[redacted]

SMLOUVA O POSKYTOVÁNÍ SLUŽEB TECHNICKÉ PODPORY

komunikační brány MSp pro přístup ke správním evidencím a základním registrům

Smluvní strany

Česká republika - Ministerstvo spravedlnosti

se sídlem: Vyšehradská 16, 128 10 Praha 2

zastoupena: Ing. Janem Ladinem, ředitelem odboru informatiky

IČO: 00025429

(dále jen „**Objednatel**") **na straně jedné**

a

KOMIX s.r.o.

se sídlem: Drtinova 467/2a, Smíchov, 150 00 Praha 5

jejímž jménem jedná: Ing. Tomáš Rutrle, jednatel

IČO: 471 17 087

DIČ: CZ 471 17 087

zapsaná v Obchodním rejstříku vedeném Městským soudem v Praze, oddíl: C, vložka: 12440

(dále jen „**Poskytovatel**") **na straně druhé**

se dohodly, že ve smyslu § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „OZ") uzavírají níže uvedeného dne, měsíce a roku tuto

Smlouvu o poskytování služeb technické podpory
(dále jen „Smlouva")

Prohlášení smluvních stran

A. Objednatel prohlašuje, že je ústředním orgánem státní správy zřízený zákonem č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů, a že splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

B. Poskytovatel prohlašuje, že je právnickou osobou řádně založenou a zapsanou podle českého právního řádu v obchodním rejstříku vedeném Městským soudem v Praze, v oddíle C, číslo vložky 12440, a že splňuje veškeré podmínky a požadavky v této Smlouvě stanovené, a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

C. Smluvní strany uzavírají tuto Smlouvu, aby upravily vzájemná práva a povinnosti při poskytování služeb technické podpory s cílem poskytnout pevný základ právního vztahu.

D. Definice pojmů:

Doba odezvy: Doba, která uplyne od okamžiku doručení požadavku provedeného dohodnutým způsobem oprávněným pracovníkem Objednatele do první interakce Poskytovatele s Objednatelem s cílem potvrdit příjem požadavku.

Dostupnost služby: Časový rozsah, v kterém je služba poskytována.

Havarijní zásah: Havarijní zásah je zásah prováděný Poskytovatelem, který si lze vyžádat v situaci, kdy je systém v takovém stavu, že nelze normálně provozovat jeho běžné funkce, nebo kdy je z hlediska provozu nutné použít právě ty funkce, které se provádějí nesprávně. V případě plošně nasazených systémů se jedná o situace, kdy alespoň 30% uživatelů nemůže provádět běžné úkony.

Normální zásah: Akce Poskytovatele vyžádaná Objednatelem, která není Havarijním zásahem.

Požadavek: Pro účely této Smlouvy znamená obecně požadavek na odstranění vady, požadavek na změnu, požadavek na informaci nebo reklamaci.

Software: Programové vybavení.

Software Poskytovatele: Software, který byl vyvinut Poskytovatelem, Poskytovatel má k dispozici jeho zdrojové kódy a je oprávněn takový software upravovat.

Software třetí osoby: Software, který nebyl vyvinut Poskytovatelem, Poskytovatel tedy obvykle nemá k dispozici jeho zdrojové kódy a není oprávněn takový software upravovat nebo je rozsah jeho oprávnění omezen.

Článek 1
Předmět Smlouvy

1.1 Poskytovatel se zavazuje za podmínek stanovených v této Smlouvě, poskytovat Objednateli následující plnění (dále také jen „**Služby**“ nebo „**Služba**“):

Zajišťování technické podpory programového vybavení Objednatele uvedeného v Příloze č. 1, která sestává zejména z:

- Údržby programového vybavení definovaného v Příloze č. 1 (dále jen „**Programové vybavení**“);
- rozvoje Programového vybavení na základě změn v podmínkách poskytování dat ze strany provozovatele správních evidencí a registrům státní správy;
- poskytování součinnosti dodavatelům software;
- poskytování konzultace Hot-line;
- monitoringu systému;
- pohotovost k zásahu;
- odstraňování provozních problémů běhu aplikace;
- testování a instalace aktualizovaných verzí;
- příjem hlášení prostřednictvím ServiceDesk;
- vedení a správa ServiceDesk;
- neprofylaktická kontrola 6 hod měsíčně;
- zasílání informací Objednateli v elektronické podobě;
- účasti pracovníka Poskytovatele, do jehož kompetencí spadá předmět této smlouvy, na poradách se zástupci Objednatele a provozovatele správní evidence;
- aktualizace provozní, technické a uživatelské dokumentace.

1.2 Rozsah služeb a jejich parametry jsou definovány v článku 8 této Smlouvy.

1.3 Objednatel se zavazuje služby v souladu s touto Smlouvou průběžně přebírat a zaplatit za ně sjednanou cenu. Dále se zavazuje vyvinout a poskytovat stanovenou součinnost k zajištění sjednaných služeb.

Článek 2
Místo plnění

2.1 Místem plnění je sídlo Objednatele, kde je instalováno programové vybavení (uvedené v Příloze č. 1 této smlouvy), k němuž se váže podpora Poskytovatele, pokud se smluvní strany nedohodnou jinak.

2.2 Chce-li Objednatel změnit místo, kde je instalováno podporované programové vybavení, je povinen v dostatečné lhůtě předem s Poskytovatelem tuto změnu projednat a po dohodě s ním zajistit potřebné technicko-organizační podmínky pro pokračování poskytování služeb Poskytovatelem. Změna podmínek bude stvrzena písemným dodatkem této Smlouvy podepsaným oběma smluvními stranami.

Článek 3
Cena

3.1 Cena za poskytování Služeb specifikovaných ve Smlouvě v bodě 1.1 je hrazena formou měsíčního paušálního poplatku, který zahrnuje veškeré náklady Poskytovatele spojené s poskytováním těchto Služeb a činí 41 500,00 Kč bez DPH (slovy: čtyřicet jedna tisíc pět set korun českých) za každý kalendářní měsíc. DPH činí 8 715,00 Kč, celková cena včetně DPH činí 50 215,00 Kč (slovy: padesát jedna tisíc dvě stě patnáct korun českých).

3.2 Cena Předmětu plnění bude Objednatelem hrazena pouze za kalendářní měsíce, v nichž byly Služby poskytovány, tj. počínaje kalendářním měsícem, v němž bylo zahájeno poskytování Předmětu smlouvy dle Článku 1.1. Pokud doba poskytování Služeb nezačíná či nekončí prvním, resp. posledním dnem kalendářního měsíce, bude platba Ceny Paušálních služeb za příslušný kalendářní měsíc snížena o alikvotní část.

3.3 Tato cena je cenou nejvýše přípustnou a nepřekročitelnou, zahrnuje veškeré náklady Poskytovatele spojené s plněním Předmětu smlouvy a je platná po celou dobu realizace smlouvy.

3.4 Změna ceny je přípustná pouze v případě změny zákonem stanovené sazby DPH, na základě písemného dodatku, podepsaného k tomu oprávněnými zástupci obou smluvních stran. Ke sjednané ceně bez DPH se připočte daň z přidané hodnoty ve výši stanovené právními předpisy v době zdanitelného plnění.

Článek 4
Platební podmínky

4.1 Poskytovatel je oprávněn vystavit daňový doklad (dále také jen „Faktura") již den následující po uplynutí kalendářního měsíce, v němž byly Služby poskytovány.

