SMLOUVA O POSKYTOVÁNÍ SLUŽEB

Zdravotní pojišťovna ministerstva vnitra České republiky
se sídlem: Praha 3, Vinohrady, Vinohradská 2577/178, PSČ 130 00
IČO: 47114304
zapsaná v: obchodním rejstříku vedeném Městským soudem v Praze, oddíl A, vložka 7216
zastoupená: MUDr. Davidem Kostkou, MBA, generálním ředitelem
bankovní spojení: [redacted]

(dále též jako „***Objednatel***“ či „***ZP MV ČR“***),

a

ALP Security, s.r.o.
se sídlem: Rybná 716/24, 110 00 Praha 1
IČO: 03311171
zapsaná/ý v: u Městského soudu v Praze, C 229940
zastoupená/ý: Alešem Vokálem, jednatelem
bankovní spojení: [redacted]

(dále též jako ***„Poskytovatel“***),

(Objednatel a Poskytovatel společně též jako „***Smluvní strany***“ či jednotlivě „***Smluvní strana***“),

uzavřeli níže uvedeného kalendářního dne, měsíce a roku v souladu s ust. § 1746 odst. 2 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „***občanský zákoník***“) a na základě výsledků veřejné zakázky malého rozsahu s názvem „*Poskytování služeb penetračního testování*“, vedené Objednatelem pod č.j. ZP-910898/2021-R, tuto

SMLOUVU O POSKYTOVÁNÍ SLUŽEB

evidovanou u Objednatele pod č.j. 000162-000/2021-00
evidovanou u Poskytovatele pod č.j. 2022-ZPMV-01

(dále jen „***Smlouva***“)

Článek I.
Předmět Smlouvy

1. Poskytovatel se zavazuje na základě této Smlouvy poskytovat Objednateli služby provádění vnějších a vnitřních penetrační testů. Poskytnuté služby budou rozčleněny do následujících okruhů:
   1.1. Provádění vnějších penetrační testů představujících simulaci napadení systémů útočníkem. Cílem testů je zjistit, jak snadno identifikovatelný cíl informační systémy Objednatele představují, jaké informace lze získat o zvenčí dostupných systémech, jak detekovat zranitelnosti, které mohou být zneužity k získání neautorizovaného přístupu k citlivým systémovým zdrojům, a navrhnout doporučení k jejich odstranění.

1.2. Provádění vnitřních penetrační testů realizovaných z prostředí vnitřní LAN sítě Objednatele. Cílem penetračních testů je prověření bezpečnosti systému v rámci jeho provozního prostředí a provozu vnitřní sítě bez destrukčního dopadu.

Bližší specifikace předmětu plnění je uvedena v Příloze č. 1 této Smlouvy (dále jen ***„Služby“***).

2. Za řádně poskytnuté Služby náleží Poskytovateli odměna, kterou se Objednatel zavazuje Poskytovateli hradit dle podmínek uvedených dále v této Smlouvě.

3. Poskytovatel prohlašuje, že si je vědom skutečnosti, že Objednatel má zájem na realizaci veřejné zakázky v souladu se zásadami odpovědného zadávání veřejných zakázek ve smyslu § 6 odst. 4 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „***ZZVZ***“). Poskytovatel se zavazuje po celou dobu trvání smluvního vztahu založeného touto Smlouvou zajistit dodržování veškerých obecně závazných právních předpisů vztahující se k vykonávané činnosti, zejména předpisy o bezpečnosti a ochraně zdraví při práci a o požární bezpečnosti, dále interní předpisy Objednatele, pokud byla příslušná dokumentace zpřístupněna Poskytovateli, dále se řídit organizačními pokyny odpovědných zaměstnanců Objednatele a především pracovněprávních předpisů týkající se odměňování, pracovní doby, doby odpočinku, přesčasů, atd. Poskytovatel se zavazuje řádně a včas plnit finanční závazky vůči všem účastníkům dodavatelského řetězce, pokud se budou podílet na plnění této Smlouvy.

Článek II.
Místo, termín a způsob plnění

1. Místem plnění je sídlo Objednatele na adrese Zdravotní pojišťovna ministerstva vnitra České republiky, ředitelství, budova Crystal, Vinohradská 2577/178, 130 00 Praha 3 – Vinohrady.

2. Poskytovatel bude Služby dle této Smlouvy poskytovat průběžně, a to na základě oboustranně odsouhlaseného zadání, kdy Objednatel předá Poskytovateli své požadavky na provedení Služeb spolu s potřebnými informacemi k jejich provedení (např. IP rozsahy příp. termín provedení) a Poskytovatel do 5 pracovních dnů potvrdí Objednateli způsob jejich provedení a ve spolupráci s Objednatelem navrhne časový harmonogram jejich provedení. Termín provedení požadovaných služeb musí být stanoven do 5 pracovních dnů, pokud se Smluvní strany nedohodnou jinak. Požadavek Objednatele může být učiněn v písemné či ústní formě, a to i prostřednictvím e-mailu, telefonicky nebo osobně.

3. Předání a převzetí výsledků Služeb poskytnutých dle odst. 2 tohoto článku (dále též „***dílčí plnění***“) bude provedeno na základě Poskytovatelem vyhotoveného Akceptačního protokolu, který po splnění akceptačních kritérií potvrdí zástupci obou Smluvních stran.

