MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Registr. číslo	PRÁVNÍ ODBOR
	0277/2025

Smlouva o poskytování služeb správy, údržby, servisu, technické podpory telekomunikačního systému Unify OpenScape 4000 MZČR včetně jeho příslušenství a provozuschopnosti koncových telefonních přístrojů a zařízení

Česká republika – Ministerstvo zdravotnictví

se sídlem:	Palackého náměstí 375/4, Praha 2, PSČ 128 00
IČO:	00024341
bankovní spojení:	2528001/0710
jednající:	Ing. Jan Gábriš, ředitel odboru IT
IDDS:	pv8aaxd

dále jen „**Objednatel**“ na straně jedné

a

IGNUM Telekomunikace s.r.o.

se sídlem:	Vinohradská 190, 130 00 Praha 3
IČO:	27637417
DIČ:	CZ27637417
bankovní spojení:	Raiffeisenbank a.s., 500500028/5500

zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 120611

zastoupen:	Michal Filip, jednatel
IDDS:	52vbhii

dále jen „**Poskytovatel**“ na straně druhé

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

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

1. Úvodní ustanovení

1) Objednatel uzavírá s Poskytovatelem tuto Smlouvu na základě Poskytovatelem podané nabídky na veřejnou zakázku s názvem „*Poskytování služeb správy, údržby, servisu, technické podpory telekomunikačního systému Unify OpenScape 4000 MZČR včetně jeho příslušenství a provozuschopnosti koncových telefonních přístrojů a zařízení*“ (dále jen „**veřejná zakázka**“), neboť splnil všechny jeho podmínky a jeho nabídka byla vybrána jako ekonomicky nejvýhodnější.

2) Objednatel prohlašuje, že splňuje veškeré podmínky a požadavky ve Smlouvě stanovené a je oprávněn Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

3) Poskytovatel prohlašuje, že:

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

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

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

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

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

4) Poskytovatel dále prohlašuje, že se detailně seznámil s rozsahem a povahou předmětu plnění, že jsou mu známy veškeré relevantní technické, kvalitativní a jiné podmínky nezbytné k realizaci předmětu plnění, a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci předmětu plnění za dohodnutou cenu uvedenou v čl. 6 Smlouvy, a to rovněž ve vazbě na jím prokázanou kvalifikaci pro plnění veřejné zakázky.

2. Účel a předmět Smlouvy

1) Smlouva je uzavírána za účelem poskytování služeb správy, údržby, servisu, technické podpory telekomunikačního systému Unify OpenScape 4000 MZČR včetně jeho příslušenství a provozuschopnosti koncových telefonních přístrojů a zařízení.

2) Předmětem Smlouvy je závazek Poskytovatele poskytovat Objednateli servisní činnost dle čl. 3 Smlouvy, a to za podmínek stanovených v této Smlouvě.

3) Předmětem Smlouvy je zároveň závazek Objednatele za řádně a včasně poskytnutou servisní činnost dle čl. 3 Smlouvy zaplatit Poskytovateli sjednanou cenu.

3. Servisní činnost

1) Servisní činností, pro účely této Smlouvy, se rozumí

   a) poskytnutí služeb spočívajících v zajištění správy, údržby, servisu, technické podpory, která je blíže popsána písm. b) až k) tohoto odst. 1 telekomunikačního systému Unify OpenScape 4000 MZČR včetně jeho příslušenství, kterým se rozumí hlavní rozvod, rack rozvaděč, vnitřní rozvody, DECT zařízení (dále jen „**telekomunikační systém**“) a provozuschopnosti koncových telefonních přístrojů a zařízení v sídle Objednatele v rozsahu:

      i. 648 digitálních poboček

      ii. 168 analogových poboček

      iii. 30 IP poboček

      iv. 116 DECT telefonů

      v. 39 BS DECT základnových stanic

      vi. Hlasová pošta

      vii. Tarifikační program Accountix;

   b) programové změny dat v telekomunikačním systému dle požadavků Objednatele v měsíčním rozsahu 20 on-site přítomností v sídle Objednatele včetně dalších navazujících nákladů (doprava, apod.);

   c) realizace konfiguračních změn v telekomunikačním systému vzdáleným přístupem, opravy a úpravy přípojných šňůr, zásuvek, kabeláže, úpravy na hlavním rozvodu a v rack rozvaděčích v sídle Objednatele;

   d) přezkušování telefonních přístrojů (digitálních I analogových) a provádění drobných oprav (výměna sluchátkových šnůr, klávesnice apod.);

   e) zavedení změn do telekomunikačního systému (zřizování, rušení a změny poboček s tím související úkony k zajištění služeb jako např. oprávnění, blokace apod.);

   f) zajištění náhradních dílů pro koncové telefonní přístroje a zařízení souvisejících s činností uvedenou pod písm. d) výše;

   g) správa tarifikačního programu Accountix včetně provádění měsíčních reportů ve standardním formátu;

   h) řešení problémů spojených s telekomunikačním systémem ve vazbě na jednotnou telekomunikační síť (JTS a VDS);

   i) jednání s výrobcem telekomunikačního systému při odstraňování závad, zasahování do systému a zajišťování potřebných provozních podmínek pro provoz pracovišť Objednatele;

j) udržování komunikačního systému a propojovacích rozvodů komunikačního systému v provozuschopném stavu včetně evidence uživatelských dat;

k) provádění servisních zásahů dle specifikace Objednatele.

Dále vše jen „**servisní činnost**“

4. Servisní podmínky

1) Servisní činnost bude Poskytovatel poskytovat především v pracovní době Objednatele, která je v pondělí až pátek 8:00 – 17:00 hod.

2) Servisní činnost může v neodkladných nebo odůvodněných případech a se souhlasem Objednatele být poskytnuta i mimo vymezenou pracovní dobu.

3) Objednatel je oprávněn požadovat od Poskytovatele servisní činnost formou písemného požadavku odeslaného na e-mailovou Poskytovatele dle čl. 11 Smlouvy.