4.2 Dnem zdanitelného plnění je den akceptace plnění. U služeb dle odst. 1.1 je dnem zdanitelného plnění poslední den období, v němž byla služba poskytována.

4.3 Daňový doklad musí obsahovat:

a. náležitosti stanovené § 435 zák. č. 89/2012Sb., občanský zákoník, ve znění pozdějších předpisů,

b. náležitosti stanovené zák. č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů,

c. evidenční číslo smlouvy objednatele,

4.4 Daňový doklad – Fakturu Poskytovatel objednateli doručí písemně, buď v listinné podobě na adresu Ministerstvo spravedlnosti ČR, Vyšehradská 16, 128 10 Praha 2 nebo elektronicky do datové schránky objednatele.

4.5 Pokud faktura neobsahuje všechny náležitosti, je Objednatel oprávněn ji do data splatnosti vrátit zpět k doplnění či opravě, aniž se tak dostane do prodlení. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněného či opraveného dokladu Objednateli.

4.6 Doba splatnosti faktury je sjednána na 30 (třicet) kalendářních dnů od data doručení faktury Objednateli. Takto sjednaná doba splatnosti, není-li průkazně dohodnuto jinak, nahrazuje den splatnosti uvedený na faktuře. V případě, že poslední den lhůty splatnosti faktury připadne na den pracovního klidu, resp. volna, bude se za den splatnosti považovat nejblíže následující pracovní den. Dnem úhrady je den podání bankovního příkazu k úhradě fakturované částky z účtu Objednatele ve prospěch účtu Poskytovatele. Platba faktury bude provedena bezhotovostním převodem na bankovní účet Poskytovatele uvedený na faktuře.

4.7 Objednatel neposkytuje zálohy a ani jedna smluvní strana neposkytla ani neposkytne druhé smluvní straně závdavek.

4.8 V případě prodlení Objednatele s úhradou fakturované ceny je Poskytovatel oprávněn požadovat úrok z prodlení z neuhrazené dlužné částky podle konkrétní faktury za každý den prodlení ve výši stanovené zvláštním právním předpisem v platném znění, kterým se stanoví výše úroků z prodlení (nařízení vlády č. 351/2013 Sb.).

Článek 5
Obecné podmínky služeb

5.1 Poskytovatel může odmítnout poskytnutí služby k programovému vybavení, které je užíváno v rozporu s licenční smlouvou o udělení práv k jeho užívání (licenční smlouvou) Poskytovatele.

5.2 Operační systém, programové vybavení užívané v souvislosti s programovým vybavením, ke kterému je poskytována služba, i technické vybavení, na kterém toto programové vybavení pracuje, musí vyhovovat technické specifikaci určené jeho výrobcem a musí splňovat požadavky stanovené výrobci programového vybavení, které má na předmětném technickém vybavení pracovat.

Článek 6
Odpovědnost za vady

6.1 Záruka za dodávku software třetích osob se řídí licenčními podmínkami příslušných výrobců.

6.2 Záruka na autorská díla Poskytovatele, konzultace, školení a služby poskytnuté Poskytovatelem činí 12 (dvanáct) měsíců od jejich převzetí Objednatelem.

6.3 Dodavatel nese veškeré náklady spojené s odstraňováním vad, a to včetně nákladů spojených s dopravou. Objednatel má právo na bezplatné odstranění vad.

6.4 Zárukou za jakost nejsou dotčena práva a povinnosti z vadného plnění plynoucí ze zákona.

6.5 Nároky z vad plnění se nedotýkají práv Objednatele na náhradu újmy vzniklé Objednateli v důsledku vady.

Článek 7
Měsíční výkaz

Objednatel může požádat Poskytovatele o předložení měsíčního výkazu. Poskytovatel měsíční výkaz předloží nejpozději do 15 dnů od žádosti Objednatele. Měsíční výkaz bude obsahovat:

7.1 vymezení stran;

7.2 evidenční číslo smlouvy objednatele;

7.3 seznam poskytnutých Služeb na základě Požadavků Objednatele;

7.4 výkaz provozních problémů včetně uvedení času nahlášení, času vyřešení a způsobu vyřešení.

Článek 8
Rozsah služeb

8.1 Poskytovatel se zavazuje poskytovat Objednateli služby v rozsahu definovaném touto Smlouvou.

8.2 Vymezení služeb poskytovaných Poskytovatelem:

8.2.1 Poskytovatel bude provádět údržbu programového vybavení prostřednictvím dálkového připojení při řešení problémů vzniklých při práci s podporovaným programovým vybavením, včetně možnosti telefonické konzultace, která může být vedena též elektronickou poštou.

8.2.2 Poskytovatel se zavazuje provozovat aplikaci ServiceDesk sloužící k evidenci a řízení plnění požadavků Objednatele a tuto aplikaci v rámci plnění této Smlouvy zpřístupnit prostřednictvím internetu vybraným pracovníkům Objednatele. Pro přístup k aplikaci ServiceDesk musí mít Objednatel k dispozici PC s připojením k síti internet tak, aby byl dosažitelný server KOMIX na adrese http://servicedesk.komix.cz, a dále instalaci internetového prohlížeče. Po uzavření Smlouvy budou Objednateli Poskytovatelem vytvořeny účty pro vybrané uživatele s přístupovým heslem.

8.2.3 Požadavek se uplatňuje prostřednictvím ServiceDesku Poskytovatele.

8.2.4 Návod k obsluze ServiceDesk Poskytovatel Objednateli zpřístupní od okamžiku platnosti této Smlouvy.

8.2.5 Servisní podmínky:

Služba/parametr	Hodnota parametru	Poznámka
ServiceDesk Dostupnost aplikace	24 x 7	S výjimkou technologických odstávek avizovaných na www.komix.cz
ServiceDesk - dostupnost služby - dostupnost telefonní a e-mailové linky Hot-line	7.00 – 17.00 v pracovní dny	telefonní linka hot-line: [redacted]

Služba/parametr	Hodnota parametru	Poznámka
Doba provádění servisních zásahů	7.00 – 17.00 v pracovní dny	
Havarijní zásah Doba odezvy	Maximální Doba odezvy technika k zahájení řešení incidentu 4 hod. od nahlášení požadavku Poskytovateli v době poskytování zásahu	viz definice pojmu Havarijní zásah
Normální zásah Doba odezvy	Maximální Doba odezvy technika k zahájení řešení incidentu 8 hod. od nahlášení požadavku Poskytovateli v době poskytování zásahu	viz definice pojmu Normální zásah

Požadavek zadaný mimo Dobu provádění servisních zásahů se považuje za doručený v 7.00 hod. následujícího pracovního dne a od tohoto okamžiku se počítá Doba odezvy.

8.2.6 Službami dle čl. 1.1 jsou také:

a) technická pomoc prostřednictvím dálkového připojení při řešení jednoduchých problémů vzniklých při práci s podporovaným Programovým vybavením, včetně možnosti telefonické konzultace, která může být vedena též elektronickou poštou.

b) pomoc při řešení složitějších problémů a fixací případných závad v podporovaném Programovém vybavení nebo závad, jejichž příčina je v interakci podporovaného Programového vybavení s dalším programovým vybavením pracujícím na podporovaných výpočetních systémech,

c) technická pomoc při problémech vzniklých při práci s podporovaným Programovým vybavením,

d) výkonová optimalizace provozu aplikace na vyžádání,

e) aktivní účast na změnách konfigurace podporovaného Programového vybavení,

f) poskytování informací o nových verzích a vlastnostech programového vybavení, k němuž se vztahuje tato Smlouva,

g) spolupráce na tvorbě a úpravách provozních předpisů a standardů pro provoz „Programového vybavení".

