezpečnostních události (méně významné, významné a velmi významné události, či incidenty),
- informování manažera kybernetické bezpečnosti o závažné kybernetické bezpečnostní události, či incidentu,
- postoupení řešení odpovědným osobám a je-li to žádoucí, provede také nezbytná opatření vedoucí k řešení (či alespoň snížení stupně klasifikace bezpečnostního incidentu).

**Forenzní analytik**

Je pracovní pozice, která úzce spolupracuje s analytiky. Je odpovědná za zpracování informací o kybernetických bezpečnostních událostech a incidentech s využitím specializovaných metod analýzy dat a technik pro získávání důkazů souvisejících s případnou trestní činností. Mezi jeho odpovědnosti a příslušné kompetence v rámci procesu patří zejména následující:

- obsluha a administrace nástrojů nejpokročilejších technologických řešení pro načítání, prohledávání, analýzy a vizualizaci velkých a složitých datových souborů,
- shromažďování relevantních informací, které jsou nezbytné při řešení případných soudních sporů, vyšetřování a řešení regulatorních otázek, finanční a jiné trestné činnosti,
- využití techniky ke shromažďování a uchovávání důkazního materiálu, zajištění důvěryhodnosti získaných údajů z konkrétního výpočetního celku a to způsobem, který je vhodný pro následné právní úkony,
- identifikace dalších systémů zforenzního pohledu, které mohou být s jistou pravděpodobnosti ohroženy kybernetickými útoky,
- poskytování znaleckého svědectví v soudním řízení,
- postoupení informací a řešení odpovědným osobám.

**Bezpečnostní expert**

Je pracovní pozice, která je zodpovědná za zpracování bezprostředního incidentu v rámci řešení aktivních bezpečnostních opatření k zamezení kybernetického útoku **ve specifických oblastech vztažených ke konkrétním systémům.** V rámci aktivitní správy dílčích systémů disponuje příslušnou znalostní úrovni **a vlastní příslušné platné certifikace výrobců spravovaných technologií.** Expert úzce spolupracuje s analytikem a forenzním analytikem. Mezi jeho odpovědnosti a příslušné kompetence v rámci procesu patří zejména následující:

- administrace a konfigurace specifických technologií v rámci zásahů při aktivním řešení incidentů v rámci kybernetické bezpečnosti (rozsah bude upřesněn v Prováděcím projektu ve vztahu k jednotlivému zdravotnickému zařízení),
- spolupráce s analytikem v úzce specializovaných oblastech vztažených k technologiím jednotlivých výrobců,

- pokud je to vzhledem k závažnosti incidentu žádoucí, pak realizuje nezbytná opatření vedoucí k řešení (či alespoň snížení stupně klasifikace bezpečnostního incidentu),
- postoupení dalšího, následného řešení incidentu odpovědným osobám na straně zdravotnického zařízení.

V těchto pracovních pozicích zastoupeni Bezpečnostní experti min. pro tyto oblasti:

- síťové prvky včetně Firewallu,
- operační systémy
- databáze
- serverová infrastruktura včetně virtualizační platformy
- SIEM a Log Management

**Bezpečnostní specialista na hardening**

Je pracovní pozice, která úzce spolupracuje s experty, analytiky a auditorem. Je odpovědná za nastavení procesů řízení zranitelnosti, hardening a kontroly souladu (compliance).

Mezi jeho odpovědnosti a příslušné kompetence v rámci procesu patří zejména následující:

- vytváření a aktualizace hardeningových bezpečnostních politik,
- stanovení strategií postupů k přístupu a stanovení priorit, okamžitých oprav a oprav vedoucích k posílení zabezpečení a ochrany systémů v oblasti software, firmware, BIOS (serverů, sítí a jejich prvků, aplikací, databází, operačních systémů a nepotřebných účtů a oprávnění),
- odpovědnost za řízení procesu zabezpečení konfigurace systémů vedoucí k omezení výskytu zranitelnosti,
- odpovědnost za návrhy hardeningu zabezpečení a ochrany systémů,
- odpovědnost za hardening aplikací s kontrolou vzájemných integrací s jinými aplikacemi a systémy s odstraněním nebo omezením nepotřebných integračních komponent a oprávnění.

### 3.2.2 Moravskoslezské datové centrum, p. o.

Moravskoslezské datové centrum v procesu aktivní kybernetické bezpečnosti plní role odpovídající činnostem **manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti a auditora kybernetické bezpečnosti** definovaných legislativně.

Pro implementaci ISMS představuje organizace v systému prvek řešící korporátní úroveň systému řízení bezpečnosti informací. Současně poskytuje služby těchto rolí řízeným organizacím. Je v této oblasti řídící složkou pro ostatní příspěvkové organizace v roli povinných osob, které spadají pod dikci zákona a vyhlášky o KB.

**Konkrétně pak MSDC zodpovídá za:**

- definici strategie řízení kybernetické bezpečnosti korporace, řízení systému managementu informační bezpečnosti a plní vyjmenované specifické role uvedené v dále popisovaných modelech,
- návrh a kontrolu opatření,
- řízení a kontrolu IT procesů z hlediska kybernetické bezpečnosti,
- koordinaci činností.

**V rámci MSDC jsou zastoupeny role, které jsou do ZZ outsourcovány. Jedná se o role s následujícími kompetencemi a příslušnou zodpovědností:**

**Manažer kybernetické bezpečnosti**

Manažer kybernetické bezpečnosti MSDC (dále také „manažer KB“) je osoba odpovědná za systém řízení bezpečnosti informací (ISMS). Z hlediska ISMS je pro ZZ osobou, která je pro tuto činnost vyškolena a má předepsanou způsobilost. Manažer KB je hlavním řídícím a výkonným prvkem, který aplikuje kybernetickou bezpečnost v intencích strategického směrování určeného Výborem korporátního řízení kybernetické bezpečnosti, resp. Výborem pro řízení kybernetické bezpečnosti na úrovni ZZ. Manažer KB zajišťuje a odpovídá za to, že všechny aktivity související s informačními technologiemi jsou prováděny v souladu s korporátní bezpečnostní politikou a z ní vycházejícími interními předpisy, dále zajišťuje přípravu a schválení těchto předpisů, identifikuje významné změny v rizicích, zajišťuje podporu vzdělávání a bezpečnostního povědomí a zajišťuje vyřešení zjištění identifikovaných v rámci auditů a kontrol. Manažer KB udržuje seznam aktiv a garantů aktiv a seznam pracovníků a jim přidělených bezpečnostních rolí, má výkonnou pravomoc v rámci schválených předpisů a pracovních postupů vůči všem dotčeným pracovníkům.

Manažer KB vykonává zejména tyto činnosti:

- koordinaci činností v oblasti kybernetické bezpečnosti,
- iniciování, sledování a vyhodnocování implementace opatření kybernetické bezpečnosti,
- informování Výboru korporátního řízení kybernetické bezpečnosti, odboru zdravotnictví KÚ, vedení ZZ a vedení oddělení informatiky o aktuálním stavu systému řízení bezpečnosti informací,
- koordinaci tvorby bezpečnostního konceptu řízených ZZ, na základě přijaté strategie kybernetické bezpečnosti korporace, konceptu plánu obnovy a ostatních dílčích konceptů a systémových bezpečnostních pravidel, jakož i vydávání doplňujících pravidel a vodítek celkové kybernetické bezpečnosti,
- úzce spolupracuje s CSIRT - SOC
- ověřování, vyšetřování a hlášení kybernetických bezpečnostních incidentů předkládaných SOC včetně závěrů CSIRT - SOC,
- iniciování a koordinování opatření ke zvýšení bezpečnostního povědomí v ZZ a školení kybernetické bezpečnosti ve spolupráci s vedoucím personalistou zdravotnického zařízení,
- iniciování a koordinování opatření ke zvýšení fyzické bezpečnosti ve zdravotnickém zařízení ve spolupráci s vedoucím úseku údržby zdravotnického zařízení,
- provedení identifikace a hodnocení aktiv. Je koordinátorem pro jednotlivé garanty aktiv, kteří hodnocení konkrétních primárních a podpůrných aktiv v rámci hodnocení provádějí,
- hodnocení a řízení rizik, jakož i provádění a aktualizaci Plánu zvládání rizik,
- udržování a aktualizace dokumentace ISMS,
- komunikaci s příslušnými státními orgány a ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany (dále také „NÚKIB“) ve věcech kybernetické bezpečnosti,
- přímá spolupráce s manažerem kybernetické bezpečnosti krajského úřadu, zejména v oblasti technologických celků a sdílených služeb využívaných zdravotnickými zařízeními.

Předpokladem je, že role manažera KB (z důvodů oddělení pravomocí, jelikož je nelze kombinovat s rolí auditora kybernetické bezpečnosti), je v rámci zapojených subjektů personálně plně oddělena.

**Auditor kybernetické bezpečnosti**

(dále jen „auditor KB“) provádí audit kybernetické bezpečnosti a vyhodnocování účinnosti bezpečnostních opatření. Vykonává svoji roli nestranně a odděleně od dalších rolí v oblasti kybernetické bezpečnosti, hodnotí správnost a účinnost zavedených opatření. Auditor KB je osoba, která je pro tuto činnost vyškolena a má předepsanou odbornou způsobilost. Auditor KB vykonává zejména tyto činnosti:

- plánování auditu podle specifických podmínek řízených organizací,
- vedení dokumentace o průběhu auditu podle stanovených implementovaných metodik,
- vyhodnocování shromážděných nálezů z auditu a jejich srovnávání s kritérii auditu,
- sdělování výsledků auditu a navrhování doporučení (opatření),
- zpracování závěrečných zpráv z auditu,
- kontrola účinnosti přijatých opatření,
- kontrolní činnost naplňování smluvního vztahu v oblasti procesů, kvality a rozsahu dodávaných služeb SOC,
- re-auditní činnost,
- kontaktní osoba pro externí audit NÚKIB, je zodpovědná za dodání všech informací auditorům

Předpokladem je, že role auditora KB (z důvodů oddělení pravomocí, jelikož ji nelze kombinovat s rolemi manažera kybernetické bezpečnosti a architekta kybernetické bezpečnosti), je v rámci organizace personálně plně oddělena.

**Architekt kybernetické bezpečnosti**

(dále jen „architekt KB“) zajišťuje návrh a implementaci technických bezpečnostních opatření a po schválení Výborem korporátního řízení kybernetické bezpečnosti / Výborem pro řízení kybernetické bezpečnosti na úrovni ZZ se podílí na jejich implementaci. Architekt KB je osoba, která je pro tuto činnost vyškolena a má předepsanou odbornou způsobilost. Architekt KB vykonává zejména tyto činnosti:

- návrh bezpečnostních opatření pro snižování rizik, příprava pravidel a standardů pro oblast kybernetické bezpečnosti,
- určování nástrojů či technických opatření směřujících ke zvýšení kybernetické bezpečnosti, realizovaných v rámci MSDC, nebo ZZ a požadavků na specifické výstupy služeb SOC, v rámci plnění této veřejné zakázky, které rovněž směřují ke zvýšení kybernetické bezpečnosti,
- definice klíčových projektů, které vedou k naplnění bezpečnostní politiky a k cílovému stavu modelu architektury kybernetické bezpečnosti, dohled na jejich realizaci a vyhodnocení,
- analýzu úrovně architektury kybernetické bezpečnosti korporace, definici metrik a identifikaci existujících rizik s návrhem strategie na zmírnění rizik,
- vytváření plánů implementace architektury kybernetické bezpečnosti ZZ podle schválené bezpečnostní politiky, určovaní části a milníků k dosažení očekávaného cílového stavu.

Předpokladem je, že role architekta KB (z důvodů oddělení pravomocí) není slučitelná s rolemi odpovědnými za provoz informačních a komunikačních systémů.

### 3.2.3 Zdravotnická záchranná služba Moravskoslezského kraje, p.o.

ZZ je konzumentem služeb aktivní kybernetické bezpečnosti v definovaném rozsahu a hranicích. Současně je povinnou osobou[2]. V naplňování procesu aktivní kybernetické bezpečnosti disponuje těmito personálními rolemi:

**Vedení ZZ**

Jednotliví členové vedení jsou odpovědní za zajišťování bezpečnostního povědomí a dodržování bezpečnostních pravidel v rámci svých útvarů. Podílí se a naplňují tyto cíle:

- podílí se na definici strategie bezpečnostní politiky a aktivně podporují korporátní kybernetickou bezpečnost v rámci zdravotnického zařízení,
- přezkoumávají aktuálnost a účinnost implementace bezpečnostní politiky,
- poskytují zpětnou vazbu a viditelnou podporu bezpečnostním iniciativám,
- zajišťují dostatečné zdroje k realizaci bezpečnostních opatření.

**Systémový IT administrátor**

Je pracovní pozice na úrovni zdravotnického zařízení. Je odpovědná za administraci související s realizaci opatření plynoucích z události kybernetických incidentů. Mezi jeho odpovědnosti v rámci procesu patří zejména následující:

- koordinace činností v rámci realizace opatření v oblasti kybernetické bezpečnosti,
- vyhodnocování měsíčních zpráv SOC a návrh konkrétních podnětů k realizaci pro zvýšení KB ve vztahu k jednotlivým provozovaným ICT systémům,
- součinnost a oponentura bezpečnostního konceptu zdravotnického zařízení zpracovávaných MSDC, konceptu plánu obnovy a ostatních dílčích konceptů a systémových bezpečnostních pravidel, jakož i doplňujících pravidel a vodítek celkové kybernetické bezpečnosti pro ZZ,
- operativně vydává souhlas k aktivnímu zásahu při řešení kybernetického incidentu SOC,
- realizace bezpečnostních opatření kybernetických bezpečnostních incidentů předkládaných SOC,
- iniciování a spolupráce při koordinaci opatření ke zvýšení bezpečnostního povědomí ve zdravotnickém zařízení a součinnost při školení kybernetické bezpečnosti,
- udržování a aktualizace provozní dokumentace k jednotlivým provozovaným systémům.

**Garant aktiva** - garantem aktiva je osoba, která má vnitřním předpisem zdravotnického zařízení stanovenu odpovědnost za rozvoj, za evidenci aktiva a aktuálnost této evidence, použití a bezpečnost přiděleného aktiva v souladu s bezpečnostní politikou implementovaného ISMS a vnitřními předpisy zdravotnického zařízení. Garant aktiva je jmenován vedením zdravotnického zařízení.

Správa aktiva může být delegována, odpovědnost vždy nese garant aktiva.

[2] Zadavatel požaduje, aby k ZZ v rámci plnění veřejné zakázky bylo přistupováno, jako k povinné osobě v oblasti kybernetické bezpečnosti, a to i pokud tyto povinnosti plynoucí z platné a účinné legislativy prozatím nemá Národním úřadem pro kybernetickou a informační bezpečnost stanovené.

Garant aktiva odpovídá za primární aktiva nebo podpůrná aktiva dle odpovědnosti, vymezené vnitřním předpisem zdravotnického zařízení.

**Vedoucí úseku údržby**

Jedná se o pozici, která je na úrovni ZZ v gesci technického náměstka. Role je odpovědná za zajištění činnosti v oblasti facility managementu na úrovni zdravotnického zařízení. Plynoucí odpovědností je především zajištění realizace opatření dotčených žádanou úrovní fyzické bezpečnosti.

**Vedoucí personalista**

Je pracovní pozice na úrovni jednotlivého zdravotnického zařízení. Plynoucí odpovědností je zejména správa a účinnost elektronických identit zaměstnanců a ostatních osob s pracovně právním vztahem ke zdravotnickému zařízení. Dále koordinuje a eviduje vzdělávání nových zaměstnanců v oblasti kybernetické bezpečnosti. Svou činností se rovněž spolupodílí na vytváření prostředí pro vytvoření takového bezpečnostního povědomí, aby se bezpečnost stala neoddělitelnou součástí každodenního chodu zdravotnického zařízení.

## 3.3. Krajský úřad

ZZ využívá technologické centrum, které provozuje Krajský úřad Moravskoslezského kraje. V rámci tohoto centra jsou ZZ využívány sdílené služby krajské korporace a technologické celky centrálně provozované infrastruktury.

Z pohledu využívání služeb technologického centra kraje jednotlivými zdravotnickými zařízeními a jejich vztahů, je technologické centrum postaveno do role dodavatele, který má řešenou kybernetickou bezpečnost na své úrovni. V rámci požadavků kladených na řešení kybernetické bezpečnosti jsou v rozsahu shodné s požadavky, které jsou kladené na jakéhokoliv dodavatele.

Pak z pohledu řešení kybernetické bezpečnosti jsou v rámci krajského úřadu plně provozovány technologie a implementována opatření zajišťující kybernetickou bezpečnost provozovaných celků a sdílených služeb.

Z pohledu rolí jsou legislativou naplněné předpokládané pozice. V rámci centrálně provozovaných systémů a poskytovaných sdílených služeb bude v případně vzniklých bezpečnostních incidentů docházet k přímé spolupráci na úrovni manažerů kybernetické bezpečnosti. Zajištění komunikačních vazeb je realizováno z pozice role manažera kybernetické bezpečnosti v rámci působnosti Výboru korporátního řízení kybernetické bezpečnosti popisovaném dále v organizačním modelu.

V rámci této veřejné zakázky je předpokládáno, že v předmětu rozsahu poskytovaných služeb, může být ze strany dodavatele požadována součinnost v případě, že vyřešení incidentu bude nutno koordinovat a řešit v širších souvislostech. Tato součinnost bude ze strany Krajského úřadu dodavateli poskytnuta. V každém případě je jednoznačnou rolí, která má právo vyžadovat tuto součinnost v rámci plnění služeb SOC, role manažera KB MSDC.

# 4. Organizační model

Je úzce provázán s kompetenčním modelem. Je tvořen kolektivními orgány plnicí v tomto modelu specifické funkce vycházející z potřeb řízení aktivní kybernetické bezpečnosti a platné legislativy vZZ.

Pro rozsah této veřejné zakázky jsou jednotlivé výbory/týmy zřízeny na úrovni MSDC, ZZ a SOC.

Výbory pro řízení kybernetické bezpečnosti jsou tvořeny osobami s příslušnými pravomocemi a odbornou způsobilostí pro rozvoj systému řízení bezpečnosti informací a **osobami významně se podílejícími na řízení a koordinaci činností spojených s kybernetickou bezpečností,** jehož členem musí být alespoň jeden zástupce vrcholového vedení nebo jím pověřená osoba a manažer kybernetické bezpečnosti MSDC.

**Nutno však mít jednoznačně na zřeteli, že i při existenci kolektivních orgánů a předpokládaných smluvních závazcích určující vztahy mezi zapojenými subjekty, vždy legislativní odpovědnost nesou příslušně odpovědné statutární orgány.**

Ustanovené výbory z odborného pohledu reflektují rozdělení odpovědností, výkon kompetencí a podpůrných činnosti při plánování, řízení vztahů a realizaci v oblasti kybernetické bezpečnosti spolupracujících subjektů. Konkrétně vyjádřené povinnosti, kompetence a součinnost apod. mezi zapojenými subjekty budou stanoveny na úrovni smluvních vztahů.

### 1) Výbor korporátního řízení kybernetické bezpečnosti

Výbor pro řízení kybernetické bezpečnosti na korporátní úrovni koordinuje a vykonává dohled nad kybernetickou bezpečností v korporaci v rámci zapojených subjektů a plní tyto funkce v rámci své působnosti:

- odpovědnost za definici strategie Korporátní bezpečnostní politiky ISMS v rámci celkového řízení a rozvoje kybernetické bezpečnosti na úrovni korporace dle informační koncepce MSK,
- koordinaci postupu zajištění bezpečnosti informací a realizace bezpečnostní politiky v korporaci,
- realizace určených cílů strategii kybernetické bezpečnosti, příprava aktualizací Korporátní bezpečnostní politiky ISMS,
- vyhodnocení auditních zpráv a zprávy o stavu implementace Korporátní bezpečnostní politiky ISMS od Výborů pro řízení kybernetické bezpečnosti v jednotlivých zapojených subjektech v této oblasti,
- zajištění potřebné součinnosti mezi zapojenými subjekty,
- plánování a předkládání požadavků na potřebné zdroje pro provozování a rozvoj ISMS v resortu zdravotnictví,
- informování o změnách legislativy a standardů souvisejících s kybernetickou bezpečností,
- souhrnné hodnocení kybernetických bezpečnostních incidentů v resortu zdravotnictví a projednání návrhů řešení,
- přípravu podkladů pro vedení resortu zdravotnictví.

Za svolání výboru a jeho řízení odpovídá předseda výboru. Za stanovení jeho programu odpovídá manažer kybernetické bezpečnosti. Předseda výboru je volen členy výboru na jeho prvním zasedání.

V odůvodněných případech, na žádost kteréhokoli člena výboru, předseda výboru přizve najednání výboru:

- zástupce klíčových dodavatelů,
- zástupce dodavatelů dílčích služeb,
- další zaměstnance organizací, kteří mají k řešené problematice znalostní či kompetenční vztah.

Stálými členy Výboru korporátního řízení kybernetické bezpečnosti jsou:

- zástupce vedení MSDC,
- delegovaný zástupce zdravotnického zařízení pro oblast KB, který je současně členem vedení zdravotnického zařízení (zpravidla vedoucí ICT zdravotnického zařízení) za každou povinnou organizaci, dle zákona č.181/2014 Sb. Delegovaného zástupce jmenuje statutárním orgán zdravotnického zařízení,
- zástupce odvětvového odboru zřizovatele (odbor zdravotnictví),
- zástupce právního a organizačního odboru (na jednání je dle programu přizýván),
- manažer kybernetické bezpečnosti MSDC,
- manažer kybernetické bezpečnosti KÚ MSK,

- auditor korporace - není členem výboru, ale má právo se kdykoli účastnit jednání výboru.