4) Poskytovatel se zavazuje poskytnout servisní činnost na základě požadavku Objednatele dle předchozího odstavce, učiněný v době od 8:00 do 16:00, do 24 hodin během pracovních dnů od učinění požadavku. Požadavek podaný po 16:00 bude považován za požadavek podaný následující pracovní den v 8:00.

5) Pracovním dnem se pro účely této Smlouvy rozumí pondělí až pátek, s výjimkou dnů označených jako dny pracovního klidu dle ustanovení § 3 zákona č. 245/2000 Sb., o státních svátcích, o ostatních svátcích, o významných dnech a o dnech pracovního klidu.

6) V případě, že k poskytnutí servisní činnosti bude třeba využít náhradních dílů (dále jen „**náhradní díly**“), je Poskytovatel oprávněn použít k opravě náhradní díly v hodnotě do 1.000 Kč bez DPH bez předchozího souhlasu Objednatele. V případě, že hodnota náhradních dílů překročí částku uvedenou v předchozí větě, je Poskytovatel oprávněn takové náhradní díly použít pouze po předchozím souhlasu Objednatele, nestanoví-li Smlouva jinak.

7) V případě, že cena náhradních dílů na jednu opravu překročí částku ve výši 1.000 Kč bez DPH, je Poskytovatel oprávněn takové náhradní díly použít pouze na základě písemné objednávky Objednatele (dále jen „**Objednávka**“). Pro účely uzavření Objednávky se zavazuje Poskytovatel bezodkladně po výzvě Objednatele vypracovat cenovou nabídku náhradních dílů, které jsou nezbytné k poskytnutí servisní činnosti (dále jen „**cenová nabídka**“). Cenovou nabídku předloží Poskytovatel Objednateli k posouzení. Objednatel cenovou nabídku bez zbytečného odkladu od jejího předložení, nejpozději však do 7 pracovních dnů, posoudí. Pro vyloučení pochybností smluvní strany uvádí, že předložení cenové nabídky Poskytovatelem není návrhem na uzavření Smlouvy a nijak Objednatele nezavazuje k tomu, aby postupoval podle odst. 9 a násl.

8) Pro vyloučení pochybností smluvní strany uvádějí, že postup Objednávek uvedený v tomto článku se použije pouze na objednávání náhradních dílů, nikoli na poskytování servisní činnosti, která je poskytovaná pravidelně.

9) Po předložení cenové nabídky dle odst. 7 tohoto článku, Objednatel je oprávněn, nikoli však povinen, zaslat Poskytovateli písemnou Objednávku. Objednávka bude vždy obsahovat: označení smluvních stran, evidenční číslo Objednávky stanovené Objednatelem, vymezení a popis plnění, dobu a místo plnění, cenu za náhradní díly dle cenové nabídky, datum a podpis osoby jednající za Objednatele.

10) Objednatel bude Objednávky zasílat na e-mailovou adresu Poskytovatele dle čl. 11 odst. 3 této Smlouvy.

11) Objednávky budou zasílány Objednatelem Poskytovateli v pracovní dny do 16:00 hod. Objednávka zaslaná Poskytovateli po 16:00 hod. bude považována za Objednávku učiněnou následující pracovní den.

12) K přijetí Objednávky Objednatele Poskytovatelem, není-li ve Smlouvě stanoveno jinak, dochází její písemnou akceptací ze strany Poskytovatele zaslanou elektronicky na emailovou adresu kontaktní osoby Objednatele dle čl. 11. odst. 3 této Smlouvy.

13) Poskytovatel má právo Objednávku písemně odmítnout do jednoho pracovního dne od jejího doručení, neodmítne-li ji nebo nedoručí-li písemnou informaci o odmítnutí Objednateli ve lhůtě jednoho pracovního dne od doručení Objednávky, strany si ujednaly, že Objednávka se stává závaznou pro obě smluvní strany a vzniká platná dílčí smlouva.

14) Dílčí smlouva nabývá platnosti a účinnosti doručením Poskytovatelem podepsané dílčí smlouvy Objednateli. Tím není dotčen odst. 13 tohoto článku. V případě, že hodnota dílčí smlouvy přesáhne hodnotu 50.000 Kč bez DPH, účinnosti nabývá dílčí smlouva v souladu se zněním zákona č. 340/2015 Sb. (zákon o registru smluv). Zveřejnění dílčí smlouvy bez zbytečného odkladu zajistí na své náklady Objednatel a o jejím uveřejnění Poskytovatele bez zbytečného odkladu vyrozumí. Smluvní strany tímto stanovují, že v případě postupu dle věty 3. a 4. tohoto odstavce, je Poskytovatel povinen zkontrolovat, zda dílčí smlouva byla uveřejněna v souladu se zákonem o registru smluv. V případě, že Poskytovatel zjistí, že dílčí smlouva nebyla řádně uveřejněna v souladu se zákonem o registru smluv, je Poskytovatel povinen Objednatele o této skutečnosti bezodkladně informovat. V případě, že Objednatel neuveřejní dílčí smlouvu do 1 pracovního dne od upozornění Poskytovatele dle předchozí věty, je Poskytovatel oprávněn uveřejnit dílčí smlouvu v registru smluv v souladu se zákonem o registru smluv a o této skutečnosti Objednatele bezodkladně informovat.

15) V případě, že Poskytovatel Objednávku přijme s výhradou či s odchylkou, vzniká platná dílčí smlouva pouze, pokud Objednatel výhradu či odchylku písemně schválí a schválení doručí nejpozději nejbližší následující pracovní den Poskytovateli, jinak dílčí smlouva uzavřena není.

5. Místo a doba trvání

1) Smluvní strany tímto sjednávají, že dle povahy plnění bude Poskytovatel poskytovat servisní činnost jak vzdáleným přístupem, tak v místě sídla Objednatele uvedeném na titulní straně Smlouvy.

2) Poskytovatel se zavazuje započít s plněním dle Smlouvy bezodkladně po její účinnosti, nejdříve však dne 22.07.2025. Bezodkladně dle předchozí věty se rozumí nejpozději následující den po účinnosti Smlouvy.