8.2.7 Administrace a technická podpora systémového programového vybavení Objednatele zahrnutá v paušálním poplatku dle článku 3 Smlouvy zahrnuje zejména:

a) instalaci nebo asistenci při instalaci software nebo jeho oprav,

b) administraci systému na vyžádání,

c) profylaktickou kontrolu systému na vyžádání,

d) řešení problémů spočívajících v nastavení „Programového vybavení" komunikací „Programového vybavení" s databázovým serverem nebo řešení dynamiky „Programového vybavení",

e) podporu Objednatele při řešení závad,

f) podporu a rozvoj Programového vybavení celkovém rozsahu do 6 (šest) hodin měsíčně.

8.2.8 Podpora poskytovaná dle této Smlouvy neobsahuje zejména:

a) poskytování médií, není-li to výslovně uvedeno v této Smlouvě,

b) služby, jejichž potřeba je vyvolána vadnou funkcí technického vybavení, jiného programového vybavení odlišného od Programového vybavení, k němuž je uzavírána tato Smlouva nebo vadou médií, která nebyla dodána Poskytovatelem,

c) na základě této Smlouvy nejsou poskytovány nové verze podporovaných produktů třetích stran, ani jejich vyšší nebo opravné verze nebo opravné patche,

d) služby, jejichž potřeba je vyvolána chybnou operací Programového vybavení, které není specifikováno v Příloze č. 1 k této Smlouvě, tzn., že služba není z titulu této Smlouvy poskytována na potřeby zajištění v oblasti správy operačního systému, síťového nastavení, nastavení firewallu a dalších softwarových prvků, které jsou součástí výpočetního systému, na kterém je „Programové vybavení" provozována,

e) řešení chyb programu vzniklých v důsledku jeho užití na jiném technickém vybavení nebo operačním systému, případně ve spojení s jiným spolupracujícím programovým vybavením, než je uvedeno v této Smlouvě,

f) řešení chyb programu, které se projevily v souvislosti s porušením Smlouvy o užití programu .

Článek 9
Povinnosti a práva Objednatele

9.1 Objednatel má právo na poskytování Služeb v rozsahu uvedeném v této Smlouvě.

9.2 Zásah si může vyžádat jen oprávněná osoba tj. osoba uvedená v této Smlouvě nebo osoba uvedená na seznamu předaném Objednatelem a písemně akceptovaném Poskytovatelem.

9.3 Objednatel je povinen poskytnout Poskytovateli součinnost při řešení provozního stavu, ke kterému si vyžádal Službu, včetně zásahu na místě. Je povinen zejména:

a) poskytnout Poskytovateli dodatečné informace,

b) provést na systému akce, které Poskytovatel Objednateli písemně (e-mailem) nebo telefonicky sdělí, a informovat jej neprodleně o jejich výsledku,

c) zajistit součinnost pracovníků znalých potřebných hesel a disponujících oprávněními nutnými k provedení zásahu.

9.4 Objednatel se zavazuje bez odkladu informovat Poskytovatele o všech závadách Programového vybavení nebo jeho dokumentace, které zjistí. Objednatel se zavazuje poskytnout Poskytovateli nezbytné doplňující informace týkající se závad Programového vybavení nebo jeho dokumentace, které si Poskytovatel vyžádá za účelem opakovaného vyvolání závady nebo její lokalizace.

9.5 Objednatel je povinen data na systému denně řádně zálohovat a pravidelně (1x týdně) provádět profylaktickou kontrolu celého „Programového vybavení" pokud některou z těchto povinností nepřevzal na sebe Poskytovatel. Zjištěné problémy ohlásí Poskytovateli.

9.6 V případě výskytu závady, která brání provozu „Programové vybavení" nebo výrazně omezuje možnosti jejího užití, je Objednatel povinen bez prodlení informovat Poskytovatele o povaze a rozsahu problému. Dále je povinen učinit kroky nezbytné k minimalizaci možných škod.

9.7 Změní-li Objednatel adresu, na níž je poskytována služba, nebo konfiguraci technického či Programového vybavení, bude tato změna po oznámení Poskytovateli zahrnuta do Smlouvy formou písemného dodatku k této Smlouvě. Objednatel se zavazuje o takové změně písemně informovat Poskytovatele v dostatečném předstihu.

9.8 Objednatel je povinen umožnit Poskytovateli vzdálený přístup např. přes internet k „Programovému vybavení" případně i přístup fyzický přímo k počítači a poskytnout součinnost svých pracovníků, zejména těch, kteří jsou oprávněni pracovat jako Správce systému a databáze.

9.9 Objednatel je povinen zajistit aktivní spolupráci jím pověřených osob.

Článek 10
Povinnosti Poskytovatele

10.1 Poskytovatel je povinen řádně a s odbornou péčí poskytovat službu v rozsahu definovaném touto Smlouvou.

10.2 Poskytovatel je povinen vyvarovat se poškození nebo zničení důležitých dat, která se ve výpočetním systému nacházejí. V případě nebezpečí ztráty dat během zásahu na systému je povinen písemně upozornit Objednatele nejméně 2 pracovní dny předem na nutnost tato data před tímto zásahem zazálohovat.

10.3 Poskytovatel je povinen respektovat a dodržovat pokyny Objednatele při plnění předmětu veřejné zakázky.

10.4 Poskytovatel je podle § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů.

Článek 11
Ochrana informací

11.1 Všechny informace, které se Poskytovatel dozví v souvislosti s plněním dle této dohody, jsou důvěrné povahy. Poskytovatel se zavazuje zachovávat o důvěrných informacích mlčenlivost a důvěrné informace používat pouze k plnění této dohody. Poskytovatel zodpovídá za porušení mlčenlivosti svými zaměstnanci, jakož i třetími osobami, které se na plnění předmětu této smlouvy podílejí.

11.2 Poskytovatel při plnění této smlouvy si je vědom povinností vyplývajících z platných právních předpisů upravujících ochranu osobních údajů, zejména z Obecného nařízení Evropské Unie o ochraně osobních údajů (GDPR). Poskytovatel je oprávněn zpracovávat osobní údaje v rozsahu nezbytně nutném pro plnění předmětu této smlouvy, za tímto účelem je oprávněn osobní údaje zejména ukládat na nosiče informací, upravovat, uchovávat po dobu nezbytnou k uplatnění práv prodávajícího vyplývajících z této smlouvy, předávat zpracované osobní údaje Objednateli, osobní údaje likvidovat, vše v souladu s platnými právními předpisy upravujícími ochranu osobních údajů, zejména s Obecným nařízením Evropské Unie o ochraně osobních údajů (GDPR).

11.3 V případě, že v souvislosti s plněním závazků podle této Smlouvy získá Poskytovatel přístup k informacím obsahujícím osobní nebo citlivé údaje klientů Objednatele, zavazuje se dodržovat mlčenlivost o všech těchto údajích vůči třetím osobám, zároveň se zavazuje učinit veškerá technická i organizační opatření, aby nedošlo k porušení povinností plynoucích Objednateli z obecně závazných právních předpisů.