**Výbor je ve své působnosti odpovědný za aktivní Korporátní bezpečnostní politiku ISMS a koordinaci činností mezi řízenými organizacemi.**

**2) Výbor pro řízení kybernetické bezpečnosti ve zdravotnickém zařízení**

Výbor pro řízení kybernetické bezpečnosti ve zdravotnickém zařízení koordinuje a vykonává dohled nad kybernetickou bezpečností konkrétního zdravotnického zařízení a plní tyto funkce:

- odpovídá za implementaci Korporátní bezpečnostní politiky ISMS v rámci zdravotnického zařízení,
- vytváří koncept bezpečnosti informací ve zdravotnickém zařízení,
- vyhodnocuje stav a účinnost bezpečnosti informací ve zdravotnickém zařízení,
- vypracovává podklady o stavu a účinnosti implementace Korporátní bezpečnostní politiky ISMS pro Výbor korporátního řízení kybernetické bezpečnosti,
- schvaluje návrhy a implementace bezpečnostních opatření ve zdravotnickém zařízení,
- pomáhá zajistit součinnost jednotlivých útvarů při prosazování kybernetické bezpečnosti v rámci zdravotnického zařízení, podporuje vzdělávání v oblasti kybernetické bezpečnosti.

Za svolání výboru a jeho řízení odpovídá předseda výboru. Za stanovení jeho programu a podkladů odpovídá manažer kybernetické bezpečnosti. Zde je pravidlem, že delegovaný zástupce zapojených subjektů do Výboru korporátního řízení kybernetické bezpečnosti je současně předsedou Výboru pro řízení kybernetické bezpečnosti ve zdravotnickém zařízení. V odůvodněných případech, na žádost kteréhokoli člena výboru, předseda výboru přizve najednání výboru:

- zástupce klíčových dodavatelů,
- zástupce dodavatelů dílčích služeb,
- další zaměstnance organizace, kteří mají k řešené problematice znalostní či kompetenční vztah.

Stálými členy Výboru pro řízení kybernetické bezpečnosti ve zdravotnickém zařízení jsou:

- zástupce vedení zapojených subjektů,
- zástupce vedení organizačního útvaru informatiky,
- zástupce právního oddělení,
- manažer kybernetické bezpečnosti (MSDC),
- garanti aktiv určených významných informačních systémů dle zákona č.181/2014 Sb.,
- vedoucí úseku údržby, je přizýván na jednání, pokud je na programu problematika fyzické bezpečnosti
- vedoucí personalista
- auditor korporace (MSDC), není členem výboru, ale má právo se kdykoli účastnit jednání výboru

**Výbor je odpovědný za implementaci Korporátní bezpečnostní politiky ISMS a prosazování zásad bezpečnosti informací v konkrétním zapojeném subjektu.**

### 3) CSIRT-SOC

Vyžadovaným předpokladem je, že Computer Security Incident Response Team je ustanoven v rámci SOC (dále také „CSIRT - SOC“) a je předmětem plnění služeb této veřejné zakázky.

Sehrává klíčovou roli při ochraně kritické informační infrastruktury ZZ. Jeho cílem je zlepšovat bezpečnost, obranu a ochranu infrastruktury a dat, minimalizovat dopad, který mohou způsobit průniky nebo kompromitace.

Současně vyžadovaným předpokladem je, že v rámci své působnosti řeší synergie plynoucí ze své činnosti vůči všem subjektům. Uvedené znamená, že pokud bude dotčena kybernetická bezpečnost jakéhokoli subjektu, který je předmětem plnění služeb této veřejné zakázky, bude vždy současně z preventivních důvodu shodně postupováno vůči všem zdravotnickým zařízením.

V organizačním modelu plní tyto funkce:

- řeší všechny typy IT bezpečnostních incidentů, které vznikly nebo mohou potenciálně vzniknout, v rámci jeho působnosti,
- může poskytnout přímou podporu koncovým uživatelům,
- informuje o potenciálních zranitelnostech, a tam, kde je to možné, informuje cílovou skupinu ve své působnosti o takových zranitelnostech ještě před jejich zneužitím,
- jeho cílem je pomáhat místním správcům při řešení technických a organizačních aspektů incidentů,
- provádí třídění (věrohodnost, priority), koordinaci stran (kontaktování zúčastněných, informování CSIRT týmů) při řešení incidentu a vlastní řešení incidentu (poskytování poradenství o postupech, poskytování pomoci při shromažďování důkazů a interpretaci dat, včasné informování o možných útocích a napomáhání při ochraně proti známým útokům),
- v rámci proaktivního přístupu shromažďuje seznamy bezpečnostních kontaktů pro každou entitu v rámci svého pole působnosti, publikuje oznámení o závažných bezpečnostních hrozbách, aby se v nejvyšší možné míře zabraňovalo incidentům v oblasti informačních a komunikačních technologií a snížil se tak co nejvíce jejich dopad. V případě pozitivního nálezu zajišťuje předání relevantní informace garantu aktiva odpovědnému za postižený systém,

- provádí aktivní zásahy vedoucí ke snížení závažnosti incidentů,
- úzce spolupracuje s manažerem KB MSDC,
- řeší synergie vůči všem zapojeným subjektům,
- zajišťuje komunikaci s GovCERT/CSIRT, případně Hospital SOC.

## 5. Provozní/procesní model

Základním strukturovaným postupem pro řízení kybernetické bezpečnosti je řešení tohoto životního cyklu od:

- predikce kybernetických rizik - formou dlouhodobé analytické činnosti s cílem predikce vzniku situací vedoucích k bezpečnostním incidentům (analýza pokročilých hrozeb a behaviorální analýze chování uživatelů),
- prevence kybernetických rizik - činnost vedoucí k identifikaci bezpečnostních slabin před vznikem bezpečnostního incidentu (penetračního testování a testování zranitelností),

a v případě vzniku:

- detekování, hlášení a vyhodnocení kybernetických bezpečnostních událostí a incidentů - identifikace a monitorování kybernetických událostí v reálném čase nad platformami SIEM (které jsou součástí poskytované služby), doplněné o další korelační a analytické nástroje provozované v rámci SOC,
- reakci na kybernetické bezpečnostní incidenty a jejich řízení - evidence, eskalace, analýza (včetně analýzy dopadů) a návrh opatření,
- realizace opatření - aktivní zásah ze strany SOC **na základě určených pravidel a postupů obsažených v ISMS.**

až po závěrečnou dokumentaci kybernetického bezpečnostního incidentu a nahlášení příslušným orgánům.

Cílem realizace tohoto modelu je stanovit postupy a nástroje ke snížení dopadů kybernetických bezpečnostních incidentů a včasné zastavení jejich šíření, omezení jejich dopadů a předcházení jejich opakování.

Tento model je v rámci potřeb řešených touto veřejnou zakázkou nutně provázán s kompetenčním a organizačním modelem, jelikož výstupy poskytovaných služeb zasahují do hierarchických struktur více subjektů. **Základem pro realizaci tohoto provozního modelu je implementace ISMS.**

## 5.1. Procesní část modelu

Procesní část modelu je vyjádřena s pomocí RACI matice. V této matici jsou uvedeny příklady popisů procesů ve vztahu k potřebám řešení předmětu této veřejné zakázky. Vlastní RACI matice představuje matici aktivit (procesů) a rolí, které mají k dané aktivitě předem definovaný vztah.

Tento vztah je tvořen z písmen R, A, C, I, která mají tento význam:

- **R (Responsible) -** procesní role má fyzickou odpovědnost za vykonání dané aktivity v rámci své působnosti.
- **A (Accountable) -** procesní role má odpovědnost za fakt, že daný proces je vykonáván tak, jak bylo předdefinováno. U každého procesu může být jen jedna tato role (většinou se jedná o vedoucího pracovníka, který je odpovědný za práci svého týmu).
- **C (Consulted) -** procesní role podílející se na výkonu procesu, avšak nepřebírá za výkon procesu odpovědnost (jde o konzultační či spolupracující roli).
- **I (Informed) -** procesní role, která musí být o výstupech procesu informována.

| Příklady procesů týkajících se kybernetické bezpečnosti v návaznosti na popisované modely | | Výbor korporátního řízení KB | Výbor pro řízení KB | Bezpečnostní role | | | | Role SOC | | | | Hierarchická úroveň ZZ | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | MSDC | | | | | CSIRT tým | | | | | | |
| | | | | Manažer KB | Architekt KB | Auditor KB korporace | Garant Aktiva | *Operátor SOC* | *Analytik* | *Expert* | *Forenzní analytik* | Vedoucí ZZ (CIO) | systémový administrátor | vedoucí úseku údržby | Vedoucí personalista |
| *strategická úroveň řízení KB* | Strategické řízení a rozvoj KB na úrovni korporace | R, A , I | R , I | c , i | c , i | C , I | C , I | - | - | - | - | c , i | - | - | - |
| | Implementace, řízení a rozvoj KB na úrovni ZZ | I | R , I | R, C, I | R,C,I | c , i | c , i | - | - | - | - | A,C,I | C | C | C |
| | Audit KB | A, C, I | I | c , i | c , I | R | C, I | - | *1* | | | 1 | 1 | 1 | 1 |
| | Systém řízení bezpečnosti informací | A, C, I | R, C, I | R | C, I | C | c , I | *1* | *1* | | | - | - | - | - |
| *Taktická úroveň* | Návrh bezpečnostních opatření | c , i | c , i | c , i | R | I | C, I | | *A* | | | 1 | C,I | C,I | c,I |
| | Implementace bezpečnostních opatření | c , i | c , i | R, C, I | R | I | c , I | - | *1* | | | A,I | R,C | R,C | R,C |
| | Zajištění rozvoje, použití a bezpečnosti aktiva | c , i | c , i | R, C, I | C , I | C | R | - | *1* | | | A,I | c , i | c , i | c, 1 |
| *Operativní úroveň (ZZ)* | Detekce incidentu, přidělení k řešení | - | - | I | - | - | I | ***R*** | *R,A* | | | - | 1 | 1 | 1 |
| | Vyhodnocení incidentu | - | I | I | - | - | I | - | *R,A* | | | 1 | 1 | 1 | 1 |
| | Realizace opatření (z oblasti fyzické bezpečnosti) | - | I | R | - | - | I | - | *1* | | | A, 1 | R,C | R,C | 1 |
| | Realizace opatření z behaviorální analýzy chování uživatelů | I | I | R,I | I | I | - | - | *1* | | | A,I | i , c | 1 | R |
| | Vyhodnocení účinnosti | I | I, R | A | I | I | I | | | | | 1 | 1 | 1 | 1 |

Tabulka č. 1 - RACI matice - příklad popisu základních procesů spojených s bezpečnostními rolemi

**Dílčím cílem** v této oblasti je, že v rámci **implementace ISMS bude RACI matice obsahovat relevantní pravidelně se opakující procesy,** které doplní o aktivity a vztahy k jednotlivým rolím vzhledem k prostředí, do kterého je implementována.

## 5.2. Prevence a predikce kybernetických hrozeb

V této části modelu jsou popsány požadavky na procesní přístup a rozsah pro hodnocení kybernetických hrozeb. Aktiva si označíme jako A (assets), hrozby jako T (threat) a zranitelnosti jako V (vulnerability). Základní otázkou obvykle je, v jakém pořadí hodnotit tyto faktory.

Je možné začít hodnocením aktiv (A), pokračovat s hodnocením hrozeb (T) a zranitelností (V). Dalším adekvátním přístupem je identifikace hrozeb (T) a zranitelností (V) a stanovení pravděpodobnosti zneužití dané zranitelnosti hrozbou se stanovením jejího dopadu na aktivum (A). Rovněž nabízenou možnosti přístupu je postup, kde je započato s hodnocením zranitelnosti (V) s hledáním hrozeb (T), které by mohly nalezenou zranitelnost využít a hodnocením aktiv (A) stanovit velikost dopadu.
Pro predikci kybernetických hrozeb je možno využít jakýkoli procesní postup. Vyžadovanou podstatou a výsledkem je predikce pro stanovení pravděpodobnosti na základě vztahu, mezi aktivem, hrozbou a zranitelností, kdy existuje vysoká pravděpodobnost rizika, a současně se vyskytuje zranitelnost, které by hrozba mohla využít.

Předpokladem je, že v případě pokročilých přetrvávajících hrozeb (Advanced Persistent Threat dále také „APT“) je nutné vyhodnotit také faktory jako je velikost, významnost, známost a oblíbenost daného zdravotnického zařízení, neboť je zřejmé, že vždy se najde někdo, kdo bude mít motiv, příležitost i schopnost danou hrozbu realizovat. Uvedené pak vede ktomu, že pravděpodobnost hrozby je ve značných případech úměrná hodnotě aktiva.

**V rámci předmětu poskytovaných služeb** v oblasti prevence a predikce kybernetických hrozeb a s tím souvisejících rizik je požadováno, aby v rozsahu poskytovaných služeb SOC byla pro ZZ zajišťována:

- analýza rizik - je vyžadován nelineární proces, ve kterém interaktivně dochází v čase k přehodnocení výše uváděných (A, V, T) faktorů včetně pokročilých přetrvávajících hrozeb (APT),
- predikce kybernetických hrozeb a s tím souvisejících rizik- soustavný analytický přístup.s cílem predikce a stanovení pravděpodobnosti vzniku možných bezpečnostních incidentů,
- prevence - identifikace slabých bezpečnostních míst, které by mohly být využity ke zranitelnosti kybernetickým útokem,
- vulnerability management - služba prováděna SOC musí zajistit kontinuální skenování aktiv zadavatele definovaných danou sítí/sítěmi a zranitelnostmi relevantními pro daná aktiva. **Minimálně na začátku poskytování služby budou provedeny a vyhodnoceny plné skeny (asset discovery skeny všech sítí a aktivní nedestruktivní skeny zranitelnosti všech zařízení vyjma klientských a speciálních zdravotechnických zařízení) a dále vždy 1x měsíčně skeny rozdílové (technicky se jedná o stejné skeny jako plné skeny, ale jejich výsledek je interpretován a zobrazován i v komparaci k předchozím skenům).** Plné skeny boudou rovněž provedeny při implementaci, upgrade, či update provozovaných ICT celků v reakci na požadavek zadavatele.

**Penetrační testy jsou předmětem plnění této veřejné zakázky.** Je však požadováno, aby je prováděla na systému řízení **zcela nezávislá organizace.** Dodavatel má povinnost smluvně zajistit nezávislou organizaci, která před každým prováděným penetračním testem musí prokázat svou nezávislost. Současně je dodavatel povinen toto učinit kdykoli je objednatelem o to požádán. V případě prokazatelných pochybností Objednatele o nezávislosti organizace provádějící penetrační testování si Objednatel vyhrazuje právo požadovat změnu této organizace.

Výsledky jsou silnou zpětnou vazbou pro hodnocení účinnosti implementované kybernetické bezpečnosti.

První sadu penetračních testů ve Zdravotnické záchranné službě Moravskoslezského kraje dle Smlouvy dodavatel smluvně zajistí v rozsahu, který je vymezen v příloze č. 3 této technické specifikace na svůj náklad u nezávislé organizace dle shora uvedeného, a to po dokončení analýzy rizik v návaznosti na identifikaci aktiv, která budou podrobena penetrační testům.

Nad rámec první sady penetračních testů, zajištěných dodavatelem dle předchozího odstavce, bude v Provozní fázi SOC povinnost dodavatele smluvně zajistit nezávislou organizaci k provedení penetračních testů (jednotlivých testů, souhrnných sad testů či opakovaných testů) zahrnovat následující činnosti dodavatele:

- asistence objednateli při sestavení žádosti o předložení nabídky na provedení penetračních testů - verifikace zadání z technického hlediska
- vyhledání vhodných subjektů k oslovení s žádostí o předložení nabídky na provedení penetračních testů
- komunikace s vybranými subjekty dle preferencí objednatele a jejich přímé oslovení s žádostí o předložení nabídky na provedení penetračních testů
- asistence objednateli při posouzení došlých nabídek
    - posouzení nabídek z hlediska technického
    - připomínkování smluvní dokumentace z hlediska technického a best practices

Provedení dalších sad penetračních testů již dodavatel nezajišťuje na svůj náklad.
Tímto rozsahem smluvního zajištění je ve vztahu k provádění penetračního testování naplněn také čl. XV.24. Smlouvy.

## 5.3. Provozní část modelu pro řízení kybernetických bezpečnostních incidentů

V provozním modelu jsou dále popsány podmínky pro procesní reakci na členění, kategorizaci, stavy řešení a realizaci technických opatření v případě vzniku kybernetických bezpečnostních událostí a incidentů.

### 5.3.1 Typy kybernetických bezpečnostních incidentů

Typy kybernetických bezpečnostních incidentů jsou děleny podle dvou kritérií, a to podle příčiny a dopadu. **Podle příčiny** se kybernetické bezpečnostní incidenty dělí na následující:

1. kybernetický bezpečnostní incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb,
2. kybernetický bezpečnostní incident způsobený škodlivým kódem,
3. kybernetický bezpečnostní incident způsobený překonáním technických opatření,
4. kybernetický bezpečnostní incident způsobený porušením organizačních opatření,
5. kybernetický bezpečnostní incident spojený s projevem trvale působících hrozeb,
6. ostatní kybernetické bezpečnostní incidenty způsobené kybernetickým útokem.

**Podle dopadu** jsou kybernetické bezpečnostní incidenty rozděleny do následujících typů:

1. kybernetický bezpečnostní incident způsobující narušení důvěrnosti primárních aktiv,
2. kybernetický bezpečnostní incident způsobující narušení integrity primárních aktiv,
3. kybernetický bezpečnostní incident způsobující narušení dostupnosti primárních aktiv,
4. kybernetický bezpečnostní incident způsobující kombinaci dopadů uvedených v bodech 1. až 3 tohoto odstavce.

### 5.3.2 Kategorizace kybernetických bezpečnostních incidentů

Podle následků, negativních projevů a předpokládaného dopadu na primární a podpůrná aktiva řešených subjektů se kybernetické bezpečnostní incidenty dělí do následujících kategorií:

**Kategorie I -** méně závažný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo primárních a podpůrných aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod. V rámci této kategorie je předpokládán aktivní zásah po kontaktování a souhlasu IT administrátora ZZ.

**Kategorie II -** závažný kybernetický bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo primárních a podpůrných aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod. V rámci této kategorie je předpokládán aktivní zásah po kontaktování a souhlasu IT administrátora ZZ.

**Kategorie III -** velmi závažný kybernetický bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo primárních a podpůrných aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod. V rámci této kategorie je předpokládáno provedení aktivního zásahu a poté kontaktování administrátora IT ZZ s předanou informací o realizovaných opatřeních v rámci aktivního zásahu.

Pro určení kategorií kybernetického bezpečnostního incidentu jsou zohledněny zejména následující atributy kybernetického bezpečnostního incidentu:

- důležitost dotčených aktiv informačního systému,
- dopady na poskytované služby informačního systému,
- dopady na služby poskytované jinými informačními systémy,
- předpokládané škody a další dopady.

### 5.3.3 Fáze analýzy, rozhodnutí a zvládání

V této fázi procesu členové CSIRT-SOC určí přesný rozsah kybernetického bezpečnostního incidentu, tedy primární a podpůrná aktiva, která jsou nebo mohou být zasažena, možný dopad na základní služby. Zvolí vhodnou strategii pro řešení kybernetického bezpečnostního incidentu.

**1) <u>V závislosti na kategorii bezpečnostního incidentu</u>**

**Kybernetické bezpečnostní incidenty (Kategorie I) -** pokud je kybernetická bezpečnostní událost vyhodnocena jako méně závažný kybernetický bezpečnostní incident, určuje člen CSIRT-SOC jeho stav a může jej vyřešit ve spolupráci s operátorem.

**Závažné kybernetické bezpečnostní incidenty (Kategorie II a III) -** pokud je kybernetickému bezpečnostnímu incidentu přidělena kategorie II nebo III, je jeho řešení předáno všem členům CSIRT-SOC, kteří musí:

- <u>Shromáždit všechny další potřebné informace</u> - jak vzniknul, kdo a čím ho způsobil, co zasahuje nebo by mohl zasáhnout, dopad nebo potenciální dopad kybernetického bezpečnostního incidentu na činnost zdravotnického zařízení.
- <u>Aspekty případného záměrného technického útoku</u> - jak hluboko do systému, služby, nebo sítě útočník pronikl a jakou má úroveň kontroly, jakým primárním a podpůrným aktivům se útočníkovi podařilo získat přístup, zda je mohl zkopírovat, pozměnit nebo zničit.
- <u>Přímé a nepřímé následky kybernetického bezpečnostního incidentu</u> - například umožnění přístupu do budovy z důvodu požáru, nebo zranitelnost informačního systému z důvodu závady softwaru nebo komunikační linky nebo lidské chyby.
- <u>Souvislost s případnými dalšími</u> kybernetickými bezpečnostními incidenty.
- <u>Provést samostatně aktivní opatření,</u> pokud by odkladem hrozilo další šíření škodlivého kódu, nedostupnost kritických služeb apod. Takový zásah musí být vykonán v souladu se znalostí dopadu aktiva na provozované služby a aplikace, podle nastavených pravidel součinnosti u jednotlivých aktiv vycházející z implementace ISMS.
- Řešit v rámci synergie otázky, zda nemůžou být ohroženy šířením škodlivého kódu další zapojené subjekty.
- <u>Uvědomit manažera KB, IT administrátora.</u>
- <u>Uvědomit garanty dotčených primárních a podpůrných aktiv</u> a dalších subjektů podílejících se na řešení incidentu.