6. Cena

1) Celková cena za celou dobu trvání Smlouvy nepřesáhne částku ve výši 1.491.000 Kč bez DPH (pro účely této smlouvy též jako „**Celková cena za plnění**“). Pro vyloučení pochybností smluvní strany uvádějí, že Celková cena za plnění se skládá z Celkové ceny

za poskytování servisní činnosti uvedené v odst. 2 tohoto článku a Celkové ceny pro náhradní díly dle odst. 4 tohoto článku.

2) Cena za poskytování servisní činnosti za dobu trvání Smlouvy bez maximální ceny náhradních dílů dle odst. 4 tohoto článku nepřesáhne částku ve výši 1.128.000 Kč bez DPH (pro účely této smlouvy též jako „**Celková cena za poskytování servisní činnosti**“).

3) Cena za poskytování servisní činnosti je sjednána jako paušální, a za jeden kalendářní měsíc činí částku ve výši 23.500 Kč bez DPH (dále jen „**Odměna**“).

4) Celková cena náhradních dílů za dobu trvání Smlouvy nepřesáhne částku ve výši 350 000,- Kč bez DPH (pro účely této smlouvy též jako „**Celková cena pro náhradní díly**“). Objednatel není povinen zaplatit tu část či celou uplatněnou cenu dílčí smlouvy dle čl. 4 odst. 7 Smlouvy ani cenu náhradních dílů použitých v souladu s čl. 4 odst. 6 Smlouvy, pokud součet všech Poskytovatelem uplatněných cen dle čl. 4 odst. 6 a 7 Smlouvy přesáhne 350 000,- Kč bez DPH.

5) Odměna bude Poskytovatelem fakturována v souladu s čl. 7 odst. 5 Smlouvy.

6) Odměna zahrnuje veškeré náklady Poskytovatele spojené s poskytováním plnění dle Smlouvy s výjimkou ceny náhradních dílů.

7) Odměna je nejvyšší přípustná a nepřekročitelná, s výjimkou změny sazby DPH v souvislosti se změnou právních předpisů upravujících výši daně z přidané hodnoty.

8) V případě, že je Poskytovatel registrovaným plátcem daně z přidané hodnoty (DPH), náleží mu k odměně za poskytnuté Služby rovněž DPH ve výši stanovené platnými právními předpisy. Poskytovatel je povinen tuto skutečnost doložit platným potvrzením o registraci k DPH. Ceny, včetně odměny, uvedené v čl. 6 budou v takovém případě navýšené o příslušnou sazbu DPH.

7. Platební podmínky

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

2) Objednatel neposkytuje Poskytovateli zálohy.

3) Lhůta splatnosti faktury činí 30 dnů od jejího doručení Objednateli, a to buď

   a. na adresu jeho sídla uvedenou na titulní straně Smlouvy,

   b. do datové schránky uvedené na titulní straně Smlouvy nebo

   c. na e-mail podatelny Objednatele: podatelna@mzd.gov.cz, v případě doručení faktury na e-mail podatelny musí faktura splňovat podmínky právních předpisů stanovené pro elektronickou fakturu a musí být ve formátu sdoc/isdocx (Information System Document) verze 5.2 a vyšší, jinak lhůta splatnosti nepočne běžet.

4) Fakturu za poskytovaní servisní činnosti vystaví vždy Poskytovatel bez zbytečného odkladu poté, co mu vznikne právo fakturovat poskytovanou servisní činnost. Právo fakturovat dle předchozí věty vzniká Poskytovateli vždy následující kalendářní měsíc po měsíci, ve kterém byla poskytována fakturovaná servisní činnost.

5) Poskytovatel vystaví fakturu za poskytnutí servisní činnosti vždy za předcházející kalendářní měsíc. V případě, že servisní činnost bude poskytována pouze část kalendářního měsíce, bude cena za tento měsíc odpovídat počtu dnů poskytované servisní činnosti. Cena dle předchozí věty bude vypočtena tak, že Odměna dle čl. 6 odst. 3 Smlouvy bude vydělena počtem dnů odpovídající počtu kalendářních dnů příslušného kalendářního měsíce a následně násobená počtem dní, kdy byla servisní činnost poskytována.

6) Fakturu za náhradní díly poskytnuté na základě čl. 4 odst. 6 a na základě uzavřených dílčích smluv dle čl. 4 odst. 7 a násl. Smlouvy vystaví Poskytovatel bez zbytečného odkladu poté, co mu vznikne právo fakturovat použité náhradní díly. Dnem vzniku práva dle předchozí věty je den, který je v dílčí smlouvě uveden jako termín plnění, bylo-li plnění v ní specifikované Poskytovatelem řádně a uvedeném termínu poskytnuto, jinak den, kdy Poskytovatel plnění řádně poskytl. Přílohou faktury bude soupis skutečně využitých náhradních dílů nezbytných k poskytnutí servisní činnosti.

7) V případě, že faktura nebude obsahovat náležitosti stanovené Smlouvou, je Objednatel oprávněn ji ve lhůtě splatnosti dle čl. 7 odst. 3 Smlouvy s odůvodněním vrátit Poskytovateli k přepracování, aniž by se dostal do prodlení se splatností takové faktury. Nová lhůta splatnosti o délce 30 dnů počíná běžet dnem doručení přepracované faktury Objednateli.

8) Objednatel bude hradit přijaté faktury pouze na bankovní účty Poskytovatele uvedené na titulní straně Smlouvy a zveřejněné správcem daně způsobem umožňujícím dálkový přístup ve smyslu § 96 odst. 2 zákona o DPH, přičemž řádnou úhradou vyúčtované ceny se rozumí odepsání částky z účtu Objednatele ve prospěch účtu Poskytovatele.

