Smlouva
o poskytování služeb správy, technické podpory, údržby telekomunikačního systému Unify OpenScape 4000 a zabezpečení provozuschopnosti koncových telefonních přístrojů a zařízení

Smluvní strany:

Registr. číslo	PRÁVNÍ ODBOR
	0419 / 21

Česká republika – Ministerstvo zdravotnictví ČR
se sídlem: Palackého nám. 4, 128 01
Praha 2
jednající: Ing. Martin Zeman, ředitel
odboru IT a elektronizace
zdravotnictví
IČ: 024341
(dále jen **„objednatel")** na straně
jedné
a
IGNUM Telekomunikace s.r.o.
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C vložka 120611
se sídlem: Vinohradská 190, 130 00 Praha 3
jednající: Michal Filip, jednatel
IČ: 27637417
DIČ: CZ27637417
bankovní spojení: Raifeissenbank a.s., 500500028/5500
(dále jen **„poskytovatel")** na straně druhé

objednatel a poskytovatel společně „**smluvní strany**" nebo jednotlivě jako „**smluvní strana**"

Smluvní strany uzavírají podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**") na základě veřejné zakázky malého rozsahu ***s názvem „Poskytování služeb správy, technické podpory, údržby telekomunikačního systému Unify OpenScape 4000 a zabezpečení provozuschopnosti koncových telefonních přístrojů a zařízení" (dále jen" veřejná zakázka")*** tuto smlouvu o poskytování služeb správy, technické podpory, údržby telekomunikačního systému Unify OpenScape 4000 MZČR a zabezpečení provozuschopnosti koncových telefonních přístrojů a zařízení (dále též jen „**smlouva**").

Čl. 1
Účel smlouvy

1. Účelem této smlouvy je závazek poskytovatele poskytnout objednateli plnění dle čl. 2 smlouvy a závazek objednatele zaplatit za to poskytovateli odměnu dle čl. 6 smlouvy.

Čl. 2
Předmět plnění

1. Předmět plnění zahrnuje
   a) poskytnutí služeb spočívajících v zajištění provozuschopnosti, správy, technické podpory, údržby telekomunikačního systému Unify OpenScape 4000 včetně jeho příslušenství (hlavního rozvodu, rack rozvaděčů, vnitřních rozvodů, DECT zařízení) (dále jen „**telekomunikační systém**“) a provozuschopnosti koncových telefonních přístrojů a zařízení v sídle zadavatele v rozsahu:
   - 600 digitálních poboček
   - 216 analogových poboček
   - 120 DECT telefonů
   - 40 BS DECT základnových stanic
   - Hlasová pošta
   - Tarifikační program Accountix,

   b) programové změny dat v telekomunikačním systému (telefonní ústředna) dle požadavků objednatele v sídle objednatele;
   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;
   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;
   h) řešení problémů spojených s telekomunikačním systémem ve vazbě na jednotnou telekomunikační síť;
   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 čl. 3 smlouvy

   (vše společně dále také jen „**služby**“)

2. Předmět plnění nezahrnuje:
   a) odstranění závad, které byly způsobeny neoprávněným zásahem do telekomunikačního systému cizími osobami, přičemž cizí osobou se rozumí osoba odlišná od zaměstnance objednatele, nebo poskytovatele
   b) odstraňování závad a opravy související s událostmi vyšší moci, kterými se rozumí mimořádné, nepředvídatelné a nepřekonatelná události vzniklé nezávisle na vůli objednatele a poskytovatele.
   c) globální rozšiřovací práce na systému.