**V těchto fázích bude poskytována součinnosti v režimu 24x7 ze strany ICT administrátorů ZZ. V rámci součinnosti zadavatel poskytne veškerou nutnou součinnost potřebnou pro poskytování služeb v rámci specifikovaného plnění.**

2) **Analýza a návrh opatření**

V závislosti na typu a závažnosti kybernetického bezpečnostního incidentu vybere CSIRT-SOC vhodný postup pro řešení incidentu. Prvním krokem reakce musí být vždy zastavení šíření kybernetického bezpečnostního incidentu, a tedy omezení dalších škod. Současně se informuje a následně přiděluje řešiteli.

3) **Řešení kybernetického bezpečnostního incidentu**

Po identifikaci a stanoveném postupu řešení jsou započaty činnosti na odstranění, nebo snížení dopadů bezpečnostního incidentu. Dochází ke koordinaci činností a k monitorovaní průběhu řešení.

### 5.3.4 Dokumentace kybernetického bezpečnostního incidentu

- **Záznam o kybernetickém bezpečnostním incidentu -** všechna získaná data a informace o kybernetických bezpečnostních incidentech včetně realizovaných opatřeních jsou vedeny v provozovaném informačním systému v rámci SOC a objednatel má do systému vytvořen přístup.

- **Důkazní materiál -** CSIRT-SOC je zodpovědný za sběr všech informací týkajících se kybernetického bezpečnostního incidentu a bezpečné uložení veškerého důkazního materiálu. Musí být náležitě zdokumentováno, jak byl veškerý důkazní materiál včetně zasažených systémů uchován. Aby byl důkazní materiál přípustný pro použití v soudním řízení, musí být shromažďován v souladu se všemi obecně závaznými právními předpisy a interními předpisy zapojených subjektů. Vždy musí být zřejmé, kde a u koho se důkazní materiál nachází. Kdykoliv je důkazní materiál někomu předán, vyplní předávající osoba příslušný předávací formulář, který podepíší obě strany. Podrobný záznam k veškerému důkaznímu materiálu vede osoba, u níž je materiál uložen. Obsah záznamu bude stanoven interním předpisem zapojených subjektů v rámci implementace ISMS.

## 5.4. Stavy kybernetického bezpečnostního incidentu

Kybernetický bezpečnostní incident má po celou dobu svého životního cyklu přidělený stav, který určuje, v které fázi své existence se nachází. Tyto stavové veličiny kybernetického bezpečnostního incidentu jsou zaznamenávány v SW nástroji, který je **provozován v rámci SOC a objednatel má do systému vytvořen přístup.**

| Stav incidentu | Popis | Reakce (změna stavu) |
|---|---|---|
| Registrován | Hlášení o události bylo přijato SOC a událost byla zanesena do databáze | Operátor SOC |
| Přidělen | Kybernetický bezpečnostní incident byl přidělen týmu CSIRT-SOC | Operátor SOC |
| Neadekvátní | Stav pro nahlášené události, které nenabyly charakteru kybernetického bezpečnostního incidentu | CSIRT-SOC |
| Přijat | Řešitel kybernetického bezpečnostního incidentu ho přijal a plánuje řešení | CSIRT-SOC |
| Řešen | Kybernetický bezpečnostní incident je dle smluvních podmínek analyzován a v reakci je stanoven návrh opatření, případně je prováděn aktivní zásah | CSIRT-SOC |
| Vyřešen | Řešením kybernetického bezpečnostního incidentu bylo zastaveno jeho další šíření | CSIRT-SOC |
| Vyhodnocen | Vyhodnocení účinnosti řešení incidentu a stanovení nutných opatření | MSDC, manažer kybernetické bezpečnosti |
| Realizace | Realizace přijatých nápravných opatření | MSDC, manažer kybernetické bezpečnosti |
| Uzavřen | Řízení kybernetického bezpečnostního incidentu bylo ukončeno | MSDC, manažer kybernetické bezpečnosti |

Tabulka č. 2 - Stavové veličiny bezpečnostního incidentu

## 6. Předmět plnění veřejné zakázky

Předmětem plnění této veřejné zakázky je implementace systému řízení bezpečnosti informací ISMS *(Information Security Management System) a* komplexní zajištění služeb centra kybernetické bezpečnosti (SOC) k zajištění dohledu operátory, provozu nástrojů pro sběr a vyhodnocování kybernetických bezpečnostních událostí v provozovaných systémech a v komunikačních sítích zapojených subjektů se zajištěním prevence a aktivní reakce na případné kybernetické incidenty.

Předmětem plnění této veřejné zakázky je závazek dodavatele:

1) **Implementovat systém řízení bezpečnosti informací ISMS,** a to s využitím popsaných modelů v rámci:

   - Zdravotnická záchranná služba Moravskoslezského kraje, p.o.

2) **Poskytovat služby aktivní kybernetické bezpečnosti prostřednictvím SOC** pro ZZ v rámci popsaných modelů v rámci plnění pro ZZ.

   Služby budou poskytované zdravotnickému zařízení kraje:

   - Zdravotnická záchranná služba Moravskoslezského kraje, p.o. (2 hlavní lokality - IBC a ředitelství)

   Poskytování služeb bude rozsahem a kvalitou plně vyhovovat kladeným požadavkům zadavatele - Moravskoslezského datového centra a ZZ dotčeného touto veřejnou zakázkou.

3) **Prováděcí projekt -** v rámci předmětu plnění bude dodán Prováděcí projekt, který bude předmětem akceptačního řízení a jehož obsahem bude:

   - detailní projektový plán
   - rozdílová analýza výchozí stav/aktuální stav - bude obsahovat rozdíl mezi popsaným stavem v této Technické specifikaci a skutečností v době po nabytí účinnosti smluvního vztahu. Rozdílová analýza je nástrojem pro přesné stanovení východisek. Pro zpracování této analýzy zadavatel poskytne příslušnou součinnost
   - výstupy z adaptační fáze - prvotní analýza, Identifikace zdrojů dat, návrh modifikace nastavení monitorovacích nástrojů, scénáře pro řešení bezpečnostních a provozních incidentů a událostí s dodržením požadovaných SLA včetně návrhu hardeningových bezpečnostních politik
   - popis realizace integrací - návrh komunikace SOC se systémy třetích stran na základě standardizovaného API a podpory skriptování.
   - detailní technická specifikace implementace HW a SW prvků implementovaných do prostředí ZZ
   - reporting (pravidelné, on-demand reporty) - rozpracování v detailu nejvyšší granularity pro grafické interaktivní zobrazení obsahu prezentovaných hodnot v jednotlivých oblastech
   - exit plan s detailním popisem činností pro ukončení poskytovaných služeb s rozsahem předání dat, nastavení apod.

   Implementační projekt podléhá vlastní akceptační proceduře. Po předání implementačního projektu může objednatel do 5 pracovních dnů předat v písemné podobě zhotoviteli své výhrady. Zhotovitel neprodleně, nejpozději však do 5 kalendářních dnů, nedohodnou-li se smluvní strany jinak, zapracuje objednatelem uvedené nedostatky a připomínky. Proces akceptace lze opakovat, dokud zhotovitel nezapracuje veškeré výhrady vznesené objednatelem.

**A to v těchto základních milnících a za stanovených ostatních podmínek specifikovaných v zadávací dokumentací:**

- Zpracování, připomínkování a akceptace Prováděcího projektu
- Základní implementace v ZZ
- Implementace ISMS v ZZ
  - ustanovení ISMS v ZZ
  - zavedení ISMS
  - životní cyklus řízené dokumentace pro splnění legislativních potřeb dle ZoKB
- Monitorování a přezkoumání účinnosti ISMS v rámci provozní fáze
- Poskytování služeb SOC
  - adaptační fáze
  - provozní fáze
  - exit fáze

**Současně kategorickým požadavkem je předložení zpracovaného rámcového projektového plánu, který bude součástí zpracované nabídky obsahující splnění všech podmínek této zadávací dokumentace.**

## 6.1. Služby ISMS

Předmětem této části veřejné zakázky je implementace systému řízení bezpečnosti informací (ISMS) v souladu s požadavky legislativy (zákon č.181/214 Sb. a jeho prováděcí vyhlášky) a dle technických norem a standardů pro tuto oblast, a to v reflexi na uvedené modely v této zadávací dokumentaci.

**Předmětem poskytovaných služeb v oblasti ISMS je:**

1) **Základní implementace -** ve lhůtě **3 měsíců** od nabytí účinnosti smluvního vztahu, je provedena v rozsahu nutném pro zahájení poskytování služeb SOC. Tímto nutným rozsahem je míněna implementace základního minima pro oblast řešící reakce na bezpečnostní incidenty a bezpečnostní události.

2) **Ustanovení ISMS v ZZ -** cílem této dílčí etapy je upřesnit rozsah a hranice, kterých se řízení bezpečnosti informací týká, stanovit jasné manažerské zadání a na základě ohodnocení rizik vybrat nezbytná bezpečnostní opatření v těchto krocích:
   - definice procesů a rozdělení kompetencí a odpovědnosti s vazbou na popsané modely,
   - definice rozsahu, hranic a vazeb ISMS,
   - definice převažujících procesů vyjádřených pomocí RACI matice (viz kapitola 5.1),
   - definice a odsouhlasení Prohlášení o politice ISMS,
   - analýza a zvládání rizik,
     - definice přístupu ZZ k hodnocení rizik,
     - ocenění aktiv do kategorií (významné informační systémy) na základě úplného předloženého seznamu zadavatelem,
     - identifikace rizika včetně určení aktiv a jejich vlastníků,
     - analýza a vyhodnocení rizik,
     - stanovení kategorií a postupů eskalace ve vztahu ke kontaktování a souhlasu IT administrátora zdravotnického zařízení,
     - identifikace a ohodnocení variant pro zvládání rizik,
     - výběr cílů opatření a jednotlivých opatření pro zvládání rizik,
     - souhlas vedení zdravotnického zařízení s navrhovanými zbytkovými riziky a se zavedením ISMS,
   - prohlášení o aplikovatelnosti.

3) **Zavedení ISMS -** cílem této dílčí etapy je účelně a systematicky prosadit vybraná bezpečnostní opatření do chodu ZZ. Prosazení bezpečnostních opatření je odpovědností managementu ZZ. Zavedení ISMS bude určeno těmito kroky:
   - formulace dokumentu plánu zvládání rizik a jeho zavedení,
   - zavedení plánovaných bezpečnostních opatření a formulace příručky bezpečnosti informací, která upřesní pravidla a postupy aplikovaných opatření v definovaných oblastech bezpečnosti informací (ISO/IEC 27002),
   - definice programu budování bezpečnostního povědomí a zaškolení všech uživatelů, manažerů a odborných pracovníků z úseku informatiky, a to zejména z oblasti systému řízení bezpečnosti informací,
   - upřesnění způsobů měření účinnosti bezpečnostních opatření a sledování stanovených ukazatelů,
   - zavedení postupů a dalších opatření pro rychlou detekci a reakci na bezpečnostní incidenty,
   - řízení zdrojů, dokumentů a záznamů ISMS.

4) **Školení zaměstnanců v oblasti ISMS -** cílem je v rámci definovaného programu zvýšit bezpečnostní povědomí všech zaměstnanců dotčených systémem řízení bezpečnosti informací (viz. orientační počty vztaženy k aktuálnímu počtu zaměstnanců ke dni zahájení VZ uvedené v tabulce č. 3).

| kategorie zaměstnanců | Hlavní pracovní poměr | Dohody o práci (DPČ, DPP) |
|---|---|---|
| vedení zdravotnického zařízení | 1 | |
| vedoucí zaměstnanci (primář, staniční setra, vrchní sestra, ostatní vedoucí pracovníci) | 120 | |
| Lékaři | 100 | 163 |
| Sestry včetně záchranářů | 383 | 117 |
| ostatní zdravotní personál | 258 | 17 |
| THP | 50 | 38 |
| dělnické kategorie | 18 | 31 |
| **CELKEM** | 809[3] | 366 |

[3] Vedoucí zaměstnanci jsou zahrnuti také do jednotlivých kategorií typu lékař, sestra atp.

Tabulka č. 3 - Orientační počty zaměstnanců ve ZZ

Školení musí být periodické, musí být vyhodnocováno a přizpůsobováno kategorii zaměstnanců. Školení musí být relevantní k aktuálním hrozbám a trendům. Školení je možné provádět kombinovanou podobou s využitím učeben (zajistí ZZ), dálkového vzdělávání, webových nástrojů, samovzdělávacích kurzů atd. V rámci školení musí být vytvořeny a předány školící materiály. Školení musí dále obsahovat potřebnou administrativu, která zahrnuje pozvánky, prezenční listiny, přezkoušení, potvrzení o absolvování školení atd.

5) **Monitorování a přezkoumání ISMS -** cílem této dílčí etapy je zajištění zpětné vazby účinnosti všech aplikovaných bezpečnostních opatření a jejich důsledků na bezpečnost informací v ZZ.
Vlastní přezkum začíná u přímé kontroly odpovědných osob ze strany jejich nadřízených či manažera kybernetické bezpečnosti.
Další důležitou roli sehrává nezávislé posouzení fungování a účinnosti ISMS pomocí interních auditů ISMS, které jsou předmětem plnění. Obecným cílem v této oblasti je na základě všech použitých zpětných vazeb připravit dostatek podkladů o skutečném fungování ISMS, které budou v rámci interního auditu předloženy vedení organizací za účelem přezkoumání, zdaje realizace ISMS v souladu s obecnými potřebami ZZ. Během této části plnění je nezbytné provést následující činnosti:

- v pravidelných intervalech monitorovat a ověřit účinnost prosazení bezpečnostních opatření,
- provést interní audity ISMS, jejichž náplň pokryje celý rozsah ISMS,
- připravit auditní zprávu o stavu ISMS a na jejím základě lze přehodnotit ISMS na úrovni vedení zdravotnického zařízení (včetně revize zbytkových a akceptovaných rizik).

6) **Životní cyklus správy bezpečnostní dokumentace -** cílem této etapy je zajištění celého životního cyklu bezpečnostní dokumentace tak, aby splnila minimálně legislativní požadavky spojené s provozem systémů základní služby.

Zadavatel plánuje pořídit aplikační prostředí umožňující přístup všem správcům aktiv ZZ, pracovníkům bezpečnosti MSDC (především manager KB, architekt KB, auditor KB) a k vybraným informacím rovněž pracovníků SOC. Do doby pořízení je k dispozici MS Teams/SharePoint MSDC.

Aplikační systém bude podporovat:

- Zajištění kompletního životního cyklu dokumentů (vznik/verzování, schválení, distribuci a archivaci) potřebných pro řízení kybernetické bezpečnosti - pro automatizaci a řízení procesů prostřednictvím nástrojů workflow.
- Zajištění veškerých standardních procesů v návaznosti na platnou legislativu kybernetické bezpečnosti:
    - publikace vzorové dokumentace pro KB
    - podpora komunikace v rámci systémů KB mezi jednotlivými rolemi
    - systém obsahující jednoduchou databázi aktiv a rizik
    - hlídání termínů pro splnění povinností dle nastaveného kalendáře pro povinné úkony
    - distribuce úkolů jednotlivým rolím, včetně zajištění auditní stopy
    - základní proces řešení kybernetické bezpečnostní události/incidentu
    - podpora práce řídícího výboru, vč. řízení úkolů, předání, jejich provedení, včetně zanechání auditní stopy
    - podpora kontroly a auditu
- Vzory základních dokumentů používaných v rámci systému
- Pokud nástroj DMS nebude k dispozici bude se řešit v rámci MS Teams/SharePoint MSDC.

V rámci implementace ISMS budou dodavatelem zpracovány příslušné dokumenty, které budou publikovány pro využití v rámci systému pro správu bezpečnostní dokumentace.

Celková implementace ISMS bude provedena v detailu touto veřejnou zakázkou, a to vlastní plněním:

- ISMS pro ZZ v popisovaných modelech v této zadávací dokumentaci.

Řešené oblasti výstupů implementace ISMS jsou prováděny v následujících dílčích krocích, které jsou rozpracovány v podřízených dokumentech systémových bezpečnostních politik. Výsledkem implementace je, že každá implementovaná organizace bude mít zpracovánu svou systémovou bezpečnostní politiku, která vychází ze systémové bezpečnostní politiky korporace *(pozn: tato korporátní bezpečnostní politika vzejde z implementace části - MSDC)* a může být upravena dle konkrétních postupů v oblasti řízení bezpečnosti informací ZZ. Uvedenými oblastmi jsou:

- klasifikace a řízení aktiv,
- hodnocení a řízení rizik,
- řízení provozu a komunikací,
- bezpečnost využívaných komunikačních sítí,
- detekce kybernetických bezpečnostních událostí,
- sběr a vyhodnocení kybernetických bezpečnostních událostí,
- zajištění úrovně dostupnosti,
- řízení přístupu,
- ochrana před škodlivým kódem,
- řízení technických zranitelností,
- bezpečné používání kryptografické ochrany,
- bezpečné používání mobilních zařízení,
- bezpečné předávání a výměna informací,
- zálohování a obnova,
- dlouhodobé ukládání a archivace informací,
- fyzická bezpečnost,
- bezpečnost lidských zdrojů,
- bezpečné chování uživatelů,
- GDPR, obecné nařízení o ochraně osobních údajů,
- poskytování a nabývání licencí programového vybavení a informací,

- akvizice, vývoj a údržba,
- řízení dodavatelů,
- případná interakce s NBÚ.

**Dále v rámci předmětu plnění jednotlivých oblastí jsou dodavatelem zpracovány tyto skupiny bezpečnostních opatření:**

- **Bezpečnostní politika -** definice základních pravidel bezpečnosti informací a vyjádření podpory ZZ.
- **Organizace bezpečnosti -** upřesnění struktury pro řízení bezpečnosti informací uvnitř ZZ a řízení bezpečnosti ve vztahu k externím subjektům (zákazníkům, dodavatelům atd.).
- **Řízení aktiv -** udržování přehledu o existujících aktivech organizace a stanovení odpovědnosti za udržování přiměřené míry ochrany jednotlivých aktiv.
- **Bezpečnost z hlediska lidských zdrojů -** vymezení povinností za ochranu informací u všech pracovníků a zajištění potřebného bezpečnostního povědomí.
- **Fyzická bezpečnost a bezpečnost prostředí -** definice pravidel pro přístup osob do klíčových prostor ZZ a ochrana zařízení zejména zařízení ICT (prostředí).
- **Řízení komunikací a řízení provozu -** zajištění spolehlivého a bezpečného chodu produkčních informačních a komunikačních systémů ZZ.
- **Řízení přístupu -** pravidla pro přidělování přístupu ke všem prostředkům informačních a komunikačních systémů, včetně sledování způsobu využívání dostupných prostředků.
- **Akvizice, vývoj a údržba informačních systémů -** prosazení principů bezpečnosti informací do projektů rozvoje ICT a dalších podpůrných aktivit.
- **Zvládání bezpečnostních incidentů** - pravidla a postupy určené pro řešení bezpečnostních incidentů včetně shromažďování potřebných důkazů.
- **Řízení kontinuity ICT činností -** stanovení politiky řízení kontinuity činností, havarijních plánů, včetně realizace opatření pro zvýšení odolnosti komunikačních systémů vůči kybernetickým bezpečnostním incidentům souvisejících s provozováním informačního a komunikačního systému a služeb s naplněním ZoKB v této oblasti.
- **Soulad s požadavky -** ZZ dokladuje naplnění požadavků vyplývajících z právních, smluvních a jiných závazků v oblasti ISMS a kybernetické bezpečnosti.

Základní implementace ISMS, ve lhůtě **3 měsíců** od nabytí účinnosti smluvního vztahu, je v rozsahu nutném pro zahájení poskytování služeb SOC. Tímto nutným rozsahem je míněna implementace základního minima pro oblast řešící reakce na bezpečnostní incidenty a bezpečnostní události. Zadavatel požaduje, že tato základní část bude implementována se zahájením poskytování služeb SOC.

Zadavatel rovněž požaduje, že z časového a obsahového pohledu bude implementace ISMS součástí detailního projektového plánu, jako součást prováděcího projektu.

## 6.2. Poskytování služeb SOC

### 6.2.1 Adaptační fáze

V rámci předmětu plnění dodavatel v adaptační fázi provede:

- **Prvotní analýzu** bezpečnostních hrozeb relevantních pro aplikace a služby provozované objednatelem.

- **Identifikaci zdrojů dat,** jejichž provozně bezpečnostní informace bude nutné, popř. vhodné sbírat, korelovat a analyzovat. Zdroje dat budou vybrány z tzv. primárních a podpůrných (technických) aktiv ZZ. Zejména se jedná o informační systémy základní služby. V současnosti není ZZ provozovatel významného informačního systému podle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 360/2020 Sb.
  Počet monitorovaných systémů, resp. jejich kategorizace se může po dobu poskytování služby změnit jak z podnětu dodavatele, tak zadavatele.

- **Návrh modifikace nastavení monitorovacích nástrojů,** včetně atributů a parametrů potřebných pro řádné a efektivní provozování dohledových nástrojů, 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 legovaných informací z dalších zdrojů pro zlepšení jejich relevantnosti či srozumitelnosti.