9) Poskytovatel prohlašuje, že správce daně před uzavřením této Smlouvy nerozhodl, že Poskytovatel je nespolehlivým plátcem ve smyslu § 106a zákona o DPH (dále jen „**nespolehlivý plátce**“). V případě, že správce daně rozhodne o tom, že Poskytovatel je nespolehlivým plátcem, zavazuje se Poskytovatel o tomto informovat Objednatele do 2 pracovních dnů. Stane-li se Poskytovatel nespolehlivým plátcem, uhradí Objednatel Poskytovateli pouze základ daně, přičemž DPH bude Objednatelem uhrazena přímo příslušnému správci daně.

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

8. Práva a povinnosti smluvních stran

1) Objednatel se zavazuje poskytnout Poskytovateli při provádění servisní činnosti v nezbytně nutném rozsahu potřebnou součinnost.

2) Objednatel se zavazuje Poskytovateli poskytnout veškeré informace o technických okolnostech, které mohou mít vliv na řádný provoz telekomunikačního systému.

3) Objednatel se zavazuje zajistit při provádění servisní činnosti uvolnění telekomunikačního systému z provozu na dobu nezbytně nutnou pro její provedení.

4) Poskytovatel je při provádění servisní činnosti povinen zajistit odbornou technickou úroveň svých pracovníků a jejich materiální vybavení.

5) Poskytovatel se zavazuje poskytovat servisní činnost v souladu s Politikou provozní bezpečnosti, poskytování a nabývání licencí programového vybavení a informací MZ ČR, která tvoří Přílohu č. 1.

6) Poskytovatel se zavazuje vést evidenci o veškerých změnách na telekomunikačním systému, včetně evidence uživatelských dat.

7) Poskytovatel se dále zavazuje poskytnout Objednateli veškeré informace potřebné k běžnému udržování telekomunikačního systému z hlediska uživatele.

9. Poddodavatelé a pojištění

1) Poskytovatel je povinen Objednatele informovat o všech svých poddodavatelích, uvedených spolu s rozsahem jimi poskytovaného plnění v Příloze č. 4 Smlouvy. Poskytovatel je povinen uvádět identifikační údaje poddodavatele v rozsahu, v jakém jsou uvedeny jeho vlastní identifikační údaje na titulní straně Smlouvy.

2) O změně v seznamu poddodavatelů je Poskytovatel povinen Objednatele informovat bez zbytečného odkladu poté, kdy s konkrétním poddodavatelem uzavřel smluvní vztah nebo nastala změna, nejpozději však do 7 dnů od okamžiku, kdy taková skutečnost nastala. Informační povinnost dle § 105 odst. 3 ZZVZ tím není dotčena.

3) Poskytovatel je oprávněn změnit poddodavatele, pomocí něhož prokázal část splnění kvalifikace v rámci zadávacího řízení veřejné zakázky, na jehož základě byla uzavřena Smlouva, jen z vážných důvodů a s předchozím písemným souhlasem Objednatele, přičemž nový poddodavatel musí disponovat kvalifikací ve stejném či větším rozsahu, než je kvalifikace, kterou původní poddodavatel prokázal za Poskytovatele. Poddodavatel, pomocí kterého Poskytovatel prokázal část splnění kvalifikace veřejné zakázky, bude poskytovat i tomu odpovídající část plnění. Objednatel nesmí souhlas se změnou poddodavatele bezdůvodně odmítnout, pokud mu budou příslušné doklady, v ujednané lhůtě, na které se smluvní strany předem dohodly, Poskytovatelem předloženy.

4) Zadání provedení části plnění dle Smlouvy, poddodavateli Poskytovatelem nezbavuje Poskytovatele jeho výlučné odpovědnosti za řádné provedení takového plnění vůči Objednateli. Poskytovatel odpovídá Objednateli za plnění předmětu Smlouvy, které svěřil poddodavateli, ve stejném rozsahu, jako by jej poskytoval sám.

5) Poskytovatel je povinen po celou dobu účinnosti Smlouvy udržovat v platnosti pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Poskytovatelem třetí osobě při výkonu jeho podnikatelské činnosti, přičemž pojistná částka takového pojištění musí činit nejméně 1.000.000 Kč se spoluúčastí maximálně 15.000 Kč na jednu pojistnou událost. Na výzvu Objednatele je plnění povinnosti dle předchozí věty Poskytovatel povinen bezodkladně, nejpozději však do 2 pracovních dnů prokázat, a to předložením dokladu o uzavřeném pojištění, přičemž takovým dokladem se rozumí pojistná smlouva, pojistka nebo potvrzení pojišťovny, resp. jiného pojistného zprostředkovatele o existenci pojištění dle tohoto ustanovení. Případ, kdy Poskytovatel nesplní povinnost prokázat existenci platné pojistné smlouvy dle předchozí věty, je podstatným porušením Smlouvy ze strany Poskytovatele.

10. Realizační tým

1) Poskytovatel se zavazuje, že servisní činnost bude poskytována výhradně členy realizačního týmu, kteří splňují požadavky stanovené v zadávací dokumentaci. Seznam členů realizačního týmu tvoří Přílohu č. 3 této Smlouvy.
2) Poskytovatel je povinen po celou dobu trvání Smlouvy na výzvu Objednatele prokázat, že disponuje realizačním týmem dle požadavků stanovených v zadávací dokumentaci. Povinnost dle předchozí věty splní, doloží-li bez zbytečného odkladu poté, co byl Objednatelem k prokázání disponování s realizačním týmem vyzván, nejpozději však do 5 pracovních dnů od takové výzvy, datované čestné prohlášení člena realizačního týmu, které v den předložení nebude starší než 3 dny, o tom, že se podílí na plnění veřejné zakázky.
3) Poskytovatel může v průběhu realizace veřejné zakázky změnit člena realizačního týmu pouze s předchozím písemným souhlasem Objednatele. Změnou realizačního týmu se pro účely této Smlouvy rozumí náhrada stávajícího člena realizačního týmu novým členem realizačního týmu nebo doplnění realizačního týmu novým členem realizačního týmu. Noví členové realizačního týmu musí splňovat všechny uvedené kvalifikační požadavky na členy realizačního týmu uvedené v zadávací dokumentaci. Je povinností Poskytovatele zajistit si písemný souhlas Objednatele se změnou člena realizačního týmu dříve, než dojde k poskytnutí plnění tímto členem realizačního týmu.
4) Poskytovatel se zavazuje, že po celou dobu trvání této Smlouvy bude realizační tým zahrnovat alespoň jednoho člena, který disponuje platným certifikátem Unify Certified Implementation & Support Specialist OpenScape 4000.
5) Případy, kdy by Poskytovatel nahradil člena realizačního týmu osobou, která nesplňuje požadavky stanovené zadávací dokumentací a touto Smlouvou na člena realizačního týmu nebo nenahradil člena realizačního týmu, jsou podstatným porušením Smlouvy ze strany Poskytovatele.
6) Smluvní strany tímto prohlašují, že změna realizačního týmu, tj. úprava Přílohy č. 3 Smlouvy nebudou považovat za změnu Smlouvy, která by musela být provedena dle čl. 16. odst. 8 Smlouvy. Změna realizačního týmu v důsledku postupu dle věty první tohoto článku je účinná udělením písemného souhlasu Objednatele Poskytovateli o změně či doplnění realizačního týmu.