11.4 Poskytovatel se zavazuje zajistit, aby všichni jeho zaměstnanci, jeho spolupracovníci, stejně jako jeho poddodavatelé zúčastnění na plnění této Smlouvy znali své povinnosti při zachování důvěrnosti informací, a aby dodržovali mlčenlivost dle režimu stanoveného v tomto článku. Tento závazek bude platit i při práci v prostorách Objednatele pro dodržování jeho IT interních

směrnic o bezpečnosti a pravidel užívání software, interní sítě a přístupu na Internet, s kterými Objednatel Poskytovatele seznámí.

11.5 Smluvní strany se zavazují k zachování mlčenlivosti o důvěrných a interních informacích druhé smluvní strany, se kterými v souvislosti s plněním předmětu této Smlouvy přijdou do styku. Tento závazek trvá i po splnění předmětu této Smlouvy.

11.6 Pokud jsou důvěrné informace poskytovány v písemné podobě nebo ve formě textových souborů na počítačových médiích, zavazují se smluvní strany učinit o předání průkazný záznam. Přitom je předávající strana povinna upozornit přijímající stranu na důvěrnost takového materiálu.

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

a) se staly veřejně známými, aniž by to zavinila úmyslně či z nedbalosti přijímající strana,

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

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

c) po podpisu této Smlouvy poskytne přijímající straně třetí osoba, jež takové informace přitom nezíská přímo ani nepřímo od strany, jež je jejich vlastníkem.

Článek 12
Smluvní pokuty

12.1 V případě, že Poskytovatel nedodrží Dobu odezvy, má Objednatel právo vyžadovat úhradu smluvní pokuty 10 % příslušného měsíčního paušálu za každou započatou dohodnutou jednotku Doby odezvy (hodina, den).

12.2 Zaplacením smluvní pokuty není dotčeno právo na náhradu škody.

12.3 V případě prokázaného porušení povinností sjednaných v článku 11 této Smlouvy je Objednatel oprávněn požadovat smluvní pokutu ve výši 100 000,- Kč (slovy: jedno sto tisíc korun českých) za každý jednotlivý případ.

12.4 Zaplacením smluvní pokuty není dotčeno právo na náhradu újmy ani právo na odstoupení od Smlouvy.

Článek 13
Odpovědnost za škodu

13.1 Smluvní strany nesou povinnost nahradit způsobenou škodu v rámci platných právních předpisů a této Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod. Smluvní strany se zavazují upozornit druhou smluvní stranu na riziko vzniku škody, které je jim známo.

13.2 Při provádění díla či jeho části prostřednictvím poddodavatele má Poskytovatel odpovědnost, jako by jej prováděl sám.

13.3 Žádná ze smluvních stran není odpovědna za prodlení způsobené okolnostmi vylučujícími odpovědnost. Smluvní strany se zavazují upozornit druhou smluvní stranu bez zbytečného odkladu na vzniklé okolnosti vylučující odpovědnost bránící řádnému plnění této Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání okolností vylučujících odpovědnost.

13.4 Náhrada újmy se řídí ustanovením § 2951 OZ.

Článek 14
Řešení sporů a další ujednání

14.1 Strany se zavazují, že veškeré spory vyplývající nebo související s ustanoveními této Smlouvy budou řešeny nejprve smírně. Nebude-li smírného řešení dosaženo v přiměřené době, bude mít kterákoliv ze stran právo takový spor předložit ke konečnému rozhodnutí místně příslušnému soudu v České republice.

14.2 Všechna autorská práva a jiné duševní vlastnictví existující před datem účinnosti Smlouvy budou patřit straně, která taková práva vlastnila bezprostředně před datem účinnosti Smlouvy. Žádná ze stran nezíská žádná vlastnická či autorská práva, patenty, obchodní tajemství, obchodní značky ani žádná jiná práva v oblasti duševního vlastnictví, která vlastní druhá strana.

14.3 Objednatel uděluje Poskytovateli souhlas s použitím názvu a předmětu Smlouvy dle článku 1 Smlouvy ve spojení s názvem Objednatele v seznamu referencí realizovaných projektů a v marketingových materiálech Poskytovatele.

14.4 Strany se dohodly, že zveřejnění obecných informací ve vztahu k předmětu plnění ve formě tiskových zpráv či případových studií je povoleno za podmínky, že text bude písemně odsouhlasen oběma smluvními stranami.

14.5 Objednatel je oprávněn uveřejnit celý text smlouvy na svých webových stránkách a v registru smluv, vše za předpokladu, nebrání-li uveřejnění zvláštní právní předpis. Poskytovatel s tímto zveřejněním souhlasí.

Článek 15
Trvání smlouvy

15.1 Smlouva se uzavírá na dobu určitou, tj. na dobu 4 let od účinnosti Smlouvy.

15.2 Smluvní strany se dohodly, že tato Smlouva může zaniknout následovně:

15.2.1 písemnou dohodou smluvních stran, včetně dohody o vyrovnání;

15.2.2 jednostranným odstoupením od Smlouvy pro její podstatné porušení s tím, že smluvní strany se dohodly, že ve smyslu § 2002 OZ pokládají za podstatné porušení této Smlouvy to, že druhá smluvní strana neplní ustanovení této Smlouvy a přes písemné upozornění nesjedná ve lhůtě 14 dnů nápravu;

15.2.3 jednostranným odstoupením Objednatele nebude-li schválena částka ze státního rozpočtu následujícího roku, která je potřebná k úhradě za plnění poskytované podle této smlouvy v následujícím roce;

15.2.4 jednostranným odstoupením Objednatele v případě, že v insolvenčním řízení bude zjištěn úpadek Poskytovatele nebo insolvenční návrh byl zamítnut pro nedostatek majetku Poskytovatele (v souladu se zněním zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů. Objednatel je rovněž oprávněn odstoupit od smlouvy v případě, že Poskytovatel vstoupí do likvidace;

15.2.5 písemnou výpovědí smluvní strany s tříměsíční výpovědní dobou, která počíná běžet 1. (prvním) dnem měsíce následujícího po měsíci, kdy byla výpověď doručena druhé smluvní straně.

15.2.6 Dojde-li

(a) k přeměně společnosti Poskytovatele nebo

(b) ke změně vlastnické struktury společnosti Poskytovatele nebo ke změně podílu na hlasovacích právech ve společnosti Poskytovatele, v jejichž důsledku se změní ovládající osoba oproti dni uzavření smlouvy,

je Poskytovatel povinen písemně oznámit tuto skutečnost Objednateli ve lhůtě 10 kalendářních dnů od účinnosti této změny. Objednatel je v tomto případě oprávněn písemně vypovědět dohodu. Výpovědní doba činí 10 kalendářních dnů a počíná běžet dnem následujícím po jejím doručení Poskytovateli.

15.2.7 Odstoupením od smlouvy nezaniká právo na uplatnění smluvní pokuty.

Článek 16
Závěrečná ustanovení

16.1 Poskytovatel je povinen dodržovat Instrukci Ministerstva spravedlnosti, čj. 53/2015-OI-SP, o zajištění bezpečnosti informací v prostředí informačních a komunikačních technologií resortu spravedlnosti, která je příloho č. 2 této Smlouvy.

16.2 Pracovník Objednatele oprávněný uplatnit Požadavek a provést kontrolu a převzetí provedených prací je za „Programové vybavení":

Jiří Mařík
tel.:
e-mail: [redacted]

Případné změny kontaktních osob oznámí smluvní strana písemně druhé smluvní straně. Ustanovení čl. 16.10 Smlouvy se nepoužije.