Čl. 3
Povinnosti poskytovatele

1. Služby budou poskytovatelem poskytovány v pracovních dnech od 8.00 hod. do 17.00 hod. Cena za poskytované služby zahrnuje 20 návštěv poskytovatele v sídle objednatele měsíčně, včetně souvisejících nákladů (např. cestovné). Konkrétní data návštěv budou dojednána s pracovníkem objednatele.
2. Služby budou poskytovány výhradně členy realizačního týmu dle přílohy č. 3 smlouvy. Složení realizačního týmu bylo předloženo v nabídce poskytovatele podané ve výběrovém řízení veřejné zakázky a je pro poskytovatele závazné, stejně jako požadavky na členy realizačního týmu uvedené jako kritéria technické kvalifikace ve výzvě k podání nabídek do výběrového řízení veřejné zakázky.
3. V případě potřeby změny člena realizačního týmu oproti osobám uvedeným v příloze č. 3 smlouvy je změna možná pouze se souhlasem objednatele. Objednatel tento souhlas neudělí v případě, že by po takové změně tým nesplňoval veškeré požadavky zadavatele na realizační tým uvedené ve výzvě k podání nabídek do výběrového řízení veřejné zakázky.
4. Provádění služeb musí být v souladu s dokumentem Politika provozní bezpečnosti, poskytování a nabývání licencí programového vybavení a informací MZ ČR, který tvoří přílohu č. 2 smlouvy.
5. Poskytovatel se zavazuje při provádění služeb postupovat v souladu s přílohou č. 1 smlouvy (Ochrana informací) a neohrozit bezpečnost důvěrných informací, včetně osobních údajů vedených v telekomunikačním systému.
6. Poskytovatel se zavazuje:
   a) zahájit servisní zásah do 24 hod. od ohlášení závady dle čl. 4 smlouvy, do běhu této lhůty se nezapočítávají soboty, neděle a svátky,
   b) vést dokumentaci o veškerých změnách na telekomunikačním systému, včetně evidence uživatelských dat,
   c) poskytnout objednateli veškeré informace potřebné k rutinnímu udržování telekomunikačního systému z hlediska uživatele.

Čl. 4
Způsob ohlašování

1. Závady budou ohlašovány objednatelem poskytovateli telefonicky v pracovní dny od 8.00 hod. do 17.00 hod. na telefonní číslo [redacted] Pokud poskytovatel změní toto telefonní číslo, je povinen nové číslo neprodleně oznámit objednateli. Okamžikem rozhodným pro počátek běhu lhůty podle čl. 3 odst. 6 písm. a) smlouvy je v případě neúspěšného pokusu o nahlášení (poskytovatel hovor nepřijme, s číslem nelze spojit apod.) okamžik uskutečnění tohoto pokusu.

Čl. 5
Místo plnění

Místem plnění služeb dle této smlouvy je sídlo objednatele na adrese Palackého nám. 4, 128 01, Praha 2.

Čl. 6
Cena plnění

1. Cena za poskytování služeb **za jeden měsíc** činí 23.958Kč včetně DPH (slovy: Dvacetřitisícedevětsetpadesátosm korun českých), cena bez DPH činí 19.800 Kč a DPH ve výši 21 % činí 4.158 Kč.
2. Celková cena za poskytování služeb za 48 měsíců činí 1.149.984 Kč včetně DPH (slovy: Jedenmilionstočtyřicetdevěttisícdevětsetosmdesátčtyři korun českých), cena bez DPH činí 950.400 Kč a DPH ve výši 21 % činí 199.584 Kč.
3. Cena bez DPH zahrnuje veškeré náklady poskytovatele spojené s plněním předmětu této smlouvy, tj. i vedlejší náklady, které budou na plnění smlouvy poskytovatelem vynaloženy.
4. Celková cena bez DPH je stanovena jako nejvýše přípustná a není možné ji překročit.

Čl. 7
Oprávněné osoby

1. Oprávněnou osobou jednat ve věcech převzetí předmětu plnění po věcné, technické a servisní stránce za objednatele je [redacted] vedoucí oddělení informačních a komunikačních technologií a kybernetické bezpečnosti, tel.: [redacted], e-mail: [redacted]
2. Oprávněnou osobou poskytovatele jednat ve věcech smluvních, technických a servisních je [redacted]