11. Kontaktní osoby

1) Smluvní strany se zavazují si bez zbytečného odkladu sdělovat všechny relevantní informace nezbytné pro plnění Smlouvy, zejména informace o:
    a. zjištěných překážkách plnění;
    b. uplatněných nárocích třetích stran, které by mohly ovlivnit plnění Smlouvy;
    c. vznesených požadavcích státního dozoru.
2) Smluvní strany se zavazují, že veškerá sdělení, neurčí-li Smlouva jinak, budou činit písemně na adresy svých sídel uvedené na titulní straně Smlouvy nebo do datových schránek uvedených na titulní straně Smlouvy.

3) Komunikace mezi stranami bude probíhat prostřednictvím kontaktních osob, jimiž jsou:
   a. [redacted] v případě Objednatele;
   b. [redacted] v případě Poskytovatele.
4) Změna kontaktní osoby dle tohoto článku není změnou Smlouvy a vůči druhé smluvní straně je účinná dnem doručení oznámení o změně kontaktní osoby na e-mailovou adresu:
   a. ikt@mzd.gov.cz v případě Objednatele.
   b. servis@ignumtel.cz v případě Poskytovatele.

12. Ochrana informací a mlčenlivost

1) Poskytovatel se zavazuje zajistit utajení důvěrných informací a zachovávat mlčenlivost o všech skutečnostech získaných při plnění předmětu Smlouvy obvyklým způsobem pro utajování takových informací a dále v souladu s Přílohou č. 2.
2) Poskytovatel bere na vědomí, že Objednatel vystupuje jako orgán veřejné moci, který je povinen zajišťovat důvěrnost příslušných skutečností pouze v rozsahu stanoveném zákonem.
3) Povinnost zachovávat mlčenlivost se neuplatní v případech, kdy je Poskytovatel povinen příslušnou skutečnost sdělit na základě zákona, nebo je taková informace všeobecně dostupná, nebo v případě hájení oprávněných zájmů Poskytovatele.
4) Povinnost Poskytovatele zachovávat mlčenlivost dle čl. 12 Smlouvy trvá po dobu trvání Smlouvy i po jejím ukončení. Této povinnosti jej může zprostit pouze Objednatel svým písemným prohlášením

13. Odpovědnost za vady, odpovědnost za újmu

1) Poskytovatel odpovídá za řádné a včasné provedení servisních činností ve lhůtě dle Smlouvy. Poskytovatel poskytuje záruku na provedené servisní činnosti, jejichž předmětem je oprava telekomunikačního systému, nebo jeho součásti, a to na 24 měsíců ode dne provedení takové opravy. Záruka dle věty první tohoto odstavce se vztahuje na vady vzniklé v důsledku vadné práce nebo vadného materiálu použitých při poskytnutí servisní činnosti.
2) V případě vzniku vady, na kterou se vztahuje záruka poskytnutá Poskytovatelem, má Objednatel právo na její bezplatné odstranění ve lhůtě 24 hodin od jejího oznámení. Do lhůty se nezapočítává čas mimo pracovní dobu dle čl. 4 odst. 1 Smlouvy ve spojení s čl. 4 odst. 5 Smlouvy.
3) Práva ze vadného plnění bude Objednatel uplatňovat písemnou reklamací. Písemná forma reklamace je dodržena i v případě, že je reklamace Objednatelem uplatněna na e-mailové adrese Poskytovatele uvedené v čl. 11 odst. 3 písm. b) Smlouvy.
4) Právo z vadného plnění lze uplatnit kdykoliv během záruční doby. Za včas uplatněné právo z vadného plnění se považuje i případ, kdy reklamace byla odeslána poslední den záruční doby, ale Poskytovateli byla doručena později.
5) Neodstraní-li Poskytovatel reklamovanou vadu v určené lhůtě, je Objednatel oprávněn takovou vadu odstranit na náklady Poskytovatele prostřednictvím třetí osoby.

6) Uplatněním práv z vadného plnění nejsou dotčena práva Objednatele na náhradu újmy a zaplacení smluvní pokuty.

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

8) Žádná ze smluvních stran není povinna nahradit újmu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé smluvní strany.

9) V případě, že Objednatel poskytl Poskytovateli chybné zadání a Poskytovatel s ohledem na svou povinnost provádět servisní činnost s odbornou péčí mohl chybnost takového zadání zjistit, smí se ustanovení předchozí věty dovolávat pouze v případě, že na chybné zadání Objednatele písemně upozornil a Objednatel trval na původním zadání.

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

14. Sankční ujednání

1) V případě prodlení Poskytovatele s poskytnutím servisní činnosti dle čl. 4 odst. 4 Smlouvy, je Poskytovatel povinen Objednateli uhradit smluvní pokutu ve výši 500 Kč za každou započatou hodinu prodlení.