16.3 Při rozhodování případných sporů, vzniklých ze závazkových vztahů založených touto smlouvou, budou místně a věcně příslušné soudy České republiky.

16.4 Smluvní strany v souladu s ustanovením § 558 odst. 2 občanského zákoníku vylučují použití obchodních zvyklostí na právní vztahy vzniklé z této smlouvy.

16.5 Smluvní strany souhlasně prohlašují, že tato smlouva není smlouvou uzavřenou adhezním způsobem ve smyslu ustanovení § 1798 a násl. občanského zákoníku.

16.6 Prodávající výslovně prohlašuje, že na sebe přebírá nebezpečí změny okolností ve smyslu ustanovení § 1765 odst. 2 občanského zákoníku.

16.7 Smluvní strany prohlašují, že tato Smlouva obsahuje veškerý projev jejich shodné vůle a mimo ni neexistuji žádná ujednání v jiné než písemné formě, která by ji doplňovala, měnila nebo mohla mít význam při jejím výkladu, a že se tedy žádná ze smluvních stran nespoléhá na prohlášení druhé smluvní strany, které není uvedeno v této smlouvě, jejích přílohách či dodatcích. Tím není dotčen význam následné komunikace stran, včetně pokynů Objednatele.

16.8 Stane-li se některé ustanovení této smlouvy neplatným, zdánlivým či neúčinným, nemá tato skutečnost vliv na ostatní ustanovení této smlouvy, která zůstávají platná a účinná. Smluvní strany se v tomto případě zavazují písemnou dohodou nahradit ustanovení, které bylo shledáno neplatným, zdánlivým či neúčinným novým ustanovením, které po obsahové stránce nejlépe odpovídá zamýšlenému účelu původního ustanovení. Do té doby platí odpovídající úprava obecně závazných právních předpisů České republiky.

16.9 Smlouva je vyhotovena ve 4 (čtyřech) stejnopisech, které mají všechny platnost originálu, z nichž 2 (dva) stejnopisy obdrží Objednatel a 2 (dva) stejnopisy obdrží Poskytovatel.

16.10 Tato Smlouva představuje úplnou dohodu smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit a doplňovat pouze listinnými, písemnými, oboustranně

odsouhlasenými, podepsanými a postupně číslovanými dodatky v českém jazyce, které se stávají její nedílnou součástí.

16.11 Nedílnou součást Smlouvy tvoří tato příloha: Příloha č. 1 - Specifikace programového vybavení

16.12 Smluvní strany potvrzují, že si tuto Smlouvu před podpisem přečetly, jsou seznámeny s jejím obsahem, rozumí jejímu textu, považují jej za zcela určitý a srozumitelný a prohlašují, že Smlouva nebyla ujednána v tísni ani za nápadně nevýhodných podmínek.

16.13 Tato Smlouva nabývá platnosti dnem podpisu oběma smluvními stranami. Účinnost Smlouvy nastává okamžikem jejího uveřejnění v registru smluv. Uveřejnění v registru smluv zajistí Objednatel.

V dne 30 -05- [redacted]

KOMIX s.r.
Drtinova 467/2a, 150 00
IČO: 47117087, DIČ: CZ
Tel: [redacted]

V Praze, dne 30 -05- 2019

[redacted]

Objednatel

Ing. Jan Ladin,

ředitel odboru informatiky

Ministerstvo spravedlnosti České republiky * 51 *

Příloha č. 1 - Specifikace programového vybavení

Programové vybavení, ke kterému se vztahuje Poskytovatelem poskytovaná podpora:

- Komunikační brána Objednatele připojení na správní evidence Ministerstva vnitra;
- Komunikační brána Objednatele připojení na základní registry;
- Webové rozhraní pro přístup k auditním údajům komunikační brány.

Příloha č. 2 - Instrukce Ministerstva spravedlnosti, čj. 53/2015-OI-SP

Instrukce

Ministerstva spravedlnosti

ze dne 23. února 2016,

MSP-53/2015-OI-SP

o zajištění bezpečnosti informací v prostředí informačních a komunikačních technologií resortu spravedlnosti

Ministerstvo spravedlnosti stanoví:

ČÁST PRVNÍ

ÚVODNÍ USTANOVENÍ

§ 1

Působnost instrukce

(1) Tato instrukce stanoví cíle, principy, pravidla a postupy pro řízení bezpečnosti v prostředí informačních a komunikačních technologií v resortu Ministerstva spravedlnosti České republiky, a to v následujících organizačních složkách státu:

- Ministerstvo spravedlnosti České Republiky (dále jen „ministerstvo"),
- Nejvyšší správní soud,
- Nejvyšší soud,
- vrchní soudy,
- krajské soudy (Městský soud v Praze),
- okresní (obvodní) soudy a Městský soud v Brně,
- Nejvyšší státní zastupitelství,
- vrchní státní zastupitelství,
- krajská státní zastupitelství (Městské státní zastupitelství v Praze),
- Vězeňská služba České republiky,
- Zotavovna Vězeňské služby České republiky,
- Rejstřík trestů,
- Justiční akademie,
- Probační a mediační služba,
- Institut pro kriminologii a sociální prevenci,

dále jen „justiční složka".

(2) Tato instrukce platí i pro organizační složky resortu ministerstva, které budou zřízeny po datu účinnosti této instrukce, nestanoví-li vnitřní předpis jinak.

(3) Za plnění povinností vyplývajících z této instrukce odpovídají a činí právní úkony:

ministr spravedlnosti,

předsedové:

- Nejvyššího správního soudu,

- Nejvyššího soudu,
- vrchních soudů,
- krajských soudů (Městského soudu v Praze),
- okresních (obvodních) soudů a Městského soudu v Brně;

nejvyšší státní zástupce,

vrchní státní zástupci,

krajští státní zástupci (Městský státní zástupce v Praze),

generální ředitel Vězeňské služby České republiky;

ředitelé:

- Rejstříku trestů,
- Justiční akademie,
- Probační a mediační služby,
- Zotavovny Vězeňské služby České republiky,
- Institutu pro kriminologii a sociální prevenci,

(dále jen „vedoucí justiční složky").

(4) Prostředím informačních a komunikačních technologií (dále jen „ICT") resortu justice se rozumí informační systémy, výpočetní technika včetně mobilních zařízení a přídavných zařízení, veškeré počítačové sítě, komunikační infrastruktura, nosiče informací a programové vybavení justičních složek. Prostředí ICT dále zahrnuje dokumentaci ICT, správu ICT, bezpečnostní správu ICT a práci uživatelů využívajících prostředků ICT.

§ 2

Rozsah a hranice systému řízení bezpečnosti informací

(1) Řízení bezpečnosti informací v prostředí ICT se týká:

a) veškerého hardware a software,
b) uložených zpracovávaných nebo přenášených informací,
c) dokumentace prostředí ICT,
d) veškerých činností spojených s užitím služeb a prostředků prostředí ICT, jeho provozní správou, bezpečnostní správou a používáním nosičů informací (včetně služeb zajišťovaných dodavatelským způsobem) a
e) veškerých etap životního cyklu prostředí ICT.

(2) Tato instrukce se nevztahuje na systémy obsahující nebo zpracovávající utajované informace podle zákona o ochraně utajovaných informací[1].

ČÁST DRUHÁ

POLITIKA SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

§ 3

Cíle řízení bezpečnosti informací

(1) Cílem činností v oblasti bezpečnosti informací v prostředí ICT resortu justice je podporovat plnění úkolů justičních složek, zajistit jejich kontinuitu a ochránit dobré jméno justičních složek tím, že omezuje možná narušení jejich činností, následky bezpečnostních incidentů a zajišťuje potřebnou důvěrnost, integritu a dostupnost informací v prostředí ICT.