- **Vytvoření hardeningových bezpečnostních politik** včetně určení systémů, které budou předmětem. Obsahem těchto politik je stanovení pravidel pro konfiguraci aplikačního systémového prostředí, včetně provádění kontrolní činnosti a ověření shody. Součástí musí být popsaná množina systémů, kterou není možné harden-ovat a vynucovat u nich jejich kontrolu. Vyžadovaným principem je stanovení rozsahu automatizovaných kontrol, manuálního analytického a kontrolního přístupu včetně definice procesů pro udržování a aktualizaci politik.

- **Provedení prvotního skenu aktiv v rámci poskytovaných služeb vulnerability managementu -** služba prováděna SOC musí zajistit kontinuální výkonost pro skenování aktiv zadavatele definovaných danou sítí/sítěmi a zranitelnostmi relevantními pro daná aktiva. **Na začátku poskytování služby budou provedeny a vyhodnoceny plné skeny a dále vždy 1x měsíčně skeny rozdílové.** Plné skeny boudou rovněž provedeny při implementaci, upgrade, či update provozovaných ICT celků v reakci na požadavek zadavatele.

- **Návrh relevantních procesů vycházejících z jednotlivých modelů,** potřebných pro řádné a efektivní provozování centra kybernetické bezpečnosti (SOC), zahrnující mj. činnosti při zjištění bezpečnostního incidentu, výpadku či omezení dostupnosti vybraných informačních systémů, způsoby notifikace kompetentních osob objednatele (e-mail, SMS, telefon apod.) a seznam kompetentních osob zadavatele ve vazbě na základní fázi implementace ISMS.

- **Návrh vzorových reportů** (struktura) o událostech a incidentech v grafickém interaktivním zobrazení.

- **Podmínky implementace monitorovacích nástrojů** do prostředí ZZ

- **Všechny výše uvedené skutečnosti budou zahrnuty do hmotných výstupů služeb adaptační fáze, které budou tvořit v rámci Prováděcího projektu část popisující implementaci** a **podmínky implementace** a bude obsahovat mj.:
    - návrh detailní modifikace nastavení monitorovacích nástrojů,
    - scénáře pro řešení bezpečnostních a provozních incidentů a událostí s dodržením požadovaných SLA,
    - návrh vzorového reportu o událostech a incidentech.

- **Výstupem plnění adaptační fáze bude:**
    - vytvoření technických podmínek nezbytných pro řádné poskytování služby v provozní fázi včetně instalace potřebného HW a SW vybavení,
    - připojení monitorovacích nástrojů objednatele na SOC dodavatele,
    - nastavení relevantních procesů,
    - kategorizace událostí a incidentů a způsob reakce na tyto incidenty včetně definování jednotlivých SLA ve vazbě na zadané předpoklady,
    - vytvoření a předání implementační studie, včetně vzorového reportu o událostech a incidentech,
    - prvotní sken aktiv v rámci poskytovaných služeb vulnerability managementu
    - prezentace nastavení služby a výstupů adaptační fáze vybraným zaměstnancům ZZ, MSDC, popřípadě zástupcům zřizovatele MSK.
    - akceptační test, jehož účelem je otestování procesů zvládání kybernetických bezpečnostních incidentů s pomocí uměle vytvořeného nedestruktivního incidentu (výsledek akceptačního testu podmiňuje přechod do provozní fáze)

Výstupy adaptační fáze budou předloženy dodavatelem v **elektronické podobě** zadavateli a budou podléhat připomínkovacímu řízení a akceptaci. Po akceptaci zadavatel očekává konečný dokument v listinné podobě.

Adaptační fáze je provedena a ukončena ve lhůtě maximálně **4 měsíců** od nabytí účinnosti smluvního vztahu.

### 6.2.2 Provozní fáze

Dodavatel zajistí poskytované služby během provozní fáze centra kybernetické bezpečnosti od ukončení adaptační fáze dle specifikovaných podmínek v této zadávací dokumentaci.

## 7. Detailní specifikace zadání - definice požadovaných parametrů

V této části je uveden soubor všech požadavků na předmětné služby s technickou provázaností na podpůrné systémy. Zde jsou blíže **specifikovány minimální požadavky,** které je nutno dodržet za **všech ostatních uvedených podmínek** v zadávací dokumentaci. Takto specifikované požadavky představují **kompletní a současně minimální úroveň, kterou musí dodavatel splnit.**

Nutným předpokladem je, že všechna data budou dodavatelem 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/VDS, kterou zajistí do ZZ dodavatel za potřebné součinnosti MSDC a ZZ. Zabezpečení na straně dodavatele musí být na úrovní minimálně vyžadovaného vyhláškou o kybernetické bezpečnosti pro informační systémy základní služby. Na vyžádání (do 24 hodin od žádosti) musí dodavatel zadavateli umožnit kontrolu nastavení zabezpečení dat zadavatele v rámci SOC, i standardy zabezpečení samotného SOC pracoviště, a to buď přímo zadavatelem (MSDC) či jím pověřeným auditorem.

Dodavateli bude umožněno pro sběr informací instalovaní a připojení vlastních HW appliancí.

Poskytovateli, je umožněno uchovávat logy na svých zařízení po dobu nezbytně nutnou, maximálně po dobu **18 měsíců. V případě ukončení služby jsou danému zdravotnickému zařízení předány příslušné logy za posledních 18 měsíců (flow za 60 dnů až 18 měsíců dle nabídky dodavatele), či za celou dobu služby, pokud je ukončena za dobu kratší než 18 měsíců.**

**<u>Podmínky pro vyplnění tabulek</u>**

*Dodavatel potvrzuje úplné splnění podmínek, či požadavků, nebo parametrů předepsaných jako* ***ANO, a to včetně doplněného vysvětlení (je-li vysvětlení předepsáno zadavatelem).*** Specifikované podmínky a požadavky jsou vždy minimálními podmínkami, požadavky, funkcionalitami či vlastnostmi.

## 7.1. ISMS - detailní požadavky

### A. Podmínky a požadavky

| 1 | Podmínky a požadavky | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| 1. | **Implementovat systém řízení bezpečnosti informací ISMS v reflexi na popsané modely pro:**<br>• Zdravotnická záchranná služba Moravskoslezského kraje, p.o. | | ANO |
| 2. | **Ustanovení ISMS v ZZ**<br>• definice procesů a rozdělení kompetencí a odpovědnosti s vazbou na popsané modely<br>• definice rozsahu, hranic a vazeb ISMS<br>• definice převažujících procesů vyjádřených pomocí RACI matice<br>• definice a odsouhlasení Prohlášení o politice ISMS<br>• analýza a zvládání rizik<br>o definice přístupu organizace k hodnocení rizik<br>o ocenění aktiv do kategorií na základě úplného předloženého seznamu aktiv zadavatelem<br>o identifikace rizika včetně určení aktiv a jejich vlastníků<br>o analýza a vyhodnocení rizik<br>o stanovení kategorií a postupů eskalace ve vztahu ke kontaktování a souhlasu IT administrátora dotčeného subjektu<br>o identifikace a ohodnocení variant pro zvládání rizik<br>o výběr cílů opatření a jednotlivých opatření pro zvládání rizik<br>o souhlas vedení ZZ s navrhovanými zbytkovými riziky a se zavedením ISMS<br>• prohlášení o aplikovatelnosti | | ANO |
| 3. | **Zavedení ISMS**<br>• formulace dokumentu plánu zvládání rizik a jeho zavedení<br>• zavedení formou řídících aktů plánovaných bezpečnostních opatření a formulace příručky bezpečnosti informací, která upřesní pravidla a postupy aplikovaných opatření v definovaných oblastech bezpečnosti informací (ISO/IEC 27002)<br>• definice programu pro budování bezpečnostního povědomí a zaškolení všech uživatelů, manažerů a odborných pracovníků z úseku informatiky a zejména z oblasti řízení bezpečnosti informací<br>• upřesnění způsobů měření účinnosti bezpečnostních opatření a sledování stanovených ukazatelů<br>• zavedení postupů a dalších opatření pro rychlou detekci a reakci na bezpečnostní incidenty<br>• řízení zdrojů, dokumentů a záznamů ISMS | | ANO |
| 4. | **Školení zaměstnanců v oblasti ISMS**<br>realizace školení směřující ke zvýšení bezpečnostního povědomí všech zaměstnanců dotčených systémem řízení bezpečnosti informací. | | ANO |

| | Podmínky a požadavky | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| | Školení musí být periodické, musí být vyhodnocováno a přizpůsobováno kategorii zaměstnanců. Školení musí být relevantní k aktuálním hrozbám a trendům. Školení je možné provádět kombinovanou podobou s využitím učeben (zajistí ZZ), dálkového vzdělávání, webových nástrojů, samovzdělávacích kurzů atd. V rámci školení musí být vytvořeny a předány školící materiály. Školení musí dále obsahovat potřebnou administrativu, která zahrnuje pozvánky, prezenční listiny, přezkoušení, potvrzení o absolvování školení atd. | | |
| 5. | **Monitorování a přezkoumání ISMS**<br><br>• v pravidelných intervalech monitorovat a ověřovat účinnost prosazení bezpečnostních opatření<br>• provést interní audity ISMS, jejichž náplň pokryje celý rozsah ISMS<br>• připravit auditní zprávu o stavu ISMS a na jejím základě lze přehodnotit ISMS na úrovni vedení ZZ (včetně revize zbytkových a akceptovaných rizik) | | ANO |
| 6. | **Oblasti výstupů implementace ISMS**<br><br>• Klasifikace a řízení aktiv<br>• Hodnocení a řízení rizik<br>• Řízení provozu a komunikací<br>• Bezpečnost využívaných komunikačních sítí<br>• Detekce kybernetických bezpečnostních událostí<br>• Sběr a vyhodnocení kybernetických bezpečnostních událostí<br>• Zajištění úrovně dostupnosti<br>• Řízení přístupu<br>• Ochrana před škodlivým kódem<br>• Řízení technických zranitelností<br>• Bezpečné používání kryptografické ochrany<br>• Bezpečné používání mobilních zařízení<br>• Bezpečné předávání a výměna informací<br>• Zálohování a obnova<br>• Dlouhodobé ukládání a archivace informací<br>• Fyzická bezpečnost<br>• Bezpečnost lidských zdrojů<br>• Bezpečné chování uživatelů<br>• GDPR, obecné nařízení o ochraně osobních údajů<br>• Poskytování a nabývání licencí programového vybavení a informací<br>• Akvizice, vývoj a údržba<br>• Řízení dodavatelů<br>• Případná interakce s NBÚ | | ANO |
| 7. | **Zpracování skupin bezpečnostních opatření v rámci popsaných modelů**<br><br>• **Bezpečnostní politika -** definice základních pravidel bezpečnosti informací a vyjádření podpory vedením ZZ<br>• **Organizace bezpečnosti -** upřesnění struktury pro řízení bezpečnosti informací uvnitř zdravotnického zařízení a řízení bezpečnosti ve vztahu k externím subjektům (zákazníkům, dodavatelům atd.).<br>• **Řízení aktiv -** udržování přehledu o existujících aktivech organizace a | | ANO |

| | Podmínky a požadavky | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| | stanovení odpovědnosti za udržování přiměřené míry ochrany jednotlivých aktiv.<br>• **Bezpečnost z hlediska lidských zdrojů** - vymezení povinností za ochranu informací u všech pracovníků a zajištění potřebného bezpečnostního povědomí.<br>• **Fyzická bezpečnost a bezpečnost prostředí -** definice pravidel pro přístup osob do klíčových prostor ZZ a ochrana zařízení zejména zařízení ICT (prostředí).<br>• **Řízení komunikací a řízení provozu -** zajištění spolehlivého a bezpečného chodu produkčních informačních a komunikačních systémů ZZ.<br>• **Řízení přístupu -** pravidla pro přidělování přístupu ke všem prostředkům informačních a komunikačních systémů, včetně sledování způsobu využívání dostupných prostředků.<br>• **Akvizice, vývoj a údržba informačních systémů -** prosazení principů bezpečnosti informací do projektů rozvoje ICT a dalších podpůrných aktivit.<br>• **Zvládání bezpečnostních incidentů -** pravidla a postupy určené pro řešení bezpečnostních incidentů včetně shromažďování potřebných důkazů.<br>• **Řízení kontinuity činností -** stanovení politiky řízení kontinuity činností, havarijních plánů, včetně realizace opatření pro zvýšení odolnosti komunikačních systémů vůči kybernetickým bezpečnostním incidentům souvisejících s provozováním informačního a komunikačního systému a služeb s naplněním ZoKB v této oblasti.<br>• **Soulad s požadavky -** ZZ dokladuje naplnění požadavků vyplývajících z právních, smluvních a jiných závazků. | | |
| 8. | **Životní cyklus správy bezpečnostní dokumentace:**<br>• zpracování, publikace a zajištění celého životního cyklu bezpečnostní dokumentace tak, aby splnila minimálně legislativní požadavky spojené s provozem systémů základní služby.<br>• zpracování vzorové dokumentace pro kybernetickou bezpečnost,<br>• zpracování základního procesu pro řešení kybernetické bezpečnostní události/incidentu včetně formuláře pro reporting NÚKIBu a rozdělování úkolů podle nastavení incident response,<br>• zpracování vzorových dokumentů pro podporu kontroly a auditu, | | ANO |

## 7.2. Služby centra kybernetické bezpečnosti - detailní požadavky

### B. Podmínky pro instalaci hardwarových appliancí

Zadavatel požaduje, aby dodavatel v rámci požadované služby buď implementoval hardwarovou appliance do infrastruktury ZZ, nebo využil příslušné současně provozované technologické celky. Vždy však zvolené řešení nesmí nijak omezit jakýkoliv provoz na infrastruktuře ZZ.

Současně zvolené řešení nesmí být původem z nepřátelských zemí, nebo ze zemí které jsou ve válečném stavu, a to dle následujících podmínek.

Zadavatel upřesňuje, že zvolené řešení nesmí být původem z nepřátelských zemí nebo zemí, které jsou ve válečném stavu vůči ČR potažmo EU. Konkrétně se jedná o Rusko, vůči kterému bylo vydáno také varování od NÚKIB před hrozbou v oblasti kybernetické bezpečnosti spočívající v nedodržení smluvních závazků ze strany dodavatelů ICT služeb a produktů s významným vztahem k Ruské federaci (číslo jednací 3381/2022-NÚKIB-E/350 ze dne 21. 3. 2022).

Zadavatel rovněž upozorňuje, že v případě uzavření smlouvy se zadavatelem platby poskytované zadavatelem v souvislosti s realizací veřejné zakázky nemohou být poskytnuty přímo nebo nepřímo ani jen zčásti osobám, vůči kterým platí tzv. individuální finanční sankce ve smyslu čl. 2 odst. 2 Nařízení Rady (EU) č. 208/2014 ze dne 5. 3. 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině a Nařízení Rady (ES) č. 765/2006 ze dne 18. 5. 2006 o omezujících opatřeních vůči prezidentu Lukašenkovi a některým představitelům Běloruska a které jsou uvedeny na tzv. sankčních seznamech (dle příloh č. 1 obou nařízení).[4]

Dále zadavatel požaduje, aby v případě technického řešení využívající hardwarových appliance bylo hardwarem využito maximálně 2U prostoru (MSDC může odsouhlasit opodstatněné navýšení). Pokud bude nutno, aby na takto implementovaném řešení běžely níže specifikované bezpečnostní systémy, pak musí být v provedení Virtual appliance, které ve spolupráci se službou centra kybernetické bezpečnosti budou tvořit ucelené řešení nabízené služby.

Pro kompletní upřesnění zadavatel uvádí, že hardwarová appliance bude dodána jako součást služby a po jejím ukončení nezůstane ve vlastnictví zadavatele.

**Podmínky pro vyplnění tabulek**

*Dodavatel potvrzuje úplné splnění podmínek, čí požadavků, nebo parametrů předepsaných jako* ***ANO, a to včetně doplněného vysvětlení (je-li vysvětlení předepsáno zadavatelem).*** Specifikované podmínky a požadavky jsou vždy minimálními podmínkami, požadavky, funkcionalitami či vlastnostmi.

| 1 | Podmínky a požadavky | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| 9. | **Šasi hardwarových appliance**<br>Umístitelná do rozvaděče 19 palců o maximální velikosti 2U v rámci jednoho ZZ. | Nabízené řešení využívá pro vysokou dostupnost dva fyzické 1U servery instalované v ZZ. | ANO |
| 10 | **Napájecí zdroj**<br>Jednotlivé hardwarové appliance musí být osazeny párem redundantních „hot swap“ zdrojů 230 V | HW appliance obsahují redundantní napájení. | ANO |
| 11 | **Síťové rozhraní**<br>Instalovaná hardwarová aplliance splňuje podmínky pro připojení do síťové infrastruktury, tedy nevyžaduje jiné než v uvedeném rozsahu zde specifikované rozhraní. K dispozici jsou následující počty a typy síťových portů:<br>• 2ks 1Gbit/s (RJ45) portů<br>• 2ks 10Gbit/s SFP+ portů<br>• 2ks 10Gbit/s metalických portů<br>• 1ks servisního LAN portu | Nabízené HW appliance obsahují tato rozhraní:<br>2ks 10Gbit/s SFP+ port<br>2ks 10Gbit/s metalický port<br>1ks servisního LAN portu | ANO |

## C. Bezpečnostní monitoring a analýza síťového provozu

**Podmínky pro vyplnění tabulek**

*Dodavatel potvrzuje úplné splnění podmínek, či požadavků, nebo parametrů předepsaných jako* ***ANO, či doplněné o vysvětlení.*** Specifikované podmínky a požadavky jsou vždy minimálními podmínkami, požadavky, funkcionalitami či vlastnostmi.

| | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| **Obecné požadavky** | | | |
| 12. | **Systém pro analýzu síťového provozu**<br>SOC musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění.<br>Všechny komponenty systému musí být provozované na hardwarových (virtuálních) | Součástí služby bude dodávka 1 ks senzoru a 1 ks kolektoru GreyCortex do lokality IBC s dostatečnou kapacitou pro centrální sběr dat. Senzor bude instalován na dodávaných HW | ANO |

[4] Aktuální seznam lze nalézt např. zde: https://www.financnianalytickyurad.cz/blog/rusko-a-belorusko-seznam-sankcionovanych-subjektu

| 1 | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| | appliancích, která budou zapojena do prostředí ZZ („on premise“). | appliancích včetně redundantního připojení kolektoru do LAN sítě. Dále bude provozován 1 ks virtuálního senzoru na HW ředitelství ZZ | |
| 13. | **Analýza plného síťového provozu**<br>SOC musí analyzovat síť na základě zrcadleného síťového provozu (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti. Uvedené je vztaženo, jak k provozu na perimetru, tak k interní síti.<br>Systém sběru dat musí být zcela pasivní vzhledem k monitorovanému provozu, monitorovaný provoz přes něj neprochází. | Řešení GreyCortex analyzuje síť na základě zrcadleného síťového provozu a je zcela pasivní. | ANO |
| 14. | **Analýza protokolů typu NetFlow**<br>SOC musí analyzovat síť na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších. | | ANO |
| 15. | **Ukládání síťových toků**<br>SOC musí zajistit ukládání síťových toků ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku.<br>Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, POP3, IMAP, SSH, LDAP, KERBEROS, SNMP, CIFS, SMTPS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, SSL/TLS zapouzdření. | Služba SOC365 zajistí ukládání toků ve formátech, které umožní analýzu síťové komunikace dle uvedených požadavků. | ANO |
| 16. | **Uchování a vyhledávání síťových toků**<br>Je požadováno uchování datových toků na dobu minimálně 60 dnů.<br>Dále je požadováno, aby SOC umožnilo přístup k uchovaným datům administrátorům organizací a manažerovi KB, aby mohli v reálném čase volně filtrovat a vyhledávat v plné historii uložených síťových toků, dat a agregovaných síťových statistik na základě minimálně těchto parametrů: IP a MAC adresa, hostname, username, příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (klient nebo server), číslo portu, VLÁN, země, ASN. | Řešení služby SOC365 zajistí uložení datových toků minimálně na dobu 60dnů včetně přístupu k uchovaným datům, aby bylo možné v reálném čase volně filtrovat a vyhledávat v plné historii uložených síťových toků, dat a agregovaných síťových statistik na základě požadovaných parametrů | ANO |
| 171 | **Automatická detekce důležitých systémů**<br>Je požadováno, aby SOC zjistilo automatickou detekci přítomnosti klíčových služeb monitorované infrastruktury, jako jsou doménové řadiče, webové, emailové a databázové služby apod.<br>SOC musí být schopno upozornit na vznik nových služeb v interní síti a sledovat jejich změny, a to minimálně v rozsahu následujících služeb: DHCP, DNS, MS Active Directory služby, HTTP, HTTPS, SMTP, POP3, IMAP, SSH, CIFS, SMTPS, POP3S, IMAPS, MSSQL, TELNET, FTP, TFTP, a to i v případě, že nebude využíváno standardních „well known“ portů. | | ANO |
| **Požadavky na schopnost detekce bezpečnostních událostí** | | | |
| 18. | **Monitorování zařízení, segmentů sítě a využívaných síťových služeb**<br>SOC musí být schopno identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti - minimálně:<br>• změna IP/MAC adresy hosta,<br>• duplicitní IP/MAC adresa,<br>• změna VLÁN, | Služba SOC365 umožní pomocí uvedených detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení. V případě porušení požadovaných politik bude reagováno upozorněním. | ANO |