2) V případě prodlení Poskytovatele s odstraněním vady dle čl. 13 odst. 2 Smlouvy je Poskytovatel povinen Objednateli uhradit smluvní pokutu ve výši 500 Kč za každou započatou hodinu prodlení.

3) V případě porušení povinnosti včasného předložení dokladu o uzavřeném pojištění stanovené v čl. 9 odst. 5 Smlouvy je Poskytovatel povinen Objednateli uhradit smluvní pokutu ve výši 1.000, - Kč za každý den započatý den prodlení.

4) V případě porušení povinnosti ochrany důvěrných informací nebo porušení povinnosti mlčenlivosti dle čl. 12 Smlouvy je Poskytovatel povinen Objednateli uhradit smluvní pokutu ve výši 100.000 Kč za každé jednotlivé porušení povinnosti ochrany důvěrných informací nebo porušení povinnosti mlčenlivosti.

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

6) Dostane-li se Poskytovatel do prodlení se zaplacením smluvní pokuty, má Objednatel nárok na zaplacení zákonného úroku z prodlení dle nařízení vlády č. 351/2013 Sb., a to z částky uvedené ve výzvě k zaplacení smluvní pokuty dle čl. 14 odst. 5 Smlouvy.

7) Ujednání o smluvní pokutě nezbavuje Poskytovatele povinnosti nahradit v plném rozsahu újmu, která Objednateli v důsledku porušení utvrzované povinnosti vznikla.

15. Ukončení smlouvy

1) Smlouva se uzavírá na dobu určitou, a to na dobu 48 měsíců ode dne nabytí účinnosti, počítanou nejdříve však od 22.07.2025.

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

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

4) Obě smluvní strany mohou od této Smlouvy, jako i od dílčí smlouvy, odstoupit v případech stanovených občanským zákoníkem nebo touto Smlouvou.

5) Objednatel je oprávněn od Smlouvy, jako i od dílčí smlouvy odstoupit v případech podstatného porušení Smlouvy ze strany Poskytovatele. Za podstatné porušení Smlouvy se mimo případy výslovně ve Smlouvě uvedené považuje též:

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

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

   c. případ, kdy Poskytovatel opakovaně porušuje povinnosti ze Smlouvy, ačkoli byl na taková porušení opakovaně Objednatelem bezvýsledně písemně upozorněn;

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

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

   f. případ, kdy Poskytovatel opakovaně (nejméně dvakrát) Objednávku písemně odmítne.

6) Odstoupení od Smlouvy dle čl. 15 odst. 4 a 5 Smlouvy musí mít písemnou formu, kdy účinky odstoupení nastávají doručením oznámení o odstoupení smluvní straně, případně pozdějším datem stanoveným v odstoupení od Smlouvy.

7) Odstoupením se závazek touto Smlouvou založený zrušuje pouze ohledně nesplněného zbytku plnění (tj. *ex nunc*). Smluvní strany si jsou povinny vyrovnat dosavadní vzájemné závazky ze Smlouvy, a to bez zbytečného odkladu, nejpozději však do 30 dnů od doručení oznámení smluvní strany o odstoupení od této Smlouvy.

8) Odstoupením od příslušné dílčí smlouvy se závazek založený konkrétní Objednávkou zrušuje od počátku (*tj. ex tunc*) a strany dílčí smlouvy si jsou povinny vrátit vše, co si plnily, a to bez zbytečného odkladu, nejpozději však do 30 dnů od doručení oznámení odstupující strany o odstoupení od konkrétní dílčí smlouvy.

9) V případě zániku této Smlouvy, zanikají též veškeré dosud nesplněné dílčí smlouvy, nedohodnou-li se smluvní strany písemně v případě konkrétních dílčích smluv jinak. Dohoda dle předchozí věty musí být písemná a opatřena podpisy oprávněných osob obou smluvních stran. Na dílčí smlouvu, která zánikem této Smlouvy nezaniká, se pak použijí příslušné části této Smlouvy, i přesto, že zanikla.

10) Ukončením Smlouvy jakýmkoli ze způsobů uvedených v čl. 15 Smlouvy nejsou dotčena ustanovení týkající se smluvní pokuty, ochrany důvěrných informací, náhrady škody a jiných závazků, přetrvávajících ze své povahy i po ukončení Smlouvy.

16. Závěrečná ustanovení

1) Smlouva nabývá platnosti dnem podpisu poslední smluvní strany a účinnosti uveřejněním v registru smluv. Uveřejnění Smlouvy v registru smluv zajistí Objednatel. Smluvní strany tímto stanovují, že Poskytovatel je povinen zkontrolovat, zda Smlouva byla uveřejněna v souladu se zákonem o registru smluv. V případě, že Smlouva nebyla řádně uveřejněna v souladu se zákonem o registru smluv, je Poskytovatel povinen Objednatele o této skutečnosti bezodkladně informovat. V případě, že Objednatel neuveřejní Smlouvu do 1 pracovního dne od upozornění Poskytovatele dle předchozí věty, je Poskytovatel oprávněn uveřejnit Smlouvu v registru smluv v souladu se zákonem o registru smluv a o této skutečnosti Objednatele bezodkladně informovat.

2) Smlouva je vyhotovena elektronicky a podepsána kvalifikovaným elektronickým podpisem oprávněného zástupce Objednatele ve smyslu ust. § 5 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, v účinném znění (dále jen „**zákon č. 297/2016 Sb**.“), ve spojení s ust. § 11 zákona č. 297/2016 Sb., a uznávaným elektronickým podpisem oprávněného zástupce Poskytovatele ve smyslu ust. § 6 zákona č. 297/2016 Sb. Každá smluvní strana obdrží elektronicky podepsaný originál ve formátu pdf.