(2) Základní strategické cíle řízení bezpečnosti informací jsou:

[1] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

a) Zajištění bezpečného a důvěryhodného provozu justičních složek a ochrany jejich dobrého jména tím, že omezuje možná narušení činností justičních složek a následků bezpečnostních incidentů.
b) Splnění právních a dalších externích požadavků na bezpečnost.
c) Maximálně efektivní zajištění bezpečnosti odpovídající hodnotě relevantních částí chráněného ICT prostředí.

(3) Specifické cíle řízení bezpečnosti informací vychází ze strategických cílů a naplňují následující povinnosti, za jejichž splnění zodpovídají osoby podle paragrafu 1, odstavce 3 této instrukce.:

a) Zajištění ochrany informací justičních složek (informací ve veškerých formátech dat, uložených v počítačích a/nebo na nosičích informací, přenášených po komunikační infrastruktuře a předávaných mezi informačními systémy) před hrozbami vnějšími nebo vnitřními, úmyslnými nebo neúmyslnými.
b) Zajištění důvěrnosti informací – informace mají být dostupné jen tomu, kdo je k tomu oprávněn a potřebuje je znát ke své práci. Je třeba zajistit přiměřenou úroveň ochrany před neoprávněným přístupem a zveřejněním informací.
c) Zajištění integrity informací – informace mohou být měněny pouze oprávněnými osobami nebo na pokyn oprávněných osob a řízeným způsobem. Správnost a úplnost informací nesmí být narušena neoprávněnými ani neúmyslnými změnami.
d) Zajištění dostupnosti informací – informace musí být dostupné oprávněným osobám tehdy, když je potřebují.
e) Dodržování požadavků právních norem a dalších předpisů, se zvláštním zřetelem na zákon o kybernetické bezpečnosti[2], zákon o ochraně osobních údajů[3], zákon o informačních systémech veřejné správy[4], zákon o elektronickém podpisu[5] a směrnice EU.
f) Hlášení a vyšetření každého narušení bezpečnosti informací, podezření na toto narušení nebo zjištěné slabiny. Následné informování příslušných pracovníků složky (a to i v případě, kdy je zjistí pracovníci jiné justiční složky), odpovědných pracovníků resortu a zainteresovaných externích stran.
g) Efektivnost a přiměřenost opatření chránicích informace vzhledem k riziku – opatření (včetně mechanizmů systému řízení bezpečnosti informací) musí odpovídat významu chráněných informací, hrozbám, kterým jsou tyto informace vystaveny a identifikovaným potřebám v oblasti bezpečnosti informací.
h) Zvyšování bezpečnostního povědomí o bezpečnosti informací - poskytnutí informací o požadavcích a postupech při zajišťování bezpečnosti informací všem osobám přistupujícím k informacím a informačním systémům justičních složek.
i) Řízení a zajištění bezpečnosti informací při přístupu třetích stran k informacím a informačním systémům. Přístup k informacím, které nejsou veřejné, musí být upraven v příslušném smluvním vztahu.
j) Realizace služeb v oblasti ICT dodávaných třetími stranami musí být zajištěna na základě smluvního vztahu, který zajistí soulad s požadavky na zajištění bezpečnosti a nápravu případných nedostatků.

§ 4

Principy řízení bezpečnosti informací

Mezi základní principy bezpečnosti informací, které systém řízení bezpečnosti zohledňuje, patří:

a) V rámci justičních složek je zaveden jeden systém řízení bezpečnosti informací.
b) Zajištění bezpečnosti informací je trvalý proces zahrnující jednorázové, opakované i soustavné činnosti.
c) Odpovědnost je přidělena konkrétní osobě (např. na konkrétní pracovní pozici nebo v konkrétní uživatelské roli), nikoliv skupině osob.
d) Systém řízení bezpečnosti informací může v rámci svého rozsahu pokrývat více prostředí; každé z uvedených prostředí může mít vlastní seznam bezpečnostních opatření (politiku bezpečnosti informací), základní procesy řízení bezpečnosti jsou však společné.
e) Výběr bezpečnostních opatření může být pro každé z prostředí zmíněných v předchozím bodě prováděn samostatně a za použití různých strategií.
f) V rámci systému řízení jsou pro všechna prostředí zavedeny mechanizmy kontroly shody mimo liniové řízení.
g) Vedoucí justičních složek (dále také jen „vedení resortu") je informováno o stavu bezpečnosti informací v resortu spravedlnosti.

§ 5

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

---

[2] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů.
[3] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
[4] Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.
[5] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů.

(1) Pravidla a postupy zajišťující provoz systému řízení bezpečnosti informací, uvedená v příloze č. 2, části II-3 „Příručka řízení bezpečnosti", vedou ke splnění požadavků řízení bezpečnosti informací a implementaci identifikovaných opatření.

(2) Vedoucí justiční složky musí zajistit, že pravidla a postupy systému řízení bezpečnosti informací, uvedená v příloze č. 2, části II-3 „Příručka řízení bezpečnosti", jsou pravidelně kontrolovány, hodnoceny a upravovány za účelem neustálého zlepšování.

(3) Vedoucí justiční složky musí zajistit, že pravidla a postupy systému řízení bezpečnosti informací, stejně jako opatření vybraná k implementaci uvedená v příloze č. 2, jsou dokumentovaná ve formě řízené dokumentace a jsou dostupná a prezentovaná všem koncovým uživatelům.

(4) Plánovaní systému řízení bezpečnosti informací a bezpečnostních opatření pro konkrétní informační systémy je prováděno na základě posouzení bezpečnosti informací. Pravidla a postupy posouzení bezpečnosti informací jsou uvedeny v příloze č. 2, části II-I „Příručka řízení bezpečnosti" a části II-2 „Metodika analýzy rizik", čímž je zajištěno, že opakovaná posouzení bezpečnosti informací produkují konzistentní, opodstatněné a porovnatelné výsledky. Za zajištění dodržování těchto pravidel a postupů v justiční složce zodpovídá vedoucí dané justiční složky.

(5) Manažer kybernetické bezpečnosti zajistí, že minimálně jednou ročně je provedena revize systému řízení bezpečnosti informací a aktualizace dokumentace systému řízení bezpečnosti informaci a bezpečnostních opatření. Podrobnosti jsou stanoveny v uvedená v příloze č. 2, části II-3 „Příručka řízení bezpečnosti"

(6) Manažer kybernetické bezpečnosti minimálně jednou ročně vytvoří zprávu o stavu bezpečnosti informací v resortu a tu předloží Výboru pro řízení kybernetické bezpečnosti, podrobnosti jsou uvedené v příloze č. 2, části II-3 „Příručka řízení bezpečnosti".

§ 6

Odpovědnost za bezpečnost

(1) Za řízení bezpečnosti informací v prostředí resortu justice zodpovídá ministr. Jako poradní orgán ministra pro tyto účely slouží Výbor pro řízení kybernetické bezpečnosti.

(2) Výstupy výboru pro řízení kybernetické bezpečnosti v rámci systému řízení bezpečnosti slouží jako podklady pro rozhodování ministra.