| 1 | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| | • vytvoření nové podsítě,<br>• připojení nového zařízení,<br>• použití nové služby,<br>• nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení,<br>• přístup nového zařízení ke službě či zařízení.<br><br>SOC musí uživatelům umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním. | | |
| 19. | **Detekce síťových služeb**<br>SOC musí být schopno detekovat síťové služby na základě síťových metadat získaných prostřednictvím DPI (Deep Packet Inspection), nikoliv pouze čísla portu. | Služba SOC365 je schopna detekovat síťové služby na základě síťových metadat získaných prostřednictvím DPI. | ANO |
| 20. | **Detekce Indikátorů kompromitace**<br>SOC musí být schopno detekovat Indikátory Kompromitace (tzv. IoC) pro ZZ. | Služba SOC365 je schopna detekovat IoC pro ZZ. | ANO |
| 21. | **Samostatné učení behaviorálních aktivit a detekce anomálií**<br>SOC musí využívat systému behaviorální analýzy a detekce anomálií. Předpokladem je, že bude používáno matematických metod samostatného učení pro analýzu síťové aktivity, bude vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci ZZ.<br>SOC tak musí mít schopnost na základě modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména:<br>• odchylku od modelu pro přenos dat, toků a paketů,<br>• odchylku od modelu pro počet komunikačních partnerů a entropie na komunikačních portech,<br>• odchylku od modelu pro počet síťových toků a využitých síťových služeb,<br>• odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).<br>Podmínkou je, že samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy. | Služba SOC365 pracuje zcela standardně s NBA na základě, kterého je možné identifikovat nestandardní síťové chování dle uváděných požadavků. | ANO |
| 22. | **Identifikace neznámých hrozeb, podezřelých chování na síti a porušení politik**<br>SOC musí být schopno detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod.<br>Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování:<br>• průzkumné aktivity v síti,<br>• potenciální úniky dat,<br>• detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě,<br>• detekce repetitivních vzorců chování na síti,<br>• detekce botnetů a ovládání kompromitované stanice,<br>• detekce příznaků těžení kryptoměn,<br>• útoky hrubou silou a enumerace dat,<br>rozpoznání tunelovaného síťového provozu - alespoň IPv4 prostřednictvím IPv6 a DNS tunely. | Služba SOC365 zajišťuje identifikaci neznámých hrozeb. | ANO |

| 1 | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| 23. | **Detekce na základě databáze známých hrozeb (signaturní detekce)**<br>SOC musí být schopno identifikovat a reportovat události na základě detekční databáze malware, známých útoků a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik. Základní požadavek je, že tato databáze musí být aktualizovaná minimálně na hodinové bázi. Nesmí se jednat o volně dostupnou/open-source databázi, ale musí se jednat o komerční databázi výrobce nebo poskytovatele těchto služeb.<br>Služba SOC pracující na základě databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7.<br>Dále musí využívat signaturní detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace.<br>SOC musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc) a musí být schopno přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu. | Služba SOC365 zajišťuje kompletně uvedené požadavky, a to včetně přidávání vlastních detekčních pravidel v praktickém a obecně využívaném formátu. | ANO |
| 24. | **Detekce přenosu škodlivých souborů**<br>SOC musí být schopno v monitorovaném provozu porovnávat hash zachycených souborů s databázemi známých hashů škodlivých souborů. | | ANO |
| 25. | **Analýza šifrované komunikace**<br>SOC musí být schopno zajistit analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb. | | ANO |
| 26. | **Kontrola platnosti certifikátů**<br>SOC musí mít schopnost ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení. | | ANO |
| 27. | **Asistované učení a korelace událostí**<br>SOC musí být schopno zajistit korelace jakýchkoliv detekovaných událostí ze všech detekčních metod a úpravy samostatného učení a dalších detekčních metod tak, aby byly v maximální míře eliminovány falešné alarmy. SOC musí být schopno eliminovat falešné alarmy i pro události detekované v historii.<br>SOC musí mít schopnost vedení zařízení podle souhrnné kritičnosti identifikovaných událostí - minimálně v rozsahu kritické, důležité a střední. | Služba zajišťuje korelaci detekovaných událostí s cílem eliminovat falešné alarmy včetně vedení jednotlivých zařízení podle úrovně kritičnosti. | ANO |
| 28. | **Aktuální databáze blacklistů**<br>SOC musí být schopno vyhodnocovat IP adresy, se kterými komunikují vnitřní hosté v sítí prostřednictvím minimálně denně aktualizovaných reputačních databází s možností přidání vlastní reputační databáze. | | ANO |
| **Požadavky na zajištění sítové viditelnosti** | | | |
| 29. | **Vyhledávání, filtrování a vizualizace všech dat**<br>SOC musí být schopno zajistit okamžité vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka a bez hlubokých znalostí konkrétních komunikačních protokolů. | | ANO |
| 30. | **Ukládání a vyhledávání aplikačních metadat**<br>SOC musí být schopno ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou | | ANO |

| 1 | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| | být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, MS-SQL, SIP, Kerberos, SSL/TLS, ARP, MODBUS.<br>V rámci metadat u HTTP, SMTP, SMB a NFS je požadováno ukládání informací o po síti přenášených souborech alespoň v rozsahu:<br>• název souboru,<br>• velikost souboru,<br>• HASH souboru. | | |
| 31. | **Kontextuální informace**<br>SOC musí být schopno pro každé zařízení získávat, vizualizovat a integrovat v jednotném grafickém rozhraní kontextuální informace:<br>• Jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně její historie<br>• Hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu<br>• IP geolokace<br>• IP reputace, vč. údaje, jestli je IP adresa blacklistovaná nebo podezřelá<br>• Historie použitých MAC adresa a výrobce zařízení<br>• Operační systém a jeho historie na zařízení<br>• Uživatelem zadané poznámky a informace k zařízení | | ANO |
| 32. | **Monitoring výkonu aplikací a sítě**<br>SOC musí v celé monitorované síti, mezi všemi zařízeními a na všech službách měřit a vytvářet automaticky (bez nutnosti nastavovat manuálně limitní hodnoty nebo jiné parametry) model normálního chování pro výkonnostní parametry minimálně:<br>• přenosová rychlost sítě,<br>• rychlost odezvy aplikace,<br>• odezva systému z pohledu uživatele,<br>• informace o retransmission a out of order paketech.<br>Výkonnostní anomálie na jednotlivých zařízeních a jejich službách jsou reportovány uživateli. | | ANO |
| 33. | **Zaznamenávání a ukládání**<br>SOC musí být schopno zajistit volitelné nahrávání plného síťového provozu (full packet capture) na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. | | ANO |

**D. Požadavky na procesní zpracování kybernetických událostí**

**Podmínky pro vyplnění tabulek**

*Dodavatel potvrzuje úplné splnění podmínek, či požadavků, nebo parametrů předepsaných jako **ANO, a to včetně doplněného vysvětlení (je-li vysvětlení předepsáno zadavatelem).** Specifikované podmínky a požadavky jsou vždy minimálními podmínkami, požadavky, funkcionalitami či vlastnostmi.*

| 1 | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| 34. | **Procesní zpracování**<br>SOC musí využívat federalizovaného, nebo centralizovaného řešení, které bude v rámci poskytovaných služeb nabízet jednak centrální přehled o incidentech a alertech a bude vytvářet podmínky, kdy v případě výskytu incidentu na ZZ bude procesně zajištěn synergický přístup pro realizaci preventivních opatření ve všech ostatních zapojených subjektech také z prvního zadávacího řízení (Řešení kybernetické bezpečnosti v nemocnicích MSK) | Služba SOC365 využívá centralizované řešení, preventivní opatření a jsou aplikována napříč všech ostatních zapojených subjektech. | ANO |
| 35. | **Management bezpečnostních událostí a incidentů**<br>SOC musí být schopno zajistit integrované rozhraní pro:<br>• reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident),<br>• spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele,<br>• jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů,<br>• možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.). | Služba SOC365 využívá ticketovací systém, který plně splňuje dané požadavky. | ANO |

**E. Požadavky na integraci, reporting a alerting**

**<u>Podmínky pro vyplnění tabulek</u>**

*Dodavatel potvrzuje úplné splnění podmínek, či požadavků, nebo parametrů předepsaných jako **ANO, či doplněné o vysvětlení.** Specifikované podmínky a požadavky jsou vždy minimálními podmínkami, požadavky, funkcionalitami či vlastnostmi.*

| 1 | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO/NE |
|---|---|---|---|
| 36. | **Integrace**<br><br>SOC musí být schopno operativní integrace s nástroji třetích stran:<br>• nástrojem typu SIEM prostřednictvím minimálně syslog, CEF a LEEF,<br>• nástroji pro generování nebo zpracování síťových statistik ve formátu IPFIX/NetFlow, včetně možnosti filtrovat IPFIX/NetFlow exportované statistiky dle všech filtrovaných parametrů jako výše,<br>• s dalšími nástroji prostřednictvím okamžitě definovatelných a jednoduše použitelných odkazů (URL) na požadované pohledy v nástroji. | Služba SOC365 je schopna zajistit sjednocení bezpečnostních nástrojů třetích stran, pomocí BI nástroje, který poskytuje možnost rychle filtrovat požadované informace.<br><br>Účastník potvrzuje, že „Služba SOC365 je schopna operativní integrace s nástroji třetích stran:<br>- Nástrojem typu SIEM prostřednictvím minimálně syslog, CEF a LEEF,<br>- Nástroji pro generování nebo zpracování síťových statistik ve formátu IPFIX/NetFlow, včetně možnosti filtrovat IPFIX/NetFlow | ANO |

| 1 | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO/NE |
|---|---|---|---|
| | | exportované statistiky dle všech filtrovaných parametrů jako výše,<br>- S dalšími nástroji prostřednictvím okamžitě definovatelných a jednoduše použitelných odkazů (URL) na požadované pohledy v nástroji“ | |
| 37. | **Automatické bezpečnostní hlášení (alerty)**<br><br>SOC musí být schopno zajistit upozornění prostřednictvím minimálně emailu a logu o:<br>• všech identifikovaných událostech,<br>• událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.<br>Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní aplikace. | Služba SOC365 zajišťuje upozornění o alertech, pomocí ticketovacího systému.<br><br>Účastník potvrzuje, že „Služba SOC365 je schopna zajistit upozornění prostřednictvím minimálně emailu a logu o:<br>- Všech identifikovaných událostech,<br>- Událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události,<br>země, uživatele, síťové služby, čísla portu, provozu do/z internetu.<br>Tyto aletry je služba schopna dodávat i ve strojově čitelném formátu pro využití v nástrojích typu SIEM a obsahuje minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní aplikace.“ | ANO |
| 38. | **Možnost automatizovaného reportingu**<br><br>SOC musí zajisti vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu správy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.).<br>Je požadováno vytváření reportů v českém jazyce. | Služba SOC365 vytváří reporty, založené na manažerském shrnutí s podrobnější technickou částí v českém jazyce. | ANO |

**F. Technická specifikace - bezpečnostního nástroje SIEM, Vulnerability management**

**<u>Podmínky pro vyplnění tabulek</u>**

*Dodavatel potvrzuje úplné splnění podmínek, či požadavků, nebo parametrů předepsaných jako* ***ANO, a to včetně doplněného vysvětlení (je-li vysvětlení předepsáno zadavatelem).*** Specifikované podmínky a požadavky jsou vždy minimálními podmínkami, požadavky, funkcionalitami či vlastnostmi.

| | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| **Obecné požadavky** | | | |
| 39. | **Systém pro sběr, analýzu a korelaci**<br><br>SOC musí využívat systém pro sběr, analýzu a korelaci logů napříč všemi monitorovanými zdroji s | Jedná se o základní funkcionalitu použitého nástroje SIEM. | ANO |

| 1 | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| | možností napojit přímo i nepodporovaný zdroj pomoci standartních protokolů. | | |
| 40. | **Skenování zařízení**<br><br>SOC musí zajistit aktivní a pasivní skenování zařízení v definovaných IP rozsazích pro zjišťování nových a neznámých zařízení v sítí (asset discovery). | Aktivní skenování bude prováděno nástrojem pro skenování zranitelností. Pasivní skenování zařízení bude prováděno přímo nástrojem pro skenování síťového provozu. | ANO |
| 41. | **Operační systémy**<br><br>SOC musí být schopno zajišťovat skenování zranitelností u podporovaných zdrojů (minimálně Windows/Linux), a to ne pouze na bázi open source zdrojů zranitelností, ale na bázi placených databází zranitelností. | Součástí nabízené služby SOC je skenování zranitelností komerčním nástrojem.<br><br>Účastník potvrzuje, že při realizaci veřejné zakázky bude využívána báze placených databází zranitelností.<br>Pro tyto účely využíváme technologii Greenbone a AlienVault a tyto placené databáze zranitelností jsou vždy v rámci pravidelně placených podpor výrobce. Pro vyloučení všech pochybností Účastník uvádí, že nabídka<br>je postavena na SIEM nástroji s názvem ELISA Security Manager. | ANO |
| 42. | **Network IDS**<br><br>SOC musí zajistit vyhodnocování systémů Network IDS (Výkon min. 500 Mbps pro ZZ), Host IDS a dále také Filé Integrity Monitoring. | Nabízený network IDS nástroj je dimenzován na kapacitu min. 500Mbps pro ZZ. Funkcionalitu host IDS a FIM poskytuje nástroj SIEM. | ANO |
| 43. | **Základní analýza datových toků**<br><br>SOC musí zajistit základní analýzu datových toků podporovaných síťových zařízení. | Služba SOC365 zajistí základní analýzu datových toků podporovaných síťových zařízení. | ANO |
| 44. | **Kontrola dostupnosti**<br><br>SOC musí zajistit kontrolu dostupnosti služeb u podporovaných operačních systémů (minimálně Windows/Linux). | Jedná se o základní funkcionalitu použitého nástroje SIEM. | ANO |
| 45. | **Notifikace**<br><br>SOC musí umožňovat na základě vytvořených korelačních událostí vytvářet:<br>- alerty,<br>- mailové notifikace,<br>- spouštět skripty. | Jedná se o základní funkcionalitu použitého nástroje SIEM. | ANO |
| 46. | **Provoz řešení**<br><br>Řešení musí v ceně služeb zahrnovat veškeré náklady spojené s provozem celého SOC. | Potvrzujeme. | ANO |
| **Požadavky na výkon SIEM pro ZZ** | | | |
| 47. | **Sbírané události**<br><br>Systém sběru dat pro SIEM musí umožnit sbírat události v min. výkonu 1000 EPS, dodavatel zajistí dostatečný výkon pro potřeby daného zdravotnického zařízení. | Nástroj SIEM bude provozován autonomně v ZZ a HW appliance je výkonově i kapacitně dimenzován na požadovaný výkon. | ANO |
| 48. | **Korelace událostí** | Nástroj SIEM bude provozován autonomně v ZZ a HW appliance je | ANO |

| 1 | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| | Systém korelace dat pro SOC musí umožnit korelaci událostí v min. výkonu 1000 EPS. | výkonově i kapacitně dimenzován na požadovaný výkon. | |
| 49. | **Zdroje logů**<br><br>Systém SOC musí umožňovat napojení min. 150 zdrojů logů současně přičemž tyto zdroje se můžou vyskytovat v různých lokalitách/pobočkách | Pokryto po licenční i výkonové stránce. | ANO |
| 50. | **Network IDS**<br><br>SOC musí disponovat systémem zajišťujícím sběr dat z Network IDS (Výkon min. 500 Mbps), Host IDS a dále také Filé Integrity Monitoring. | Nabízený network IDS nástroj je dimenzován na kapacitu min. 500 Mbps pro ZZ. Funkcionalitu host IDS a FIM poskytuje nástroj SIEM. | ANO |
| 51. | **Analýza datových toků**<br><br>SOC musí zajistit sběr dat pro umožnění analýzy datových toků poslaných do příslušného nástroje s min. výkonem 1Gbps provozu. | Služba SOC365 zajistí sběr dat pro umožnění analýzy datových toků poslaných do příslušného nástroje s výkonem 1Gbps. | ANO |
| **Požadavky na funkcionality SIEM** | | | |
| 52. | **Základní funkce**<br><br>SOC musí zajistit zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware a sledování síťových toků a detekce anomálií. | Jedná se o základní funkcionalitu použitého nástroje SIEM. Sledování síťových toků a detekci anomálií zajišťuje primárně nástroj pro analýzu síťového provozu. | ANO |
| 53. | **Ovládání**<br><br>SOC musí zajistit přístup systémovým IT administrátorům ZZ a manažerovi KB ke všem komponentám systému z jednotného grafického uživatelského rozhraní (GUI). Konfigurace, definice zdrojů logů, definice korelačních pravidel, tvorba reportů, řešení událostí a další běžné operace musí probíhat z jediné řídící konzole s jednotným GUI. | Nabízený nástroj SIEM poskytuje jednotné uživatelské rozhraní. | ANO |
| 54. | **Oblasti zajištění SIEM systémem SOC - správa prvků**<br><br>SOC musí využívat SIEM nástroj. Dále popsané bodu musí mít SOC zajištěny tímto systémem nebo zajištěnou integraci SIEM nástroje se specializovanými systémy. Dále jsou definovány oblasti pokrytí:<br>• Správa prvků<br>• Skupiny prvků<br>• Metadata prvků<br>• Monitorování prvků<br>• Vyhledávání prvků<br>• Detekce zranitelností<br>• Profily zranitelností<br>• Autentizované detekce zranitelnosti<br>• Detekce průniku (aktiva a síť)<br>• Detekce anomálií<br>• Sledování síťových toků - hypervisor<br>• Viditelnost síťového provozu<br>• Sledování IP reputace<br>• Ukládání logů<br>• Zpracování logů<br>• Prohledávání logů<br>• Expirace logů<br>• Zálohování logů<br>• Ochrana logů<br>• Centralizace logů<br>• Geolokace<br>• Doplňování názvů<br>• Grafy událostí<br>• Parsery<br>• Standardizace logů | Jedná se o funkcionality použitého nástroje SIEM. Sledování síťových toků, detekci průniku, detekci anomálií, viditelnost do síťového provozu, sledování IP reputace a geolokaci zajišťuje v nabízeném řešení primárně nástroj pro analýzu síťového provozu. | ANO |

| 1 | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| | • Dashboardy<br>• Reporty<br>• Upozornění<br>• Správa uživatelů<br>• Tickety<br>• Automatizace ticketů<br>• Politiky<br>• Korelace<br>• Rozšířené korelace<br>• Fultextové Vyhledávání<br>• Práce v souladu s platnou legislativou | | |
| 55. | **Provedení**<br><br>SOC bude využívat řešení SIEM v provedení Virtuální appliance nebo samostatné hardwarové appliance. | SIEM je v provedení virtuální appliance na dodávaném HW. | ANO |
| 56. | **Licence**<br><br>Licence SIEM používaných SOC v centrální lokalitě i v ZZ musí zahrnovat potřebné zdroje dat, operátory SOC, administrátory ZZ, manažera KB a auditora KB, tj. být pro min. počet připojených zdrojů (Prvků) bez licenčního omezení na velikosti aktivních i archivních dat či jiných funkcionalit systému. | Nejsou žádná kapacitní licenční omezení SIEM nástroje, vyjma počtu instalovaných agentů, kdy je Zadavatelem požadováno až 150 současně připojených zdrojů logů. | ANO |
| 57. | **Výkon** (pro ZZ)<br><br>Trvalé zpracování minimálně 1000 EPS (events per second - událostí za sekundu) | Nástroj SIEM bude provozován autonomně v každém ZZ a HW appliance je výkonově i kapacitně dimenzován na požadovaný výkon. | ANO |
| 58. | **Škálovatelnost**<br><br>V případě nedostatečné výkonnosti si SOC zajistí zvýšení výkonu doplněním dalších appliance pro sběr dat a vykovávání funkcí systémů, popřípadě rozdělením systému na více serverů. | Ano. Podporováno je horizontální i vertikální škálování výkonu. | ANO |
| 59. | **Integrace**<br><br>SOC zajistí možnost komunikace svých systémů se systémy třetích stran s využitím standardizované API, podpora skriptování.<br>Požadavkem je, aby popis standardizovaného API a podpory skriptování byl součástí přílohy nabídky. | Popis API a podpory skriptování je přílohou nabídky. | ANO |
| 60. | **Management aktiv**<br><br>SOC bude využívat systém managementu aktiv vč. uživatelsky definovaných parametrů a kategorií podle požadavků zadavatele. Aktiva musí být možno členit dle následujících parametrů:<br>- podle jejich důležitosti v procesech zadavatele,<br>- podle typu aktiva (doménový kontrolér, DNS server, koncové zařízení apod.),<br>- podle operačního systému,<br>- podle běžících služeb,<br>- podle zjištěných zranitelností. | Management aktiv je v SIEM nástroji obsažen. Podporuje kategorizaci aktiv dle požadovaných parametrů. | ANO |

## G. Technická specifikace služeb SOC - centrum pro řešení kybernetické bezpečnosti

Komplexní zajištění služeb centra pro řešení kybernetické bezpečnosti (SOC), především:

- formou služby provozovat centralizovanou správu, ukládání, vyhodnocování a korelaci log dat v nezměnitelné podobě z libovolných síťových aktivních prvků, operačních systémů a používaného aplikačního software, tj. nástroj SIEM. Implementace systému bude provedena v souladu s § 23 VoKB Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,

- formou služby provozovat centralizovanou správu, ukládání a vyhodnocování komunikačních spojení a výkonnostních parametrů datové sítě, tj. nástroj sběru a vyhodnocení síťového provozu. Implementace systému bude provedena v souladu s § 22 VoKB Nástroj pro detekci kybernetických bezpečnostních událostí.