Čl. 8
Platební a fakturační podmínky

1. Cena za poskytování služeb za jeden měsíc dle této smlouvy bude poskytovateli hrazena samostatně za každý měsíc, na základě faktur jím vystavených a zaslaných objednateli, ve výši dle čl. 6 odst. 1 smlouvy.
2. Poskytovatel je oprávněn fakturovat objednateli cenu za řádné plnění měsíčně zpětně.
3. Poskytovatel je povinen doručit fakturu objednateli na adresu uvedenou v záhlaví této smlouvy. Faktura musí obsahovat kromě náležitostí dle platných a účinných právních předpisů také evidenční číslo smlouvy objednatele uvedené v záhlaví smlouvy.
4. Fakturu za poskytnuté služby může poskytovatel vystavit nejdříve 3. den kalendářního měsíce následujícího po kalendářním měsíci, ve kterém tyto služby poskytl.
5. Jestliže faktura nebude obsahovat náležitosti uvedené v tomto článku smlouvy nebo bude obsahovat chybné údaje, je objednatel oprávněn fakturu až do uplynutí lhůty splatnosti poskytovateli vrátit, aniž by byl povinen uhradit cenu. Nová lhůta začíná běžet dnem doručení faktury se všemi náležitostmi objednateli.
6. Cena vyúčtovaná příslušnou fakturou bude hrazena ze strany objednatele bezhotovostně na bankovní účet poskytovatele uvedený v záhlaví smlouvy, přičemž řádnou úhradou vyúčtované ceny se rozumí odepsání částky z účtu objednatele ve prospěch účtu poskytovatele.
7. Smluvní strany se dohodly, že objednatel je oprávněn provést zajišťovací úhradu daně z přidané hodnoty ve smyslu ustanovení § 109a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, na účet příslušného poskytovatele daně, jestliže se poskytovatel stane ke dni uskutečnění zdanitelného plnění nespolehlivým plátcem daně ve smyslu ustanovené § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty.

8. Objednatel neposkytuje poskytovateli zálohy.
9. Případnou opravnou fakturu je poskytovatel povinen vystavit a odeslat do 14 kalendářních dnů od vyžádání objednatelem.

Čl. 9
Sankce

1. V případě porušení smlouvy spočívajícím v neprovedení služeb řádně a včas je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 5.000,- Kč za každé jednotlivé porušení.
2. Poskytovatel je povinen uhradit objednateli smluvní pokutu ve výši 5.000,- Kč za každý i započatý den trvání prodlení s odstraněním vady dle čl. 11 odst. 2 této smlouvy.
3. V případě nedodržení lhůty pro zahájení servisního zásahu uvedených v čl. 3 odst. 6 písm. a) smlouvy je poskytovatele povinen zaplatit objednateli smluvní pokutu ve výši 500,- Kč za každou započatou hodinu prodlení.
4. V případě prodlení objednatele s úhradou ceny za plnění je poskytovatel oprávněn požadovat po objednateli zaplacení úroků z prodlení ve výši určené nařízením vlády č. 351/2013 Sb., v platném znění.
5. Smluvní strany prohlašují, že s ujednanou výší smluvní pokuty souhlasí a považují ji za přiměřenou.
6. Smluvní pokuta je splatná ve lhůtě 14 dnů ode dne doručení faktury poskytovateli.

Čl. 10
Odpovědnost za škodu

1. Poskytovatel odpovídá za veškeré škody způsobené svou činností (včetně nečinnosti či opomenutí) a činností (včetně nečinnosti či opomenutí) případných poddodavatelů, které byly způsobeny objednateli nebo třetím osobám.
2. Omezení výše náhrady újmy se nepřipouští.
3. Objednatel je oprávněn požadovat náhradu újmy způsobené mu porušením povinností poskytovatelem i v případě, že se jedná o porušení povinnosti, na které se vztahuje smluvní pokuta, a to i ve výši přesahující smluvní pokutu.

Čl. 11
Odpovědnost za vady, záruka

1. Poskytovatel odpovídá za to, že služby budou prováděny v souladu s touto smlouvou v odpovídající odborné kvalitě a bez vad.
2. V případě, že objednatel zjistí vady poskytnutých služeb, oznámí toto písemně poskytovateli a poskytovatel je povinen tyto vady odstranit do 24 hodin od sdělení objednatele o vadách. S ohledem na charakter zjištěných vad je objednatel oprávněn stanovit poskytovateli lhůtu delší.
3. Poskytovatel je povinen vady odstraňovat i bez výslovné výzvy objednatele.
4. Poskytovatel odstraňuje vady na vlastní náklady.
5. Poskytovatel uhradí objednateli prokazatelné náklady vzniklé při uplatňování práv z odpovědnosti za vady.
6. Uplatněním odpovědnosti za vady nejsou dotčeny nároky na náhradu škody nebo na uplatnění smluvní pokuty.