(3) Ředitel odboru informatiky ministerstva:

a) je zpracovatelem závazných předpisů k provozu prostředí ICT;
b) je oprávněn posuzovat projekty akvizice informačních systémů s ohledem na zajištění bezpečnosti informací ICT resortu justice a
c) je odpovědný za průběžnou kontrolu činností osob využívajících služeb ICT resortu justice.

(4) Vedoucí justičních složek:

a) jsou odpovědni za uplatňování této instrukce a na ní navazující předpisy upravující provoz a bezpečnost prostředí ICT;
b) jsou oprávněni předkládat odboru informatiky ministerstva připomínky a návrhy změn v oblasti bezpečnosti prostředí ICT.
c) jsou odpovědni za zajištění dodržování postupů, stanovených platnou provozní a bezpečnostní dokumentací informačního systému, smluvními partnery dané justiční složky.

(5) Pracovníci odboru informatiky a IT oddělení justičních složek (dále jen „Informatici") jsou odpovědni za soulad správy a provozu prostředí ICT justiční složky s předpisy upravujícími provoz a bezpečnost prostředí ICT.

(6) Každý pracovník justiční složky, při výkonu role ve správě a/nebo užití informačního systému, je odpovědný za dodržování postupů stanovených platnou provozní a bezpečnostní dokumentací informačního systému.

(7) Porušení zásad řízení bezpečnosti informací při výkonu role ve správě a/nebo užití informačního systému je chápáno jako bezpečnostní incident a řešeno jako porušení pracovních povinností resp. porušení právních předpisů.

§ 7

Bezpečnostní role

(1) Za účelem zajištění výše uvedených povinností ministr určuje osoby do role Manažer kybernetické bezpečnosti (dále také jen „MKB"), Architekt kybernetické bezpečnosti a Auditor kybernetické bezpečnosti, které převezmou odpovědnosti, práva a povinnosti uvedené v Politice organizační bezpečnosti, která je součástí přílohy č. 2 této instrukce a na tuto instrukci navazujících předpisech.

(2) Ministr určuje osoby do role Garant aktiva pro aktiva, která jsou informačními systémy určenými prvky kritické informační infrastruktury nebo významnými informačními systémy dle zákona č. 181/2014 Sb. Tento garant aktiva se podílí na zajištění vývoje, provozu, použití a údržby jednotlivých částí informačního systému. Jeho další práva a povinnosti jsou uvedeny v Politice organizační bezpečnosti, uvedené v příloze č. 2 této instrukce.

§ 8

Pravidla a postupy pro řízení dokumentace

(1) K naplnění uvedené politiky jsou vytvořeny potřebné procesy a navazující předpisy, které jsou obsaženy v příloze č. 2 této instrukce.

(2) Pravidla systému řízení bezpečnosti informací, bezpečnostní politiky a další návazné dokumenty obsahující bezpečnostní opatření, pravidla a postupy zajištění bezpečnosti informací jsou vydány ve formě závazného předpisu, konkrétně ve formě instrukce Ministerstva spravedlnosti.

(3) Pravidla systému řízení bezpečnosti informací, bezpečnostní politiky a další návazné dokumenty jsou jasně identifikované a přiměřené svému účelu. Změny uvedených předpisů probíhají řízeným způsobem zahrnujícím schválení a přezkoumaní následků plánovaných změn.

(4) Kromě toho v rámci systému řízení bezpečnosti informací musí vznikat dokumenty dokládající, že procesy jsou prováděny, jak bylo plánováno.

§ 9

Pravidla a postupy pro řízení rizik

(1) Návrh bezpečnostních opatření je pro systémy spadající do oblasti působnosti zákona o kybernetické bezpečnosti prováděn v rámci procesu řízení rizik na základě hodnocení rizik.

(2) Návrh bezpečnostních opatření je pro systémy nespadající do oblasti působnosti zákona o kybernetické bezpečnosti prováděn na základě nejlepší běžné praxe nebo na základě hodnocení rizik.

(3) Pro zajištění jednotného přístupu k hodnocení rizik je definována jednotná Metodika pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik, která bude použita pro všechny informační systémy. Tato metodika je uvedena v příloze č. 2, část II, odstavec 2 této instrukce.

(4) Systém řízení rizik musí zajišťovat, že rizika jsou nejenom identifikována, ale je rozhodováno i o jejich zvládání a následně jsou v průběhu celého životního cyklu informačního systému nadále monitorována a přehodnocována.

§ 10

Pravidla a postupy pro provádění auditů kybernetické bezpečnosti

(1) Audit kybernetické bezpečnosti ověřuje správnost a účinnost zavedených bezpečnostních opatření a jejich soulad s právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky. V resortu justice jde o kontrolu bezpečnosti systémů ICT.

(2) Auditor kybernetické bezpečnosti je v rámci resortu justice organizačně zařazen jako kontrolor bezpečnosti ICT.

(3) Výsledky auditu bezpečnosti informací jsou předávány výboru pro řízení kybernetické bezpečnosti, Manažerovi kybernetické bezpečnosti a vedení resortu jako součást zprávy o stavu bezpečnosti informací v resortu.

§ 11

Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací

Systém bezpečnosti informací a bezpečnostní opatření jsou revidovány na základě výsledků prováděných kontrol shody, výsledků auditů kybernetické bezpečnosti a analýz proběhlých bezpečnostních incidentů. Podrobnosti jsou uvedeny v příloze č. 2, oddíl II, odstavec 3 („Příručka řízení bezpečnosti").

§ 12

Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací

Výbor pro řízení kybernetické bezpečnosti minimálně jednou ročně přezkoumá a zhodnotí stav systému řízení bezpečnosti informací na základě předložené zprávy o stavu bezpečnosti informací a výsledků auditů kybernetické bezpečnosti.

§ 13

Závěrečné ustanovení

Zrušuje se instrukce Ministerstva spravedlnosti č.j. 24/2012-OI-SP, o zajištění bezpečnosti informací v prostředích informačních a komunikačních technologií resortu spravedlnosti, uveřejněná pod č. 1/2013 Sbírky instrukcí a sdělení.

ČÁST TŘETÍ

BEZPEČNOSTNÍ DOKUMENTACE

§ 14

Bezpečnostní dokumentace obsahující bezpečnostní politiky, bezpečnostní opatření, pravidla a postupy zajištění bezpečnosti informací, je uvedena v příloze č. 2 a je pro resort justice závazná. Určení konkrétního rozdělení zodpovědností rolí v této dokumentaci uvedených, v rámci dané justiční složky, je v pravomoci vedoucího justiční složky.

ČÁST ČTVRTÁ

ÚČINNOST

§ 15

Tato instrukce nabývá účinnosti dnem 29. února 2016.

ministr spravedlnosti

JUDr. Robert Pelikán, Ph.D. v. r.