**Podmínky pro vyplnění tabulek**

*Dodavatel potvrzuje úplné splnění podmínek, či požadavků, nebo parametrů předepsaných jako* ***ANO, a to včetně doplněného vysvětlení (je-li vysvětlení předepsáno zadavatelem).*** Specifikované podmínky a požadavky jsou vždy minimálními podmínkami, požadavky, funkcionalitami či vlastnostmi.

| | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| **Požadavky na služby SOC** | | | |
| 61. | Zadavatel požaduje realizaci uvedených úloh prostředky a technologiemi Dodavatele, nejméně v rozsahu řešení sběru síťového provozu a SIEM řešení, které budou provozovány na hardwarových appliancích. Tyto budou implementovány do prostředí ZZ a propojením se SOC budou tvořit ucelené řešení odpovídající veškerým požadavkům na službu centra pro řešení kybernetické bezpečnosti. | Služba SOC365 zajistí všechny uvedené požadavky a to tak, aby cele řešení se službou tvořilo ucelené řešení splňující všechny požadavky zadavatele. | ANO |
| 62. | Služba SOC musí být dostupná v českém jazyce, případně slovenském jazyce. | Služba SOC365 zaměstnává výhradně české, případně slovenské občany a dodržuje povinnosti vyplývající z českého práva. | ANO |
| 63. | Služba SOC musí být zajišťována z území EU, při dodržení povinností vyplývajících z českého práva. | Služba SOC365 je zajišťována z území ČR, konkrétně z: Řipská 1321/11c, 627 00 Brno | ANO |
| 64. | V rámci služby bude Dodavatelem služby vytvořeno bezpečné úložiště pro sdílení kompletních materiálů k poskytované službě. | Služba SOC365 využívá vlastní datové úložiště, kde jsou sdíleny materiály k poskytované službě. | ANO |
| 65. | **Síťový dohled**<br><br>Zajištění centralizované správy, ukládání a vyhodnocování komunikačních spojení a výkonnostních parametrů datové sítě. | Služba SOC365 zajišťuje centralizovanou správu, ukládání a vyhodnocování provozu pomocí monitorovacího nástroje. | ANO |
| 66. | **Bezpečnostní dohled**<br><br>Zajištění správy a provozu nástroje SIEM. | sTužba SOC365 zajistí správu a provoz nástroje SIEM. | ANO |
| 67. | **Incident management**<br><br>Zajištění operátorské činnosti, Incident handling, Incident Response. | Služba SOC365 zajistí Operátory SOC365. Incident handling a Incident Response jsou standartní součástí naší služby. | ANO |
| 68. | **Analýza incidentů**<br><br>Zajištění odborné činnosti v detekci a lokalizaci příčin incidentů analytikem incidentů ze strany Dodavatele služby. | V rámci služby je zajištěna odborná činnost analytika SOC365 při inspekci incidentů. | ANO |
| 69. | **Návrhy systematických opatření**<br><br>Sestavení opatření v organizační a technické úrovni pro posouzení Zadavatelem. | Služba SOC365 navrhuje opatření v organizační a technické úrovni. | ANO |
| 70. | **Návrhy řešení incidentů**<br><br>Zajištění odborné činnosti pro kategorizaci na interní a externí příčiny incidentů a k nim příslušných opatření. | Služba SOC365 poskytuje kategorizaci příčin incidentů a poskytuje návrhy příslušných opatření, jak | ANO |

| | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| | | incidentům předcházet. | |
| 71. | **Reporting a analýza stavů, událostí a incidentů**<br><br>Zajištění odborné činnosti pro doložení úrovně bezpečnosti vůči interním kontrolním procesům nebo pro doložení vůči externím kontrolním autoritám. | sTužba SOC365 zajišťuje odbornou činnost pro doložení úrovně bezpečnosti vůči interním kontrolním procesům i vůči externím kontrolním autoritám. | ANO |
| 72. | **Business Continuity**<br><br>Služba (včetně všech komponent, které využívá) musí být odolná proti výpadkům a poruchám. Všechny komponenty služby musí být schopny dlouhodobého provozu bez změny chování a úbytku výkonu. | Služba SOC365 je odolná proti výpadkům a poruchám pomocí záložních zdrojů energie i internetové konektivity. | ANO |
| 73. | **Zajištění souladu se ZoKB (Compliance)**<br><br>Všechny parametry služby musí zajistit na úrovni technologií i procesů splnění požadavků na zajištění potřebné míry informační bezpečnosti, zejména pak: Důvěrnost, Dostupnost, Nepopíratelnost, Autentizaci, Autorizaci. | Služba SOC365 je poskytována v souladu s ZoKB. | ANO |
| 74. | **Adaptace a akceptace sdílených procesů**<br><br>Služba zajistí úpravu procesů na straně dodavatele služby a návrh na jejich integraci s relevantními procesy na straně zadavatele. | Během adaptační fáze dojde k adaptaci a akceptaci sdílených procesů. | ANO |
| 75. | **SLA procesních vstupů a výstupů**<br><br>Služba zajistí monitoring procesů na straně Dodavatele služby i Zadavatele. | Služba SOC365 zajišťuje monitoring procesů na obou stranách. | ANO |
| | **Požadavky na personální zajištění SOC** | | |
| 76. | **Personální zajištění**<br><br>Poskytování služby bude zajištěno pracovníky s odbornou způsobilostí vyhovující požadavkům na zajištění kybernetické bezpečnosti v souladu s požadavky *zákona 181/2014 Sb. v* celém průběhu poskytované služby a všech jejích procesů a rutin v rámci požadovaných modelů. | Služba SOC365 zajistí pracovníky s odbornou způsobilostí vyhovující požadavkům na zajištění ZoKB. | ANO |
| 77. | **Zastoupení rolí s požadovanou odpovědností s vazbou na uvedené modely**<br><br>• Operátor SOC<br>• Analytik kybernetické bezpečnosti<br>• Forenzní analytik<br>• Bezpečnostní experti<br>• **Bezpečnostní specialista na hardening** | Služba SOC365 stejně zajistí všechny uvedené role. | ANO |
| 78. | **Ustanovení CSIRT - SOC** s přímým vztahem na Národní úřad pro kybernetickou a informační bezpečnost - Vládní ČERT ČR. | Tým SOC365 je veden jako člen CSIRT | ANO |
| | **Technické požadavky na SOC** | | |
| 79. | **Dodavatel služby provozuje vlastní *nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,*** který umožňuje napojení na nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí v rámci specifikovaného předmětu plnění. | Služba SOC365 provozuje vlastní nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí. | ANO |
| 80. | **V rámci služby Dodavatel zajistí *provozní monitoring* bezpečnostních nástrojů,** dle předmětu zakázky, v rozsahu:<br>• dostupnost a funkčnost bezpečnostních nástrojů, | Služba SOC365 poskytuje provozní monitoring bezpečnostních nástrojů. | ANO |

| | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| | • vytíženost bezpečnostních nástrojů,<br>• detekce vyčerpání kapacitních zdrojů u bezpečnostních nástrojů. | | |
| 81. | **V rámci služby Dodavatel zajišťuje nastavování bezpečnostních nástrojů, dle předmětu zakázky, v rozsahu:**<br>• úprava a optimalizace korelačních pravidel, dle požadavků Zadavatele nebo dle best practices Dodavatele,<br>• přidávání nových zařízení pro bezpečnostní monitoring,<br>• vytváření nových scénářů pro detekci,<br>• úprava nastavení nástrojů, dle požadavku Zadavatele nebo NÚKIB.<br><br>Pro některé úkony v rámci nastavování bezpečnostních nástrojů může být vyžadována součinnost MSDC (např. při napojování nových zdrojů logů). | sTužba SOC365 zajišťuje pravidelnou konfiguraci bezpečnostních nástrojů dle vlastních best practices a dle požadavků zákazníka nebo NÚKIB. | ANO |
| 82. | **Přístup administrátorů Dodavatele ke sledovaným parametrům** služby prostřednictvím grafického rozhraní (GUI - dashboard apod.), alespoň v režimu čtení nebo v přístupové roli Auditor. | Služba SOC365 zajistí přístupy, které budou zřízeny pro určené skupiny uživatelů. | ANO |
| **Požadavky - podpora SOC** | | | |
| 83. | **Ticketovací systém**<br><br>Služba s on-line přístupem pro kompletní správu požadavků, včetně uchování historie požadavků a jejich řešení. | Služba SOC365 provozuje ticketovací systém, který je dostupný online a obsahuje historii požadavků a jejich řešení. | ANO |
| 84. | **Přístup Zadavatele k podpoře provozu systémů -** Helpdesk. | | ANO |
| 85. | **Přístup Zadavatele k podpoře *Incident Response* -** Helpdesk, telefon/ email na členy CSIRT-SOC. | Komunikační matice obsahuje všechny důležité kontakty. | ANO |
| 86. | **Proaktivní komunikace,** zakládání tiketů a jejich řešení. Komunikace s třetí stranou jako NBÚ, NÚKIB, ČERT, kooperující CSIRT atd. | Služba SOC365 zakládá tikety a navrhuje řešení incidentů. | ANO |
| 87. | **Přístup administrátorů ZZ** ke sledovaným parametrům služby prostřednictvím grafického rozhraní (GUI - dashboard apod.), alespoň v režimu čtení nebo v přístupové roli Auditor. | STužba SOC365 zajistí přístupy určeným skupinám uživatelů. | ANO |
| 88. | **Notifikace/Eskalace**<br><br>Informování odpovědných osob zadavatele o vzniku bezpečnostního incidentu v reálném čase za pomocí základních komunikačních nástrojů (mail / SMS / telefon). | Služba SOC365 provádí Notifikace dle úrovně kritičnosti mailem, SMS nebo telefonicky. | ANO |
| 89. | **Vulnerability management**<br><br>• služba musí zajistit kontinuální skenování aktiv Zadavatele definovaných danou sítí/sítěmi a zranitelnostmi relevantními pro daná aktiva. Minimálně na začátku poskytování služby budou provedeny a vyhodnoceny plné skeny a dále vždy 1x měsíčně skeny rozdílové,<br>• plné skeny boudou rovněž provedeny při implementaci, upgrade, či update provozovaných ICT celků v reakci na požadavek Zadavatele. | Služba SOC365 zajistí VA sken, dle požadavků zadavatele, včetně vyhodnocení. | ANO |
| 90. | **Pravidelné reporty - Bezpečnostní zpráva**<br><br>Pravidelným požadovaným výstupem poskytovaných služeb je bezpečnostní zpráva, která bude zpracována vždy za měsíční sledované období. Předpokladem je, že | Služba SOC365 si naprosto zakládá na Bezpečnostní zprávě, která obsahuje všechny požadované náležitosti a je | ANO |

| | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| | bezpečnostní zpráva bude dostupná v grafickém interaktivním zobrazení.<br>Požadována je vzdálená prezentace bezpečnostní zprávy, např. formou videokonference v rozsahu min. 2hod.<br><br>Nutnou podmínkou je, že dodavatel v rámci prováděcího projektu rozpracuje v detailu nejvyšší granularity obsah prezentovaných hodnot a jejich závislostí v jednotlivých uvedených oblastech.<br><br>Minimální rozsah bezpečnostní zprávy:<br><br>- **Manažerský souhrn pro potřebu vrcholového vedení ZZ**<br>souhrnné manažerské shrnutí poskytovaných služeb pro ZZ včetně souhrnu bezpečnostních zjištění a návrh doporučených opatření pro další období pro zvýšení bezpečnosti, dostupnosti a prevenci eliminace incidentů v rozsahu max. 5 normovaných stran A4 pro ZZ.<br>- **Souhrnná technická zpráva obsahující** podrobný popis bezpečnostních incidentů, zjištění a evidence všech ticketů v následném požadovaném rozsahu:<br>o Monitorovaná zařízení včetně vydefinování neznámých zařízení v síti<br>o Evidované alerty - ve vhodné kategorizaci zachycují kompromitaci škodlivým kódem, riziko úspěšného zneužití, zranitelnosti nebo instalaci škodlivého kódu, probíhající útoky, potencionální skenovací aktivitu a anomálie v síti nebo porušení politik<br>o Analýza událostí ve formě souhrnné statistiky, povolené a zamítnuté komunikace na firewallu<br>o Neúspěšná přihlášení ve formě souhrnné statistiky neúspěšných přihlášení ve vazbě nejčastějších uživatelů neúspěšných přihlášení<br>o Úspěšná přihlášení, souhrnná statistika úspěšných přihlášení<br>o Anomálie síťového provozu, souhrnná statistika nejčastěji detekovaných anomálií v síťovém provozu<br>o Analýza příchozí komunikace do interní sítě, souhrnná analýza příchozí komunikace do interní sítě a nejčastějších zdrojů příchozí komunikace v závislosti na geolokaci<br>o Analýza odchozí komunikace z interní sítě, souhrnná analýza komunikace z interní sítě a nejčastějších cílů odchozí komunikace v závislosti na geolokaci<br>o Analýza komunikace v interní síti, souhrnná analýza komunikace se známými škodlivými adresami<br>o Analýza komunikace se známými škodlivými adresami, souhrnná analýza komunikace se známými škodlivými adresami a komunikace se známými škodlivými adresami v závislosti na geolokaci<br>o Vnější detekce zranitelnosti, souhrnná statistika scanu detekovaných zranitelností a příslušné počty zranitelnosti v jednotlivých úrovních rizika<br>o Popis vybraných vnějších zranitelností u hostů z nejvážnější zranitelnosti či největším množstvím zranitelností, včetně doporučení pro jejich odstranění<br>o Vnitřní detekce zranitelnosti, souhrnná statistika scanu detekovaných vnitřních zranitelností a příslušné počty zranitelnosti v jednotlivých úrovních rizika<br>o Popis vybraných vnitřních zranitelností, popis vybraných vnitřních zranitelnosti u hostů z nejvážnější zranitelnosti či největším | tvořena tak, aby jí rozuměli jak manažeři, tak technici zákazníka. | |

| | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| | množstvím zranitelností, včetně doporučení pro jejich odstranění | | |
| 91. | **Reporty - on-demand**<br><br>Služba zajistí na vyžádání provádění on-demand spouštění některých pravidel a z výstupu bude vytvářet grafické interaktivní reporty. | sTužba SOC365 poskytne na vyžádání provádění některých pravidel, jejichž výstupy bude možné sledovat v interaktivním grafickém rozhraní. | ANO |
| 92. | **Technologie sběru dat**<br><br>Služba zajistí zprovoznění nástrojů SIEM, sběru a vyhodnocení síťového provozu jako základních zdrojů dat a bude s nimi komunikovat průmyslově standardními protokoly.<br>Požadované architekturní řešení Dodavatele služby:<br>• zajištuje na straně Zadavatele sběr, přenos, uložení logů, jejich vyhodnocování a korelaci v rámci nástroje SIEM nasazeným v infrastruktuře Zadavatele. Případný SIEM Dodavatele služby plní pouze roli Federativní komponenty k výkonu Operátorské činnosti v rámci služby SOC,<br>• zajištuje na straně Zadavatele sběr a vyhodnocení síťového provozu v rámci nástroje nasazeného v infrastruktuře. | Služba SOC365 zajistí zprovoznění všech nástrojů včetně SIEM na základě požadované architektury a funkčnosti celku jako uceleného řešení. | ANO |
| 93. | **Base line analýza**<br><br>Služba zajistí porovnání neobvyklých počtů určitých událostí oproti jinému období z minulosti. | Base line analýza je součástí Bezpečnostní zprávy. | ANO |
| 94. | **Historická korelace**<br><br>Zajistí ověření nového korelačního pravidla proti historickým datům. | STužba SOC365 zajišťuje ověření nového korelačního pravidla proti historickým datům. | ANO |
| 95. | **Kategorizace aktiv**<br><br>Služba zajistí jednotnou evidenci a vyhodnocení kategorií aktiv. Podle těchto kategorií bude Dodavatel služby utvářet další pravidla nebo reporty v prostředcích zapojených subjektů. | Služba SOC365 zajišťuje evidenci a kategorizaci aktiv podle kterých vytváří další pravidla nebo reporty. | ANO |
| 96. | **Režim Maintenance**<br><br>Služba musí být schopna běhu v režimu údržby ohlášenou zapojeným subjektem, kdy se údržbou dotčených zdrojů/aktiv nebudou vyhlašovat alerty. | Služba SOC365 nebude hlásit alerty v případě ohlášené údržby. | ANO |
| 97. | **Služba Monitoringu a detekce**<br><br>• průběžné sledování provozu prostředí zadavatele,<br>• real-time analýza situace v napojených nástrojích podle skupin, kategorií zařízení a podle kontextu log záznamů nebo událostí.<br>• 3x denně odborné posouzení bezpečnostní situace a provozního stavu. V případě anomálie posouzení její relevance a závažnosti,<br>• posouzení kontextu anomálie a příčin vzniku situace s případnou eskalací problému Zadavatele na analytického specialistu Dodavatele služby. | Služba SOC365 poskytuje monitoring a detekci dle požadavků zadavatele, za pomoci operátorů a analytiků SOC. | ANO |

| | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| 98. | **Služba včasné výstrahy a reakce na nestandardní situace v provozu bezpečnostních systémů**<br><br>• zpracování analytických scénářů na aktuální kybernetické hrozby,<br>• posouzení eskalovaného problému Zadavatele analytikem, nebo expertem,<br>• detekce a vyhodnocení závažnosti identifikovaných anomálií,<br>• posouzení a případná eskalace nestandardní situace v provozu Zadavatele na službu včasné výstrahy a reakce na incident v rámci bezpečnostních struktur ČR. | Služba SOC365 poskytuje součinnost při zpracování analytických scénářů na aktuální kybernetické hrozby. Poskytuje službu analytika nebo experta v dohodnutém režimu a poskytuje součinnost při eskalaci.<br><br>Účastník potvrzuje, že „Služba SOC365 zajišťuje včasné výstrahy a reakce na nestandardní situace v provozu bezpečnostních systémů):<br>- „zpracování analytických scénářů na aktuální kybernetické hrozby,<br>- Posouzení eskalovaného problému Zadavatele analytikem, nebo expertem,<br>- Detekce a vyhodnocení závažnosti identifikovaných anomálií,<br>- Posouzení, případná eskalace nestandardní situace v provozu Zadavatele na službu včasné výstrahy a reakce na incident v rámci bezpečnostních struktur ČR.“ | ANO |
| **SLA** | | | |
| 99. | Dodavatel služby musí provozovat vlastní bezpečnostní dohledovou službu v režimu **24x7x365** na úrovni systémů, s nepřetržitou dostupností operátorů SOC a s minimální dostupností analytiků, forenzních analytiků a expertů, tak, aby plnil stanovená SLA pro detekci a reakci pro všechny kategorie incidentů. | Služba SOC365 provozuje vlastní bezpečnostní dohled v režimu 24x7x365 na úrovni systémů a nepřetržitou dostupností operátorů a s minimální dostupností analytiků, forenzních analytiků a expertů tak, aby byly splněny veškeré požadavky na SLA.<br><br>Účastník potvrzuje, že „Služba SOC365 provozuje vlastní | ANO |

| 1 | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| | | bezpečnostní dohledovou službu v režimu 24x7x365 na úrovni systémů, s nepřetržitou dostupností operátorů SOC a s minimální dostupností analytiků, forenzních analytiků a expertů, tak, aby plnil stanovená SLA pro detekci a reakci pro všechny kategorie incidentů. | |
| 100 | Pro detekované anomálie prochází Dodavatel služby následným postupem k určení kategorií kybernetických bezpečnostních událostí a incidentů (dle § 31, VoKB) podle následků a negativních projevů pro doporučení opatření či součinnosti v následné reakci:<br><br><u>Fáze Detekce</u><br>• Monitoring prostředí vymezeného Zadavatelem.<br>• Dohledování bezpečnostní situace Zadavatele.<br>• Detekce anomálie - rozpoznání odchylky od běžného stavu nebo od Zadavatelem normovaného stavu.<br><br><u>Fáze Přiřazení</u><br>• Klasifikace anomálie - určení závažnosti ve škále:<br>o False-Positive Alarm - *způsobuje falešný alarm z důvodu:*<br>■ *chyby v úsudku míry závažnosti anomálie,*<br>■ *nepřesnosti rozpoznání odchylky vzniklé při dohledování a monitoringu v předchozí fázi detekce.*<br>o Bezpečnostní událost - *anomálie, která může způsobit narušení bezpečnosti:*<br>■ *informací v informačních systémech Zadavatele,*<br>■ *služeb Zadavatele,*<br>■ *integrity datových sítí Zadavatele.*<br>o Bezpečnostní incident - *anomálie, která narušila či narušuje bezpečnost:*<br>■ *informací v informačních systémech Zadavatele,*<br>■ *služeb Zadavatele,*<br>■ *integritu datových sítí Zadavatele nebo jiných subjektů.*<br><u>Fáze Analýza</u><br>• Vyhodnocení anomálie - vyhodnocení relevance:<br>o *k systémům Zadavatele,*<br>o *k procesům Zadavatele,*<br>o *k zákonným normám ČR vztažených na Zadavatele.*<br>• Klasifikace incidentu - začlenění incidentu do bezpečnostního typu kategorie dle určení zadavatelem nebo dle §30, VoKB: | sTužba SOC365 prochází detekované anomálie za účelem určení kategorie kybernetických událostí a incidentů pro doporučení opatření či součinnosti v požadovaných reakcích. | ANO |

| | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| | o Podle příčiny:<br>■ incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb,<br>■ incident způsobený škodlivým kódem,<br>■ incident způsobený překonáním technických opatření,<br>■ incident způsobený porušením organizačních opatření,<br>■ incident spojený s projevem trvale působících hrozeb,<br>■ ostatní incidenty způsobené kybernetickým útokem.<br>o Podle dopadu:<br>■ incident způsobující narušení důvěrnosti aktiv,<br>■ incident způsobující narušení integrity aktiv,<br>■ incident způsobující narušení dostupnosti aktiv,<br>■ incident způsobující kombinaci výše uvedených dopadů.<br>• Kategorizace incidentu - začlenění incidentu podle významnosti. | | |
| 101 | **Kategorie III -** maximální doba detekce **do 30 minut -** velmi závažný kybernetický bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu, včetně minimalizace vzniklých i potenciálních škod. V rámci této kategorie je požadováno provedení aktivního zásahu a poté kontaktování administrátora IT dotčeného subjektu s předanou informací o realizovaných opatřeních v rámci aktivního zásahu. | | ANO |
| 102 | **Kategorie II -** maximální doba detekce **do 2 hodin -** závažný kybernetický bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického incidentu včetně minimalizace vzniklých škod. V rámci této kategorie je požadován aktivní zásah po kontaktování a souhlasu IT administrátora dotčeného subjektu. | | ANO |
| 103 | **Kategorie I -** maximální doba detekce **do 24 hodin - méně** závažný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod. Jedná se o bezpečnostní incidenty, které nespadají do kategorií III a II. V rámci této kategorie je požadován aktivní zásah po kontaktování a | | ANO |

| | Minimální požadované funkcionality - vlastnosti | Nabízené řešení, včetně vysvětlení, jak je zadání naplněno | Splněno ANO |
|---|---|---|---|
| | souhlasu IT administrátora dotčeného subjektu. | | |
| 104 | Požadovaná minimálně zajištěná kvalita služby - SLA SOC je 99,9% | | ANO |