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

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

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

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

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

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

9) Nedílnou součástí Smlouvy jsou i její přílohy:

   - Příloha č. 1 – Politika provozování bezpečnosti, poskytování a nabývání licencí programového vybavení a informací MZ ČR

- Příloha č. 2 – Ochrana informací
- Příloha č. 3 – Realizační tým
- Příloha č. 4 – Seznam poddodavatelů

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

V Praze dne	V Praze dne
Za Objednatele	Za Poskytovatele
…….	…….
Ing. Jan Gábriš	**Michal Filip**
ředitel odboru IT	jednatel
Česká republika - Ministerstvo zdravotnictví	IGNUM Telekomunikace s.r.o.

Příloha č. 2 Výzvy

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

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

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

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

Obsah

Seznam zkratek a pojmů

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

1 Úvod

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

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

1.1 Závaznost politiky

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

1.2 Revize politiky

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

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

2 Politika provozní bezpečnosti

2.1 Řízení bezpečnosti komunikací a provozu

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

2.1.1 Pravomoci a odpovědnosti spojené s bezpečným provozem

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

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

2.1.2 Postupy bezpečného provozu

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

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

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

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

2.1.3 Požadavky a standardy bezpečného provozu

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

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

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

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

2.1.4 Řízení technických zranitelností

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

Náprava odhalených zranitelností může zahrnovat některé z následujících kroků:

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

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

V případě zranitelností s vysokou mírou rizika a rozsáhlým dopadem do ICT infrastruktury stanoví Manažer kybernetické bezpečnosti ve spolupráci se správci dotčených technických aktiv s přihlédnutím k průběžnému provoznímu riziku a možnostem jeho zmírnění předpokládaný časový harmonogram nápravy. Tato povinnost se týká zejména zranitelností, které jsou aktivně zneužívány, nebo u kterých toto zneužití bezprostředně hrozí. Mezi hlavní

možnosti zmírnění rizika patří např. nasazení patchů zranitelných systémů, znepřístupnění či vypnutí služeb, nasazení filtrů na hranici perimetru. Konečné rozhodnutí o způsobu řešení dané situace přijme Manažer kybernetické bezpečnosti a následně jej komunikuje všem dotčeným pracovníkům odpovídajícím způsobem.

Povinností Manažera kybernetické bezpečnosti a Garantů technických aktiv je zejména:

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

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

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

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

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

2.2 Řízení změn

V rámci řízení změn jsou:

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

U významných změn se provádí:

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

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

2.3 Řízení přístupu

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

2.3.1 Princip minimálních oprávnění

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

2.3.2 Požadavky na řízení přístupu

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

2.3.3 Životní cyklus řízení přístupu

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

2.3.4 Řízení privilegovaných oprávnění

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

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

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

2.3.5 Řízení přístupu pro mimořádné situace

V případě mimořádní situace je přípustné dočasné přidělení privilegovaných oprávnění v rozsahu nutném pro zvládání mimořádné situace, aplikaci nápravných opatření či nastolení normálního stavu pracovníkům či dodavatelům, kteří těmito oprávněními standardně nedisponují. Rozhodnutí o přidělení mimořádných oprávnění spadá do kompetence Manažera kybernetické bezpečnosti, takové rozhodnutí musí být spolu s rozsahem přidělených oprávnění řádně zdokumentováno.

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

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

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

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

2.4 Politika bezpečného chování uživatelů

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

2.4.1 Pravidla pro bezpečné nakládání s aktivy

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

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

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

2.4.2 Bezpečné použití přístupového hesla

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

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

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

2.4.3 Bezpečné použití elektronické pošty a přístupu na internet

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

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

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

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

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

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

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

2.4.4 Bezpečný vzdálený přístup

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

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

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

2.4.5 Bezpečné chování na sociálních sítích

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

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

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

2.4.6 Bezpečnost ve vztahu k mobilním zařízením.

Cílem je zajistit bezpečnost informací při používání mobilních zařízení.

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

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

2.5 Politika práce na dálku

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

2.6 Politika ochrany osobních údajů

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

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

2.7 Politika ochrany před škodlivým kódem

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

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

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

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

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

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

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

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

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

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

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

2.9 Politika bezpečného používání kryptografické ochrany

2.9.1 Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu

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

2.9.2 Pravidla kryptografické ochrany informací

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

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

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

Pro ochranu aktiv informačního a komunikačního systému se používají:

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

3 Politika poskytování a nabývání licencí

3.1 Pravidla a postupy nasazení programového vybavení a jeho evidence

3.1.1 Nasazování programového vybavení

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

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

3.1.2 Evidence licencí

3.1.2.1 Dokumentace

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

a) smlouvami na dodávky počítačového programu (pokud byly takovéto smlouvy uzavřeny),
b) nabývacími doklady,

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

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

3.1.2.2 Vedení evidence o instalaci počítačových programů

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

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

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

3.1.2.3 Vedení evidence o počítačových programech instalovaných na jednotlivých počítačích

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

a) odinstalování určitého počítačového programu,
b) instalace nového počítačového programu,
c) aktualizace stávajícího počítačového programu.

3.1.2.4 Vedení evidence o vyřazení počítačových programů

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

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

3.1.3 Převod práv k užívání počítačových programů

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

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

3.2 Pravidla a postupy pro kontrolu dodržování licenčních podmínek

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

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

4 Závěrečná ustanovení

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

Příloha č. 2 – Ochrana informací

1.1 Smluvní strany jsou si vědomy toho, že v rámci plnění závazků z této smlouvy:

1.1.1 si mohou vzájemně vědomě nebo opominutím poskytnout informace, které budou považovány za důvěrné, vč. osobních údajů vedených se spravovaných informačních systémech (dále jen „důvěrné informace"),

1.1.2 mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé strany nebo i jejím opominutím přístup k důvěrným informacím druhé strany.

1.2 Smluvní strany se zavazují, že žádná z nich nezpřístupní třetí osobě důvěrné informace, které při plnění této smlouvy získala od druhé smluvní strany.