Příloha 1

ZKRATKY A POJMY

V této instrukci jsou použity následující zkratky a pojmy:

a) Aktivum - obecně cokoliv, co má pro organizaci nebo i jednotlivce hodnotu, v případě této politiky a návazných předpisů pojem označuje informační aktiva resp. aktiva s nimi související, která se dělí na primární aktiva a podpůrná aktiva.
b) Bezpečnostní incident - jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, které mohou s vysokou pravděpodobností kompromitovat činnost organizace nebo ohrožovat bezpečnost informací.
c) Bezpečnostní událost - identifikovaný stav systému, služby nebo sítě, který signalizuje možné porušení bezpečnostní politiky nebo selhání bezpečnostních opatření, popř. jinou předtím nepoznanou situaci, která může být významná z pohledu bezpečnosti informací.
d) Bod obnovy dat (Recovery Point Objective - RPO) - místo v čase, ke kterému musí být obnovena data po selhání.
e) Centrálním úložištěm bezpečnostních logů je myšlen centrální systém shromažďující a případně dále zpracovávající záznamy potenciálně související s kybernetickými bezpečnostními událostmi. Počet těchto systémů v prostředí resortu justice není v této politice určen.
f) Doba obnovy chodu (Recovery Time Objective - RTO) - časové období, během kterého musí být po havárii obnovena minimální úroveň funkčnosti systému.
g) Dostupnost informací (aktiva) – informace musí být dostupné oprávněným osobám tehdy, když je potřebují.
h) Důvěrnosti informací (aktiva) – informace mají být dostupné jen tomu, kdo je k tomu oprávněn a potřebuje je znát ke své práci.
i) Externí síť – komunikační síť, která není pod správou resortu spravedlnosti nebo justiční složky.
j) Garant aktiva (GA) - fyzická osoba pověřená justiční složkou k zajištění rozvoje, použití a bezpečnosti aktiva.
k) Havarijní plán (Disaster Recovery Plan - DRP) - Plán pro záložní postupy, odezvu na nepředvídanou událost a obnovu po havárii.
l) Hrozba – potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození informačního systému nebo organizace.
m) Informační a komunikační technologie (ICT) - veškeré informační technologie používané pro komunikaci a práci s informacemi.
n) Informační technologie - každý elektronický přístroj schopný zpracovávat nějaké informace (neboli provádět algoritmus), tedy přijmout nějaká vstupní data, samostatně s nimi provést nějaké operace a vydat příslušná data výstupní (popřípadě část této technologie).
o) Informační systém (IS) - celek složený z počítačového hardwaru a souvisejícího softwaru spolu s lidmi a procesy, a navržený ke sběru, zpracování a šíření informací potřebných k plánování, rozhodování a řízení.
p) Informační systém kritické informační infrastruktury (KII) – informační systém, který je prvkem nebo systémem prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti (termín definovaný zákonem č. 181/2014 Sb. o kybernetické bezpečnosti).
q) Integrita informací (aktiva) – informace mohou být měněny pouze oprávněnými osobami nebo na pokyn oprávněných osob a řízeným způsobem.
r) Interní síť – komunikační síť, která je pod správou resortu spravedlnosti nebo justiční složky.
s) MKB – Manažer kybernetické bezpečnosti.
t) Opatření (Bezpečnostní opatření) – ochranná opatření pro zajištění bezpečnostních požadavků kladených na systém. Mohou mít různý charakter.
u) Plán kontinuity činnosti (Business Continuity Plan - BCP) - Dokumentovaný soubor postupů a informací, který je vytvořen a udržován v pohotovosti pro užití při incidentu za účelem umožnění organizaci uskutečňovat své kritické činnosti na přijatelné, předem stanovené úrovni.
v) Podpůrné aktivum - technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému.
w) Politika systému řízení bezpečnosti informací (nebo také „politika systému řízení") – Jedná se o systém řízení popsaný v druhé části této instrukce.
x) Pracovník – uživatel nebo správce.
y) Primární aktivum - informace nebo služba, kterou zpracovává nebo poskytuje informační systém.
z) Privilegovaná oprávnění - oprávnění překračující svým rozsahem oprávnění standardních uživatelů.
aa) Riziko - možnost, že určitá hrozba využije zranitelnosti informačního systému a způsobí poškození aktiva.
bb) SLA (Service Level Agreement) – dohoda o úrovni poskytovaných služeb - dohoda mezi poskytovatelem služby a jejím konzumentem definující rozsah, úroveň a intenzitu poskytovaných služeb.
cc) Soukromý klíč – jeden z páru klíčů používaných v asymetrické kryptografii, který musí být chráněný a používaný pouze jednou osobou.
dd) Správce - fyzická osoba pověřená Garantem aktiva zajišťující správu, provoz, použití, údržbu a bezpečnost technického aktiva (administrátor); ve většině případů označuje zaměstnance justičních složek nebo pracovníka smluvního partnera, který má přístup k informačním službám, informacím nebo jiným aktivům justičních složek, přičemž má přidělený rozsah oprávnění překračující svým rozsahem oprávnění uživatelů. V předpisu Vnitřní kancelářský řád pro okresní, krajské a vrchní soudy je správce označován pojmem informatik.

ee) Standardní informační systém (SIS) – informační systém, který není určen prvkem kritické informační infrastruktury (KII) nebo významným informačním systémem (VIS).
ff) Tajný klíč – klíč symetrické kryptografie používaný pro šifrování i dešifrování.
gg) Technické aktivum - technické vybavení, komunikační prostředky a programové vybavení informačního systému a objekty, ve kterých je tento systém umístěn.
hh) Uživatel – fyzická nebo právnická osoba anebo orgán veřejné moci, který využívá primární aktiva; ve většině případů zahrnuje zaměstnance justičních složek nebo pracovníka smluvního partnera, který má přístup k informačním službám, informacím nebo jiným aktivům justičních složek, přičemž má přidělený běžný rozsah oprávnění přístupu.
ii) Vedení resortu - tímto pojmem se rozumí ministr nebo ministryně.
jj) Vedoucí justiční složky – vedoucí dané organizační složky resortu justice.
kk) Veřejný klíč – jeden z páru klíčů používaných v asymetrické kryptografii určený ke zveřejnění (většinou obsažen v certifikátu uživatele nebo serveru).
ll) Významný informační systém (VIS) - informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci (termín definovaný zákonem č. 181/2014 Sb. o kybernetické bezpečnosti).
mm) Zástupce vedení resortu – osoba zastupující vedení resortu pro oblast bezpečnosti informací.
nn) Zranitelnost - slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

Příloha 2

BEZPEČNOSTNÍ DOKUMENTACE

Tato příloha obsahuje bezpečnostní dokumentaci. Bezpečnostní dokumentace je rozdělena na bezpečnostní politiky a další bezpečnostní dokumentaci.

I. Bezpečnostní politiky

(1) Politika akvizice a vývoje.

(2) Politika organizační bezpečnosti.

(3) Politika řízení dodavatelů.

(4) Politika klasifikace aktiv.

(5) Politika bezpečnosti lidských zdrojů.

(6) Politika řízení provozu a komunikací.

(7) Politika řízení přístupu.

(8) Politika bezpečného chování uživatelů.

(9) Politika zálohování a obnovy.

(10) Politika bezpečného předávání a výměny informací.

(11) Politika řízení technických zranitelností.

(12) Politika bezpečného používání mobilních zařízení.

(13) Politika poskytování a nabývání licencí programového vybavení a informací.

(14) Politika dlouhodobého ukládání a archivace informací.

(15) Politika ochrany osobních údajů.

(16) Politika fyzické bezpečnosti.

(17) Politika bezpečnosti komunikační sítě.

(18) Politika ochrany před škodlivým kódem.

(19) Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí.

(20) Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

(21) Politika bezpečného používání kryptografické ochrany.

(22) Politika zvládání kybernetických bezpečnostních incidentů.

(23) Politika auditu a kontroly souladu.

II. Další bezpečnostní dokumentace

(1) Strategie řízení kontinuity činností.

(2) Metodika analýzy rizik.

(3) Příručka řízení bezpečnosti.

(4) Směrnice - Zajištění bezpečné infrastruktury prostředí ICT