## 8. Přílohy

### Příloha č. 1 - Přehled infrastrukturních a aplikačních prvků/systémů

[redacted]

[redacted]

Tabulka č. 4 - Přehled infrastrukturních a aplikačních prvků

## Příloha č. 2 - Dokumentace IT systémů a sítí ZZ

(tvoří samostatný dokument)

## Příloha č. 3 - Rozsah penetračního testování (1. sada penetračních testů)

(tvoří samostatný dokument)

# Dokumentace IT systémů a sítí

## Zdravotnické záchranné služby Moravskoslezského kraje

Verze 1.1, aktualizace ke dni 21.8.2023

Autor: **IT zaměstnanci ZZS MSK**

*Obsah:*


**Seznam zkratek** **5**
**Předmět dokumentu** **6**
**Obecné informace** **7**
Struktura sítí 7
Používané sítě a domény 7
Antimalware řešení 9
Zálohování 9
**IBC MSK** **10**
[redacted] 10
10
13
13
15
15
17
19
19
20
21
**Ostrava** **22**
[redacted] 22
22
23
24
24
24
25
25
25
25
**Opava** **26**
[redacted] 26
27
28
28
29
29
29
29
30
30
31

[redacted] 31
**Bruntál** **31**
[redacted] 31
32
32
32
33
33
33
33
34
34
34
34
**Nový Jičín** **35**
[redacted] 35
35
36
36
36
36
37
37
37
37
38
38
38
38
39
39
**Frýdek-Místek** **40**
[redacted] 40
40
41
41
41
41
42
42
42
42
43
43

[redacted] 43
43
**Karvina** **44**
[redacted] 44
44
44
45
45
45
46
46
46
46
47
47
48
48
48
48

# Seznam zkratek

| | |
|---|---|
| **MSK** | Moravskoslezský kraj |
| **IZS** | Integrovaný záchranný systém ČR |
| **ZZS MSK** | Zdravotnická záchranná služba Moravskoslezského kraje |
| **KZOS** | Krajské zdravotnické operační středisko |
| **IBC MSK** | Integrované bezpečnostní centrum MSK - dispečink všech složek IZS MSK |
| **HZS MSK** | Hasičský záchranný sbor MSK |
| **IS OŘ** | Informační systém operačního řízení |
| **IS ZD ZZS** | Informační zdravotnické dokumentace ZZS |
| **VSS IBC** | Vrstva společných služeb IBC MSK |
| **NIS IZS** | Národní informační systém IZS |

# Předmět dokumentu

Předmětem dokumentu je popis síťového prostředí celé organizace Zdravotnické záchranné služby od fyzických prostředků, přes virtuální sítě, IP prostory, po popis serverového prostředí a aplikací používaných v rámci organizace.

# Obecné informace

## Struktura sítí

[redacted]

## Používané sítě a domény

[redacted]

[redacted]

[redacted]

## Antimalware řešení

[redacted]

## Zálohování

[redacted]

# IBC MSK

## Síťové prvky, umístění, propojení, management IP

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Informační systém ZD ZZS

[redacted]

[redacted]

[redacted]

Personální systém Vema

[redacted]

[redacted]

[redacted]

[redacted]

Ostrava

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Opava

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

# Příloha č. 3 technické specifikace - Rozsah penetračního testování (1. sada penetračních testů)

## 1.1 Cíl penetračního testování

Cílem penetračních testů je otestovat tu část infrastruktury, která zpracovává pacientská data (zvláštní data dle GDPR), otestovat zálohovací systémy daného ZZ a případně otestovat všechna aktiva, za pomoci, kterých mohou být kompromitována pacientská data, ale neslouží primárně k účelu jejich zpracovávání.

Jsou tedy kladeny otázky: “Dokáže útočník odcizit pacientská data?“ a „Dokáže se útočník napříč infrastrukturu nemocnice dostat k pacientským datům?“.

## 1.2 Scénáře

Jsou požadovány **tři scénáře pro testování.**

### 1.2.1 Test zvenčí

V tomto scénáři je požadováno, aby se tester pokusil kompromitovat FW, a skrze něj infiltrovat IT infrastrukturu daného ZZ a pokračovat dle cíle viz 1.1.

### 1.2.2 Fyzický vnitřní test

V tomto scénáři je požadováno, aby se tester fyzicky dostavil do lokality ZZ (Zdravotní záchranná služba MSK ), a pokusil se kompromitovat personální (ne pacientské volně dostupné) bezdrátové Wi-Fi sítě a pokračoval dle cíle viz 1.1.

### 1.2.3 Logický vnitřní test

V tomto scénáři je simulováno převzetí stanice útočníkem (např. instalací škodlivého souboru na uživatelské stanici apod.). V tomto scénáři je požadováno, aby tester měl k dispozici stanici (virtuální) v segmentu, kde pracují běžní zaměstnanci ZZ. Za pomocí této stanice se bude snažit eskalovat práva a pokračovat dle cíle viz 1.1.

## 1.3 Rozsah

**Rozsahem pro penetrační testování ZZ budou kritická technická aktiva dle provedené analýzy rizik dodavatelem a případně i taková aktiva, která zpracovávají pacientská data a nejsou klasifikována jako kritická. Počtem se jedná o maximálně 10 aktiv za celé ZZ.**
**Z pohledu délky naceňovaného období se jedná o jednorázový test.**

## 1.4 Certifikace

Pro zajištění kvalitních a relevantních výstupů a maximalizaci nedestruktivity jsou vyžadovány minimálně dvě z následujících certifikací:

- CEH
- OSCP
- OSWP
- CPENT

Tyto certifikace zaručují, že dodavatel penetračních testů má potřebné znalosti a dovednosti k provedení penetračních testů na vysoké úrovni, a v souladu s nejlepšími postupy a standardy v oboru.

## 1.5 Reference

Pro zajištění důvěryhodnosti a kvality prováděného penetračního testování je požadována minimálně jedna reference dodavatele v oblasti zdravotnictví nebo bankovnictví. Tento požadavek je klíčový, jelikož budou testovány IT infrastruktury obsahující citlivá data. Referenční zkušenosti v těchto oborech potvrzují schopnost dodavatele pracovat s vysokými standardy zabezpečení a přizpůsobit své služby specifickým potřebám a regulacím těchto citlivých odvětví. Tímto způsobem je zaručeno, že penetrační testování bude prováděno odborníky s relevantními zkušenostmi a znalostmi, což maximalizuje účinnost a bezpečnost celého procesu.

| **REFERENČNÍ ZAKÁZKA** | |
|---|---|
| název realizované zakázky: | |
| název objednatele: | |
| sídlo nebo místo podnikání: | |
| IČO objednatele: | |
| kontaktní osoba objednatele: | |
| telefonní spojení na objednatele: | |

| | |
|---|---|
| místo realizace zakázky: | |
| popis předmětu plnění zakázky a její rozsah: | |
| doba (termín) plnění zakázky: | |

1.6 **Výstupy**

Penetrační testování bude zakončeno publikací zprávy, která bude obsahovat minimálně:

- popis metod, metodik, norem, doporučení a vlastních postupů, které byly použity,
- seznam a charakteristiku nástrojů, které byly použity,
- popis prostředí, které bylo předmětem testů včetně,
    - seznamu IP adres, které byly předmětem testu,
    - seznam identifikovaných portů a na nich běžících služeb a protokolů použitých pro komunikaci s těmito porty a rovněž identifikovaného SW použitého pro realizaci služeb na portech
- seznam a charakteristiku testů, které byly provedeny,
- detailní seznam zjištění, minimálně v rozsahu:
    - identifikace zjištění zranitelnosti,
    - popis kde a jakým způsobem byla zranitelnost identifikována,
    - označení/název zranitelnosti (pokud lze přiřadit),
    - charakteristika zranitelnosti včetně potenciálního dopadu,
    - klasifikace zranitelnosti podle použité metodiky, kde bude obsaženo:
        - kategorii/typ zranitelnosti,
        - úroveň zranitelnosti,
        - dle pravděpodobnosti zneužití,
        - náročnosti odstranění/nápravy.
    - popis zranitelného místa/nálezu,
    - navržené opatření nebo Rozsah doporučení k eliminaci nebo minimalizaci zranitelnosti, případně odkazy na doporučení výrobce/distributora nebo jiné best practice,
    - další využití zranitelnosti, pokud bylo v rámci manuálních testů
    - další podstatné skutečnosti,
- stručné manažerské shrnutí včetně přehledových charakteristik a celkového hodnocení zabezpečení prostředí testované organizace
- závěrečné zhodnocení provedeného testu a hodnocení aktuálně dosažené úrovně bezpečnosti infrastruktury
- celková doporučení nebo navržení dalších kroků,
- přílohy (výstupy z použitých nástrojů, důkazy apod.).

Dodavatel penetračních testů dále seznámí dotčené ZZ s výsledky penetračních testů formou online schůzky, kde budou prezentovány a komentovány výsledky z testování.

**Příloha č. 2 smlouvy: Zástupci smluvních stran oprávnění jednat ve věcech této smlouvy a realizační tým**

Osoby uvedené v této příloze smlouvy jsou osobami, které jsou oprávněné jednat ve věcech této smlouvy

**Za objednatele:**

[redacted]

**Za poskytovatele:**

[redacted]

**Organigram a rozdělení kompetencí členů realizačního týmu poskytovatele:**

ORGANIGRAM DODAVATELE

[redacted]

**Pohotovostní kontakty objednatele - komunikace v českém jazyce**

[redacted]

**Realizační tým**

Poskytovatel je povinen plnit smlouvu s využitím následujících pracovníků, přičemž případné nahrazení pracovníků se řídí čl. X odst. 1 smlouvy.

[redacted]

**Zdravotnická záchranná služba Moravskoslezského kraje, p.o.**
Výškovická 2995/40, Zábřeh, 700 30 Ostrava

# Směrnice ZZS Moravskoslezského kraje
# č. 7/2023

Název: Používání informačních a komunikačních technologií

Obsah:
Směrnice upravuje práva a povinnosti uživatelů
a správců informačních a komunikačních technologií

Rozdělovník:
- všichni zaměstnanci ZZS MSK

[redacted]

## Obsah

1. Úvod ..... 4

2. Rozdělení sítí ..... 4

a) VLÁN privátního charakteru a povinnosti uživatelů ..... 4

b) Typy přístupů a oprávnění ke stanicím v interních sítích ..... 6

c) VLÁN veřejného charakteru ..... 6

3. Povinnosti správců IT a rozdělení působnosti ..... 7

4. Provozní pravidla informačních systémů ..... 8

a) Intranet, elektronická pošta, portál ZD, mobilní zadávání dat ..... 8

b) Ekonomický IS ..... 9

c) Personální IS ..... 9

d) IS operačního řízení ..... 9

5. Přidělení výpočetní techniky ..... 10

## Seznam zkratek

| | |
|---|---|
| **ICT** | - informační a komunikační technologie |
| **IT** | - informační technologie |
| **IS** | - informační systém |
| **LAN** | - lokální počítačová síť |
| **NAS** | - úložiště přímo připojené k síti |
| **VLÁN** | - virtuální LAN |
| **ZD** | - zdravotnická dokumentace ZZS |

## 1. Úvod

[redacted]

## 2. Rozdělení sítí

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Moravskoslezský kraj

# Bezpečnostní politika místních nesdílených aplikací

| | |
|---|---|
| Datum zhotovení | 16. 10. 2020 |
| Zhotovitel | 13 Consultants s.r.o. |
| Zpracoval za zhotovitele | [redacted] |
| Verze | 01 |
| Veřejná zakázka | 176/2019 |
| Smlouva | 00115/2020/Ř |
| Objednatel | Moravskoslezský kraj |
| Počet stran | 41 |

**Krajský úřad Moravskoslezského kraje má zavedené systémy řízení kvality, environmentu a bezpečnosti informací.**

Klasifikace informací: Neveřejné

# Kontrola a schválení dokumentu

## Provedené revize

| Verze | Autor | Datum | Revize |
|---|---|---|---|
| 1.0 | [redacted] (13 Consultants s.r.o.) | | Finalizace dokumentu. |
| | | | |
| | | | |
| | | | |
| | | | |

## Tento dokument byl zkontrolován

| | Kontrolu provedl/a | Datum kontroly |
|---|---|---|
| 1. | [redacted] HI3 Consultants s.r.o.) | 19.10.2020 |
| 2. | | |
| 3. | | |

## Tento dokument byl schválen

| | Jméno | Podpis | Datum schválení |
|---|---|---|---|
| 1. | [redacted] (MSK) | | 2.11.2020 |
| 2. | | | |
| 3. | | | |



Klasifikace informací: Neveřejné

# Obsah

Seznam zkratek a vysvětlení pojmů ... 6
1 Úvod ... 9
2 Systém řízení bezpečnosti informací ... 10
2.1 Cíle systému řízení bezpečnosti informací ... 10
2.2 Rozsah a hranice systému řízení bezpečnosti informací ... 11
2.3 Pravidla a postupy pro řízení dokumentace ... 11
2.4 Pravidla kontrolní činnosti systému řízení bezpečnosti informací ... 11
2.5 Pravidla pro řízení neshod ... 11
2.6 Pravidla a postupy pro řízení zdrojů a provozu systému řízení bezpečnosti informací ... 12
2.7 Pravidla a postupy pro provádění auditů kybernetické bezpečnosti ... 12
2.8 Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací ... 13
3 Pravidla řízení aktiv a rizik ... 13
3.1 Identifikace, hodnocení a evidence aktiv, řízení rizik ... 13
3.2 Přípustné použití aktiv ... 14
3.3 Klasifikační schéma ... 14
4 Pravidla organizační bezpečnosti ... 15
4.1 Určení bezpečnostních rolí a jejich práv a povinností ... 15
4.2 Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí ... 17
5 Pravidla řízení přístupu ... 17
5.1 Požadavky na řízení přístupu ... 17
5.2 Řízení privilegovaných oprávnění ... 18
6 Pravidla bezpečnosti lidských zdrojů ... 19
6.1 Bezpečnostní školení nových zaměstnanců ... 19
6.2 Pravidla rozvoje bezpečnostního povědomí ... 19
6.3 Pravidla pro řešení případů porušení bezpečnostní politiky systému řízení bezpečnosti informací ... 20
6.4 Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice ... 20
7 Pravidla bezpečného chování uživatele ... 20
7.1 Bezpečné chování uživatele ... 20
7.2 Použití přístupového hesla ... 22
7.3 Bezpečné chování na sociálních sítích ... 22
7.4 Pravidla pro ochranu a používání přenosných zařízení ... 23
7.4.1 Ochrana přenosných zařízení ... 23
7.4.2 Ochrana soukromých zařízení ... 23
7.4.3 Pravidla pro používání přenosných a soukromých zařízení ... 23
8 Pravidla zálohování, obnovy a dlouhodobého ukládání ... 24



Klasifikace informací: Neveřejné

9 Pravidla řízení dodavatelů ..... 25
9.1 Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti ..... 25
9.2 Pravidla pro provádění kontroly zavedení bezpečnostních opatření a hodnocení dodavatelů 25
9.3 Pravidla pro hodnocení rizik souvisejících s dodavateli ..... 26
10 Pravidla bezpečného používání zařízení ..... 26
11 Pravidla fyzické bezpečnosti ..... 27
11.1 Pravidla pro ochranu objektů ..... *Z1*
11.2 Pravidla pro kontrolu vstupu osob ..... *Z1*
11.3 Pravidla pro vstup do režimových prostor ..... 28
11.4 Pravidla zabezpečení dokumentů určených ke skartaci a archivaci ..... 28
11.5 Pravidla klíčového režimu (manipulace s klíči, čipy a čipovými kartami) ..... 29
11.6 Pravidla úklidu ..... 29
11.7 Pravidla pro zajištění fyzické bezpečnosti zařízení ..... 30
11.8 Detekce narušení fyzické bezpečnosti ..... 31
12 Pravidla bezpečnosti komunikační sítě ..... 31
12.1 Bezpečnost provozu sítě ..... 31
12.2 Pravidla a postupy pro ochranu vzdáleného přístupu k síti ..... 32
12.3 Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů ..... 33
12.4 Požadavky a standardy bezpečného provozu ..... 33
12.5 Bezpečnost aplikací (penetrační testování) ..... 34
13 Pravidla ochrany před škodlivým kódem ..... 34
14 Pravidla řízení technických zranitelností ..... 35
15 Pravidla kryptografické ochrany ..... 35
16 Pravidla nákupu a vývoje místních aplikací ..... 36
16.1 Pořizování místních aplikací ..... 36
16.2 Data pro testování ..... 36
17 Pravidla řízení změn ..... 37
18 Kybernetické bezpečnostní incidenty ..... 37
19 Pravidla řízení kontinuity činností ..... 38
20 Pravidla pro detekci kybernetických bezpečnostních událostí ..... 39
21 Politika ochrany osobních údajů ..... 39
22 Přílohy ..... 39
22.1 Příloha č. 1 - Vzorový kontrolní plán ..... 39
22.2 Příloha č. 2 - Metodika analýzy rizik kybernetické bezpečnosti ..... 40
22.3 Příloha č. 3 - Metodika analýzy rizik kybernetické bezpečnosti pro zdravotnická zařízení ..... 40
22.4 Příloha č. 4 - Bezpečnostní pravidla pro dodavatele ..... 40



Klasifikace informací: Neveřejné

22.4.1 Řízení přístupu ..... 40
22.4.2 Ochrana informací ..... 41
22.4.3 Hlášení ..... 41
22.4.4 Mlčenlivost ..... 41



Klasifikace informací: Neveřejné

**Seznam zkratek a vysvětlení pojmů**

| | |
|---|---|
| AD | Active Directory; Centralizovaná správa uživatelských účtů a zařízení organizace. |
| Aktivum | Informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém příspěvkové organizace. |
| EPS | Elektrická požární signalizace. |
| Garant aplikace | Zaměstnanec odpovědný za konkrétní aplikaci. Garant aplikace je odborný zaměstnanec se znalostí dané aplikace. Plně rozhoduje o požadavcích na přístup k dané aplikaci, rušení přístupových oprávnění a přezkoumání přístupových oprávnění. Pravidelně komunikuje se Správcem ICT ohledně způsobů nastavení a zabezpečení konkrétní aplikace. Společně se Správcem ICT je klíčovou rolí v zabezpečení dat organizace. |
| GDPR | NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). |
| Hrozba | Potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu. |
| Kybernetická bezpečnost | Zajištění digitálního prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací. |
| Kybernetická bezpečnostní událost | Událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. |
| Kybernetický bezpečnostní incident | Narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. |
| MDM | Mobile Device Management; Centralizovaná správa mobilních zařízení. |
| Místní aplikace | Souhrn všech aplikací (vyjma sdílených aplikací MSK, které mají stanovena vlastní závazná pravidla používání formou Bezpečnostní politiky sdílených ICT služeb), operačních systémů a dalších programů používaných příspěvkovou organizací. |
| Need to know | „Potřeba znát" - zásada zajištění nezbytných znalostí (přístupových oprávnění) potřebných pro vykonávání konkrétní pracovní činnosti. |
| PO | Příspěvková organizace. |
| Pracovní stanice | Stolní, nepřenosný počítač, zapojený do počítačové sítě organizace. |



Klasifikace informací: Neveřejné

| | |
|---|---|
| Přenosná zařízení | Notebooky, smartphony, tablety. |
| PZTS | Poplachové a zabezpečovací tísňové systémy, dříve nazývané EZS. |
| Rackové skříň | Standardizovaný systém umožňující přehlednou montáž a propojování různých elektrických a elektronických zařízení spolu s vyústěním kabelových rozvodů do sloupců nad sebe v ocelovém rámu, skříni neboli v rozvaděči pro IT techniku. |
| Režimový prostor | Prostor, jimiž jsou např. serverovna, místnosti s podružnými rozvaděči se síťovými prvky vnitřní sítě, místnosti s řídícími prvky systémů technické ochrany, technologické místnosti (strojovna výtahu a šachta výtahu, telefonní ústředna, kotelna apod.), spisovna. |
| RPO | Cílový bod obnovení/zotavení. Nejdelší plánované období, během kterého mohla být data (transakce) ztracena z aplikace v důsledku závažného incidentu. |
| RTO | Cílový čas/doba zotavení. Maximální plánovaná doba trvání nedostupnosti služeb/aplikací, za kterou musí být po incidentu nebo narušení obnoveny, aby se zabránilo nepřijatelným důsledkům spojeným s přerušením kontinuity procesů. |
| SHGK | Systém hlavního a generálního klíče. |
| SLA | Service Level Agreement - je dohoda o úrovni poskytovaných služeb. SLA představuje formalizovaný popis služby, kterou poskytuje dodavatel zákazníkovi. SLA definuje rozsah, úroveň a kvalitu služby. |
| Soukromá zařízení | Pracovní stanice, notebooky, smartphony a tablety, které nejsou ve vlastnictví organizace. |
| Správce ICT | Osoba odpovědná za provozování a správu počítačové sítě a prostředků ICT organizace. Disponuje nejvyššími administrátorskými účty k operačním systémům a některým aplikacím. Společně s garantem aplikace je klíčovou rolí v zabezpečení dat organizace. |
| SW | Software, programové vybavení zařízení. |
| Technické účty | Jsou účty určené pro správu aplikací, databází, infrastruktury (např. firewally, servery, routery) apod. |
| Úschovné objekty | Jsou skříňky a trezory slouží pro uložení věcí a podle stupně odolnosti jsou určené na různě vysoké hodnoty uložených věcí a dokumentů. |
| Významná změna | Změna, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko pro bezpečnost informací organizace (typicky např. |



Klasifikace informací: Neveřejné

| | |
|---|---|
| | změna platformy operačního systému např. z Linux na Windows, zavedení nástrojů SIEM, virtualizace serverů, využití cloudu apod.). |
| Wi-Fi | Způsob připojení zařízení k síti za pomocí bezdrátových technologií. |
| Zařízení | Pracovní stanice a přenosná zařízení. |
| Zranitelnost | Slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami. |



Klasifikace informací: Neveřejné

# 1 Úvod

Tento dokument stanovuje základní pravidla kybernetické bezpečnosti pro uživatele a správu místních nesdílených aplikací. Pravidla stanovená tímto dokumentem obsahují postupy, které vycházejí z požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), navazující vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) a dobré praxe bezpečnosti informací, zejména dle ČSN EN ISO/IEC 27001.