1.3 Za třetí osoby podle odst. 1.2 se nepovažují:

1.3.1 zaměstnanci smluvních stran podílející se na plnění smlouvy, kteří dané důvěrné informace potřebují k plnění smlouvy, důvěrné informace jsou jim zpřístupněny výhradně za tímto účelem,

1.3.2 orgány smluvních stran a jejich členové,

1.3.3 ve vztahu k důvěrným informacím objednatele poddodavatelé poskytovatele, za předpokladu, že se podílejí na plnění této smlouvy nebo na plnění spojeným s plněním dle této smlouvy, důvěrné informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění důvěrných informací je v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny smluvním stranám v této smlouvě.

Smluvní strany se zavazují v plném rozsahu zachovávat povinnost mlčenlivosti a povinnost chránit důvěrné informace vyplývající z této smlouvy a též z příslušných právních předpisů, zejména povinnosti vyplývající ze zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů a 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). Smluvní strany se v této souvislosti zavazují poučit veškeré osoby, které se na jejich straně budou podílet na plnění této smlouvy, o výše uvedených povinnostech mlčenlivosti a ochrany důvěrných informací a dále se zavazují vhodným způsobem zajistit dodržování těchto povinností všemi osobami podílejícími se na plnění této smlouvy.

1.4 Budou-li informace poskytnuté objednatelem či třetími stranami, které jsou nezbytné pro plnění dle této smlouvy, obsahovat data podléhající režimu zvláštní ochrany podle zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů a 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), zavazuje se poskytovatel zabezpečit splnění všech ohlašovacích povinností, které citovaný zákon vyžaduje, a obstarat předepsané souhlasy subjektů osobních údajů předaných ke zpracování.

1.5 Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající strany a přijímající strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace. S výjimkou rozsahu, který je nezbytný pro plnění této smlouvy, se obě smluvní strany zavazují neduplikovat žádným způsobem důvěrné informace druhé strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto smlouvu. Obě strany se zároveň zavazují nepoužít důvěrné informace druhé strany jinak než za účelem plnění této smlouvy.

1.6 Nedohodnou-li se smluvní strany výslovně písemnou formou jinak, považují se za důvěrné implicitně všechny informace, které jsou anebo by mohly být součástí obchodního tajemství, tj. například, ale nejenom, popisy nebo části popisů technologických procesů a

vzorců, technických vzorců a technického know-how, informace o provozních metodách, procedurách a pracovních postupech, obchodní nebo marketingové plány, koncepce a strategie nebo jejich části, nabídky, kontrakty, smlouvy, dohody nebo jiná ujednání s třetími stranami, informace o výsledcích hospodaření, o vztazích s obchodními partnery, o pracovněprávních otázkách a všechny další informace, jejichž zveřejnění přijímající stranou by předávající straně mohlo způsobit škodu.

1.7 Bez ohledu na výše uvedená ustanovení se veškeré informace vztahující se k předmětu této smlouvy považují výlučně za důvěrné informace objednatele a poskytovatel je povinen tyto informace chránit v souladu se smlouvou a touto její přílohou. Poskytovatel při tom bere na vědomí, že povinnost ochrany těchto informací podle tohoto ustanovení se vztahuje pouze na poskytovatele.

1.8 Pokud jsou důvěrné informace poskytovány v písemné podobě anebo ve formě textových souborů na elektronických nosičích dat (médiích), je předávající strana povinna upozornit přijímající stranu na důvěrnost takového materiálu jejím vyznačením alespoň na titulní stránce nebo přední straně média. Absence takovéhoto upozornění však nezpůsobuje zánik povinnosti ochrany takto poskytnutých informací.

1.9 Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:

1.9.1 se staly veřejně známými, aniž by jejich zveřejněním došlo k porušení závazků přijímající smluvní strany či právních předpisů,

1.9.2 měla přijímající strana prokazatelně legálně k dispozici před uzavřením této smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy o ochraně informací,

1.9.3 jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany,

1.9.4 po podpisu této smlouvy poskytne přijímající straně třetí osoba, jež není omezena v takovém nakládání s informacemi,

1.9.5 mají být zpřístupněny na základě zákona či jiného právního předpisu včetně práva EU nebo závazného rozhodnutí oprávněného orgánu veřejné moci

1.9.6 jsou obsažené ve smlouvě a jsou zveřejněné v souladu s obecně závaznými právními předpisy.

1.10 Za porušení povinnosti mlčenlivosti smluvní stranou se považují též případy, kdy tuto povinnost poruší kterákoliv z osob uvedených v čl. 1.3 této přílohy, které daná smluvní strana poskytla důvěrné informace druhé smluvní strany.

1.11 Poruší-li poskytovatel povinnosti ohledně ochrany důvěrných informací vyplývající z této přílohy, je povinen zaplatit objednateli smluvní pokutu ve výši 100 000,- Kč za každé porušení takové povinnosti. Ustanovení o smluvní pokutě uvedená ve smlouvě se použijí v plném rozsahu i na tento případ.

1.12 Povinnost utajovat důvěrné informace podle této přílohy zavazuje poskytovatele ode dne účinnosti smlouvy a platí i po skončení doby trvání smlouvy.

1.13 Poskytovatel prohlašuje, že jeho poddodavatelé jsou oprávněni k přístupu k důvěrným informacím a osobním údajům a zavazuje se zajistit jejich prokazatelné proškolení dle platných právních předpisů, vč. prohlášení o mlčenlivosti dle zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů ve znění pozdějších předpisů a 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) a povinnosti prokázat svoji totožnost objednateli.

Příloha č. 3 – Realizační tým

Člen realizačního týmu č. 1

Titul, jméno a příjmení: [redacted]
Telefonní kontakt: [redacted]
e-mailová adresa: [redacted]@ignumtel.cz

Člen realizačního týmu č. 2

Titul, jméno a příjmení: [redacted]
Telefonní kontakt: [redacted]
e-mailová adresa: [redacted]@ignumtel.cz

Člen realizačního týmu č. 3

Titul, jméno a příjmení: [redacted]
Telefonní kontakt: [redacted]
e-mailová adresa: [redacted]@ignumtel.cz

Příloha č. 4 – Seznam poddodavatelů

IGNUM Telekomunikace s.r.o. tímto prohlašuje, že nebude využívat služeb poddodavatele.