7. Poskytovatel poskytuje záruku za jakost plnění po dobu 24 měsíců od data poskytnutí služby.

Čl. 12
Trvání smlouvy

1. Tato smlouva se uzavírá na dobu 48 měsíců ode dne nabytí účinnosti.
2. Tato smlouva končí:
   a) uplynutím doby podle odst. 1 tohoto článku;
   b) písemnou výpovědí jedné ze smluvních stran, nebo
   c) písemným odstoupením od smlouvy jedné ze smluvních stran pro její podstatné porušení druhou smluvní stranou.
3. Podstatným porušením smlouvy ze strany poskytovatele se rozumí zejména, nikoliv výlučně, opakované (minimálně dvakrát) neposkytnutí služby v souladu se smlouvou.
4. Smluvní strany se dohodly, že jsou oprávněny písemně vypovědět tuto smlouvu bez udání důvodu. Smlouva zanikne uplynutím 6 měsíců ode dne doručení písemné výpovědi druhé smluvní straně.
5. Objednatel je oprávněn tuto smlouvu vypovědět bez výpovědní doby v případě, že poskytovatel vstoupí do likvidace, je proti němu zahájeno insolvenční řízení či trestní stíhání.
6. Odstoupení od této smlouvy se nedotýká práva na náhradu újmy vzniklého z porušení smluvní povinnosti, práva na zaplacení smluvní pokuty a úroku z prodlení.

Čl. 13
Závěrečná ustanovení

1. Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem zveřejnění dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (dále jen „**zákon o registru smluv**“). Smlouva bude zveřejněna objednatelem.
2. Poskytovatel prohlašuje, že je srozuměn se skutečností, že objednatel je osobou povinnou ve smyslu zákona o registru smluv, je tak povinen o této smlouvě a právním vztahu jí založeném zpřístupňovat všechny informace, které zákon ze zpřístupňování nevylučuje.
3. Poskytovatel se zavazuje v plném rozsahu a v souladu s přílohou č. 1 smlouvy, zachovávat mlčenlivost a povinnost chránit důvěrné informace vyplývající z této smlouvy a též z příslušných právních předpisů, zejména ze 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).
4. Doplňování nebo změnu této smlouvy bude možné provádět jen se souhlasem obou smluvních stran, a to pouze formou písemných, vzestupně číslovaných dodatků.
5. Smluvní strany se dohodly, že korespondence mezi nimi bude doručována doporučeně na jejich adresy pro doručování korespondence uvedené v záhlaví této smlouvy.
6. Tato smlouva je vyhotovena ve 3 výtiscích s platností originálu, přičemž poskytovatel obdrží 1 vyhotovení, objednatel 2 vyhotovení. Předchozí věta neplatí v případě, že smlouva bude uzavřena v elektronické formě; v takovém případě obdrží každá smluvní strana elektronický soubor elektronicky podepsaný oběma smluvními stranami.
7. Na důkaz souhlasu s podmínkami této smlouvy připojuji smluvní strany své podpisy.

8. Nedílnou součástí smlouvy jsou tyto její přílohy:

   příloha č. 1 – Ochrana informací
   příloha č. 2 – Politika provozní bezpečnosti, poskytování a nabývání licencí programového vybavení a informací MZ ČR
   příloha č. 3 – Složení realizačního týmu

V Praze dne *(dle údaje u podpisu)*

Michal Filip, jednatel
IGNUM Telekomunikace s.r.o.

V Praze dne *(dle údaje u podpisu)*

_____

Ing. Martin Zeman
ředitel odboru IT a elektronizace zdravotnictví
ČR – Ministerstvo zdravotnictví

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.

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		
1.	27. 3. 2019		
Podpis			

Obsah

Seznam zkratek a pojmů

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

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.

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.

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.

Politika provozní bezpečnosti

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.

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.

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.

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,
- řídicí 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.

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

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.

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.

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.

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.

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).

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Politika ochrany před škodlivým kódem

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.

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.

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.

Politika bezpečného používání kryptografické ochrany

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.

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.

Politika poskytování a nabývání licencí

Pravidla a postupy nasazení programového vybavení a jeho evidence

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.

Evidence licencí

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.

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.

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.

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).

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).

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. 3 smlouvy

SEZNAM ČLENŮ REALIZAČNÍHO TÝMU

Vedoucí realizačního týmu:

- [redacted]

Člen:

- [redacted]

Člen:

- [redacted]