Pro PO a její uživatele jsou tato pravidla doporučující, vyjma pravidel uvedených v kap. č. 7.1 *„Bezpečné chování uživatelé'.* Tato pravidla jsou totožná s pravidly bezpečného chování uživatele při jeho práci s daty ve sdílených ICT službách, které jsou MSK stanoveny prostřednictvím dokumentu „Bezpečnostní politika sdílených ICT služeb".

[redacted]



Klasifikace informací: Neveřejné

[redacted]

# 2 Systém řízení bezpečnosti informací

## 2.1 Cíle systému řízení bezpečnosti informací

***Úroveň1, Úroveň2, Úroveň3***

[redacted]



Klasifikace informací: Neveřejné

## 2.2 Rozsah a hranice systému řízení bezpečnosti informací

***Úroveň1, Úroveň2, Úroveň3***

[redacted]

## 2.3 Pravidla a postupy pro řízení dokumentace

***Úroveň2, Úroveň3***

[redacted]

## 2.4 Pravidla kontrolní činnosti systému řízení bezpečnosti informací

***Úroveň1, Úroveň2, Úroveň3***

[redacted]

## 2.5 Pravidla pro řízení neshod

***Úroveň1, Úroveň2, Úroveň3***

[redacted]

[redacted]

## 2.6 Pravidla a postupy pro řízení zdrojů a provozu systému řízení bezpečnosti informací

***Úroveň2$_f$ Úroveň3***

[redacted]

## 2.7 Pravidla a postupy pro provádění auditů kybernetické bezpečnosti

***Úroveň3***

[redacted]



Klasifikace informací: Neveřejné

[redacted]

### 2.8 Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací

***Úroveň3***

[redacted]

## 3 Pravidla řízení aktiv a rizik

[redacted]



Klasifikace informací: Neveřejné

[redacted]

### 3.2 Přípustné použití aktiv

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

### 3.3 Klasifikační schéma

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

| Klasifikační stupeň | Označení | Základní popis |
|---|---|---|
| **Veřejná informace** | Veřejné (W) | Veřejnou informací je informace, která je ze své povahy primárně určena ke zveřejnění. Důvěrnost veřejných informací není nutno chránit.<br><br>Informace, které lze běžně sdělovat a publikovat.<br><br>Jedná se zpravidla o informace a dokumenty určené ke zpřístupnění veřejnosti, médiím apod. |
| **Neveřejná informace (interní)** | Neveřejné (N) | Jedná se o dokumenty, které jsou určeny pouze pro interní potřebu PO.<br><br>Externí přístup k těmto informacím je omezen, informace jsou poskytovány pouze na základě právní úpravy, uzavřené smlouvy nebo se souhlasem ředitele nebo jiné oprávněné osoby. Interní přístup k těmto informacím je omezený na základě přístupových oprávnění jednotlivých uživatelů. V případě neoprávněného zveřejnění informace nejsou následky závažné. |

| | | |
|---|---|---|
| **Důvěrná informace** | Důvěrná<br><br>(D) | Jedná se o data a informace, které obsahují osobní údaje (zaměstnanců, klientů, zástupců smluvních partnerů) nebo které nelze bez dalšího zpřístupňovat veřejnosti.<br><br>Dále se jedná o data a informace PO, informace z vedených správních a jiných řízení, případně data třetích stran (např. obchodní tajemství).<br><br>Externí přístup k těmto informacím je omezen, informace jsou poskytovány pouze na základě právní úpravy, uzavřené smlouvy nebo se souhlasem ředitele nebo jiné oprávněné osoby. Interní přístup k těmto informacím je omezený na základě přístupových oprávnění jednotlivých uživatelů. V případě neoprávněného zveřejnění informace jsou následky závažné, avšak ne kritické. Integrita a důvěrnost dat je důležitá. |
| **Chráněná informace** | Chráněné (CH) | Informace klasifikované jako chráněné jsou zvláštní kategorie osobních údajů (citlivé údaje), jejichž vyzrazení by vedlo k významným materiálním, nebo finančním ztrátám nebo ke ztrátě důvěryhodnosti vůči veřejnosti,<br><br>a) které podléhají zvýšené ochraně dle GDPR (zejména osobní údaje zvláštní kategorie) např. údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob a informace o dětech (osobách) mladších 18 let,<br>b) které jsou poskytnuty za účelem řešení, neshody, bezpečnostní události a incidentu.<br>Přístup k těmto informacím je omezen pouze na vybranou skupinu zaměstnanců na základě přístupových oprávnění. Důvěrnost informací je velmi důležitá. Data jsou šifrovaná. |

# 4 Pravidla organizační bezpečnosti

## 4.1 Určení bezpečnostních rolí a jejich práv a povinností

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

[redacted]

***Úroveň 3***

[redacted]



Klasifikace informací: Neveřejné

[redacted]

### 4.2 Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí

***Úroveň3***

[redacted]

## 5 Pravidla řízení přístupu

### 5.1 Požadavky na řízení přístupu

***Úroveň1; Úroveň2; Úroveň3***

[redacted]



Klasifikace informací: Neveřejné

[redacted]

***Úroveň3***

[redacted]

## 5.2 Řízení privilegovaných oprávnění

***Úroveň 1; Úroveň 2; Úroveň 3***

[redacted]



Klasifikace informací: Neveřejné

[redacted]

# 6 Pravidla bezpečnosti lidských zdrojů

## 6.1 Bezpečnostní školení nových zaměstnanců.

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

## 6.2 Pravidla rozvoje bezpečnostního povědomí

***Úroveň1; Úroveň2; Úroveň3***

[redacted]



Klasifikace informací: Neveřejné

[redacted]

### 6.3 Pravidla pro řešení případů porušení bezpečnostní politiky systému řízení bezpečnosti informací

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

### 6.4 Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

## 7 Pravidla bezpečného chování uživatele

### 7.1 Bezpečné chování uživatele

***Úroveň1; Úroveň2; Úroveň3***

[redacted]



Klasifikace informací: Neveřejné

[redacted]



Klasifikace informací: Neveřejné

[redacted]

### 7.2 Použití přístupového hesla

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

### 7.3 Bezpečné chování na sociálních sítích

***Úroveň1; Úroveň2; Úroveň3***

[redacted]



Klasifikace informací: Neveřejné

[redacted]

## 7.4 Pravidla pro ochranu a používání přenosných zařízení

### 7.4.1 Ochrana přenosných zařízení

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

### 7.4.2 Ochrana soukromých zařízení

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

### 7.4.3 Pravidla pro používání přenosných a soukromých zařízení

***Úroveň1; Úroveň2; Úroveň3***



Klasifikace informací: Neveřejné

[redacted]

## 8 Pravidla zálohování, obnovy a dlouhodobého ukládání

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

***Úroveň2 a Úroveň3***

[redacted]



Klasifikace informací: Neveřejné

# 9 Pravidla řízení dodavatelů

## 9.1 Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

## 9.2 Pravidla pro provádění kontroly zavedení bezpečnostních opatření a hodnocení dodavatelů

***Úroveň1; Úroveň2; Úroveň3***

[redacted]



Klasifikace informací: Neveřejné

[redacted]

### 9.3 Pravidla pro hodnocení rizik souvisejících s dodavateli

***Úroveň 3***

[redacted]

## 10 Pravidla bezpečného používání zařízení

***Úroveň 1; Úroveň 2; Úroveň 3***

[redacted]

**Úroveň 3**

[redacted]



Klasifikace informací: Neveřejné

# 11 Pravidla fyzické bezpečnosti

## 11.1 Pravidla pro ochranu objektů

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

## 11.2 Pravidla pro kontrolu vstupu osob

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

*TI*

[redacted]



Klasifikace informací: Neveřejné

[redacted]

### 11.5 Pravidla klíčového režimu (manipulace s klíči, čipy a čipovými kartami)

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

### 11.6 Pravidla úklidu

***Úroveň1; Úroveň2; Úroveň3***

[redacted]



Klasifikace informací: Neveřejné

### 11.7 Pravidla pro zajištění fyzické bezpečnosti zařízení

***Úroveň 1; Úroveň 2; Úroveň 3***

[redacted]

***Úroveň 2***

[redacted]

***Úroveň 3***

[redacted]



Klasifikace informací: Neveřejné

[redacted]

### 11.8 Detekce narušení fyzické bezpečnosti

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

## *12* Pravidla bezpečnosti komunikační sítě

### 12.1 Bezpečnost provozu sítě

***Úroveň1; Úroveň2; Úroveň3***

[redacted]



Klasifikace informací: Neveřejné

[redacted]

### 12.2 Pravidla a postupy pro ochranu vzdáleného přístupu k síti

***Úroveň2; Úroveň3***

[redacted]



Klasifikace informací: Neveřejné

[redacted]

### 12.3 Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů

***Úroveň2 a Úroveň3***

[redacted]

### 12.4 Požadavky a standardy bezpečného provozu

***Úroveň2; Úroveň3***

[redacted]

***Úroveň3***

[redacted]



Klasifikace informací: Neveřejné

[redacted]

### 12.5 Bezpečnost aplikací (penetrační testování)

***Úroveň3***

[redacted]

## 13 Pravidla ochrany před škodlivým kódem

***Úroveň1; Úroveň2; Úroveň3***

[redacted]



Klasifikace informací: Neveřejné

[redacted]

***Úroveň2 a Úroveň3***

[redacted]

## 14 Pravidla řízení technických zranitelností

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

## 15 Pravidla kryptografické ochrany

***Úroveň1; Úroveň2; Úroveň3***

[redacted]



Klasifikace informací: Neveřejné

[redacted]

# 16 Pravidla nákupu a vývoje místních aplikací

## 16.1 Pořizování místních aplikací

***Úroveň1; Úroveň2; Úroveň3***

[redacted]

## 16.2 Data pro testování

***Úroveň3***

[redacted]



Klasifikace informací: Neveřejné

## 17 Pravidla řízení změn

***Úroveň2; Úroveň3***

[redacted]

## 18 Kybernetické bezpečnostní incidenty

***Úroveň1; Úroveň2***

[redacted]



Klasifikace informací: Neveřejné

[redacted]

## 19 Pravidla řízení kontinuity činností

***Úroveň 3***

[redacted]



Klasifikace informací: Neveřejné

## 20 Pravidla pro detekci kybernetických bezpečnostních událostí

***Úroveň 3***

[redacted]

## 21 Pravidla ochrany osobních údajů

PO disponuje samostatným předpisem pro zajištění ochranu osobních údajů.

## 22 Přílohy

[redacted]



Klasifikace informací: Neveřejné

[redacted]

## 22.2 Příloha č. 2 - Metodika analýzy rizik kybernetické bezpečnosti

Samostatný dokument (Priloha 2_Metodika analyzy rizik KB).

## 22.3 Příloha č. 3 - Metodika analýzy rizik kybernetické bezpečnosti pro zdravotnická zařízení

Samostatný dokument (Priloha 3_Metodika analyzy rizik KB_zdrav).

## 22.4 Příloha č. 4 - Bezpečnostní pravidla pro dodavatele

### 22.4.1 Řízení přístupu

[redacted]



Klasifikace informací: Neveřejné

[redacted]

### 22.4.2 Ochrana informací

[redacted]

### 22.4.3 Hlášení

[redacted]

### 22.4.4 Mlčenlivost

[redacted]



Klasifikace informací: Neveřejné

# *Příloha č. 4 Pravidla auditu*

| | | | |
|---|---|---|---|
| **Datum 1. vydání** | 1. 3. 2021 | **Platnost verze od:** | 22. 7. 2022 |

Příspěvková organizace
Moravskoslezského kraje

*© Moravskoslezské datové centrum, příspěvková organizace*

# Pravidla auditu

## Obsah

1 Účel ... 3
2 Rozsah platnosti ... 3
3 Pravidla auditu ... 3
3.1 Obecně ... 3
3.2 Nedostatky a neshody ... 3
3.3 Další povinnosti ... 3
3.4 Řízení rizik v rozsahu plnění veřejné zakázky ... 4
4 Související dokumentace ... 4
5 Přílohy ... 4

# Pravidla auditu

## 1 ÚČEL

Účelem této přílohy je stanovit pravidla pro audit prováděný na straně dodavatele v rozsahu plnění Smlouvy na implementaci systému řízení bezpečnosti informací a poskytování služeb dohledového centra, která byla uzavřena v návaznosti na výsledek zadávacího řízení na veřejnou zakázku *Začlenění organizace Zdravotnická záchranná služba Moravskoslezského kraje do jednotného krajského řešení kybernetické bezpečnosti (dále jen „Smlouva").* Dodavatelem se rozumí poskytovatel dle Smlouvy a Zadavatelem se rozumí objednatel dle Smlouvy.

## 2 ROZSAH PLATNOSTI

Tento dokument je závazný pro všechny dodavatele a poddodavatele dle Smlouvy.

## 3 PRAVIDLA AUDITU

### 3.1 Obecně

Dodavatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 8 a § 16 VKB, které musí splnit Zadavatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění dle Smlouvy poskytnout adekvátní součinnost při výkonu kontroly Zadavatele ze strany Národního úřadu pro kybernetickou a informační bezpečnost dle § 23 ZKB.

Dodavatel umožní Zadavateli alespoň jednou ročně po dobu účinnosti Smlouvy provedení auditu kybernetické bezpečnosti u Dodavatele a jeho poddodavatelů.

Rozsah auditu bude ohraničen využíváním ICT prostředků Dodavatele pro potřeby plnění Smlouvy a uloženými či zpracovávanými daty a informacemi Zadavatele v ICT prostředí Dodavatele a jehož předmětem bude naplnění Kybernetických požadavků a vyhodnocení rizik dle bodu 3.4 tohoto dokumentu.

Zadavatel je oprávněn při auditu kybernetické bezpečnosti využít třetí stranu. V případě využití třetí strany bude Zadavatel odpovídat za třetí stranu, jako by audit kybernetické bezpečnosti prováděl sám, včetně odpovědnosti za způsobenou újmu.

Dodavatel umožní Zadavateli audit kybernetické bezpečnosti provedený prostředky Zadavatele nebo třetí strany, a to v lokalitě Dodavatele i vzdáleně, pokud to technické prostředky Dodavatele umožňují.

### 3.2 Nedostatky a neshody

Dodavatel je povinen odstranit nedostatky zjištěné:

- na základě provedení hodnocení rizik bezpečnosti informací dle bodu 3.4 tohoto dokumentu, nebo
- v rámci auditu kybernetické bezpečnosti

Dodavatel je povinen odstranit nedostatky/neshody ve lhůtě určené v písemném oznámení Zadavatele, která nebude kratší než 20 pracovních dní. Nestanoví-li Zadavatel lhůtu v písemném oznámení, zavazují se Smluvní strany dohodnout na lhůtě pro odstranění nedostatku, která nepřevýší 90 dní.

### 3.3 Další povinnosti

Dodavatel je dále povinen poskytnout na vyžádání Zadavateli dokumenty a obdobné vstupy, které budou prokazovat naplnění Kybernetických požadavků.

Na požádání se Zadavatelem konzultovat kdykoli v průběhu realizace plnění dle smlouvy detailní nastavení bezpečnostních opatření k naplnění kybernetických požadavků a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků.

# Pravidla auditu

Dodavatel je dále povinen neprodleně informovat Zadavatele o všech významných změnách v naplnění Kybernetických požadavků, které nastanou kdykoli v průběhu trvání veřejné zakázky.
Dále je dodavatel povinen bezodkladně a s vyvinutím nejlepšího úsilí zajistit náhradní způsob naplnění kybernetických požadavků, pokud stávající řešení přestalo být funkční a efektivní.

Dodavatel při výkonu své činnosti včas a prokazatelně upozorní Zadavatele na zřejmou nevhodnost jeho požadavků či doporučení vztahující se ke Kybernetickým požadavkům, jejichž následkem může vzniknout újma nebo nesoulad se zákony nebo jinými obecně závaznými právními předpisy.

## 3.4 Řízení rizik v rozsahu plnění veřejné zakázky

Dodavatel se bude v rozsahu předmětu plnění veřejné zakázky aktivně podílet na splnění povinností uvedených v § 5 VKB, které musí splnit Zadavatel.

**Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění veřejné zakázky na své straně:**

- Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění dle Smlouvy.
- V minimálním intervalu jednou ročně (nebo i v případě významných změn činností prováděných pro Zadavatele nebo změn při poskytování služby SOC či jiných aktiv napojených na službu SOC) vytvořit a bude-li to Zadavatel požadovat, předložit mu zprávu o hodnocení rizik, která bude minimálně pokrývat:
    a) Vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok;
    b) Identifikaci a hodnocení rizik s vazbou na předmět plnění;
    c) Realizovaná bezpečnostní opatření;
    d) Nepokrytá bezpečnostní rizika a návrh opatření;
    e) Vyhodnocení bezpečnostních událostí a incidentů;
    f) Aktuální stav souladu Dodavatele s Kybernetickými požadavky včetně přehledu Kybernetických požadavků, které
        - nebyly aplikovány, včetně odůvodnění, a
        - byly aplikovány, včetně způsobu plnění.

## 4 SOUVISEJÍCÍ DOKUMENTACE

Dokument neobsahuje související dokumentaci.

## 5 PŘÍLOHY

Dokument neobsahuje přílohy.

OBCHODNÍ NABÍDKA PRO

MORAVSKOSLEZSKÉ DATOVÉ CENTRUM

# „Začlenění organizace Zdravotnická záchranná služba do jednotného krajského řešení kybernetické bezpečnosti" v rámci výzvy č. N006/24/V00001302 ze dne 23. 7. 2024

1 Visitech

SOC365 Security Operation Center

DATA SYS

## OBSAH

**1. PŘEDMĚT NABÍDKY ..... 3**

1.1 Rámcová Specifikace nabízeného řešení ..... 3

1.2 Popis řešení ..... 4

1.3 Distribuovaná FLOW sonda na Ředitelsví Ostrava ..... 4

1.4 Zajištění sběru logů ..... 5

**2. Cenová nabídka ..... 7**

2.1 Platební podmínky ..... 7

# 1. PŘEDMĚT NABÍDKY

[redacted]

## 1.1 RÁMCOVÁ SPECIFIKACE NABÍZENÉHO ŘEŠENÍ

[redacted]

[redacted]

## 1.2 POPIS ŘEŠENÍ

[redacted]

## 1.3 DISTRIBUOVANÁ FLOW SONDA NA ŘEDITELSVÍ OSTRAVA

[redacted]

[redacted]

[redacted]

## 2. CENOVÁ NABÍDKA

[redacted]

### 2.1 PLATEBNÍ PODMÍNKY

[redacted]

[redacted]