4. Objednatel je oprávněn odmítnout převzetí dílčího plnění, pokud dané plnění nebude zhotoveno řádně v souladu s touto Smlouvou a ve sjednané kvalitě, přičemž v takovém případě Objednatel důvody odmítnutí převzetí plnění písemně Poskytovateli sdělí, a to nejpozději do 5 (pěti) pracovních dnů od původního termínu předání plnění. Na následné předání plnění se použijí výše uvedená ustanovení tohoto článku.

5. Poskytovatel se zavazuje poskytovat Služby Objednateli neprodleně po nabytí účinnosti této Smlouvy po dobu 12 měsíců.

6. Výsledek činnosti, jenž je předmětem plnění nebo jeho části dle této Smlouvy, není Poskytovatel oprávněn poskytnout třetím osobám ve smyslu § 2633 občanského zákoníku.

7. Odpovědnými zástupci Smluvních stran jsou osoby uvedené v čl. X odst. 8 této Smlouvy. Den podepsání Akceptačního protokolu odpovědným zástupcem Objednatele se považuje za den předání plnění dle této Smlouvy.

Článek III.
Cena a platební podmínky

1. Sjednaná jednotková cena Služeb uvedených v čl. I za podmínek uvedených v čl. II této Smlouvy (dále jen „***Jednotková cena***“) činí **16.000 Kč** (slovy: šestnácttisíc korun českých) bez DPH za 1 člověkoden (tj. 8 člověkohodin) (dále jen „***MD***“). V případě, že nebude dosaženo 1 MD (tj. 8 člověkohodin), bude cena přepočtena dle doby skutečně poskytnutých Služeb, přičemž minimální účtovatelnou jednotkou je 0,5 (jedna polovina) člověkohodiny. K Jednotkové ceně bude připočtena příslušná DPH ve výši dle právních předpisů, platných k okamžiku uskutečnění zdanitelného plnění. Tato Jednotková cena je nejvýše přípustná, konečná a zahrnuje veškeré náklady Poskytovatele spojené s plněním dle této Smlouvy.

2. Smluvní strany se dohodly, že maximální výše celkových nákladů na všechna plnění vyplývající z této Smlouvy nepřesáhne částku **2 000 000 Kč** (slovy: dva miliony korun českých) bez DPH za dobu účinnosti této Smlouvy. Uvedená částka však nemusí být vyčerpána.

3. Cenu za poskytnuté Služby je Poskytovatel oprávněn vyúčtovat vždy po převzetí plnění dle této Smlouvy Objednatelem a na základě podepsaného Akceptačního protokolu dle čl. II odst. 3 této Smlouvy. Tato cena je splatná na základě oprávněně vystaveného řádného daňového dokladu Poskytovatele doručeného Objednateli (dále také jen ***„Faktura“***).

4. Faktura musí mít náležitosti daňového dokladu dle § 29 odst. 1 a odst. 2 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a náležitosti dle § 435 občanského zákoníku. Nedílnou součástí vystavené Faktury bude potvrzený Akceptační protokol dle čl. II odst. 3 této Smlouvy.

5. Splatnost řádně a oprávněně vystavené Faktury je 21 dnů ode dne jejího doručení Objednateli. Faktura se považuje za uhrazenou dnem odepsání příslušné částky z bankovního účtu Objednatele uvedeného v záhlaví této Smlouvy.

6. Objednatel je oprávněn před uplynutím lhůty splatnosti vrátit Poskytovateli bez zaplacení Fakturu, která neobsahuje požadované náležitosti a/nebo obsahuje nesprávné údaje a/nebo není-li doložena požadovanými doklady. Běh lhůty splatnosti oprávněně vrácené Faktury se přerušuje. Po doručení nové nebo opravené Faktury lhůta splatnosti pokračuje.

7. Poskytovatel, pokud je plátce DPH, prohlašuje, že si je vědom své povinnosti přiznat a zaplatit daň z přidané hodnoty z ceny za poskytnuté zdanitelné plnění dle této Smlouvy dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „***zákon č. 235/2004 Sb.***“), a že mu nejsou ke dni uskutečnění zdanitelného plnění dle této Smlouvy známy žádné skutečnosti uvedené v § 109 zákona č. 235/2004 Sb., které by splnění těchto povinností bránily.

8. Účetní doklad je možné zaslat Objednateli elektronicky ve formátu PDF prostřednictvím datové schránky ZP MV ČR, kód: 9swaix3. Nedisponuje-li Poskytovatel datovou schránkou, faktury lze též odeslat na emailovou adresu info@zpmvcr.cz. Do předmětu zprávy je třeba uvést v obou případech text „Fakturace_R“.

9. Faktura musí kromě náležitostí uvedených v odst. 4 resp. 8 tohoto článku obsahovat číslo 000162-000/2021-00, pod kterým je Smlouva evidována u Objednatele.

Článek IV.
Povinnosti Smluvních stran

1. Poskytovatel je povinen:
   a) poskytovat Služby dle této Smlouvy na svůj náklad a nebezpečí v termínech určených Objednatelem, popř. bez zbytečného odkladu, a to písemně, formou e-mailové komunikace nebo telefonicky, popř. osobně;
   b) při poskytování Služeb postupovat s náležitou odbornou péčí dle této Smlouvy, právních předpisů a technických norem;
   c) předat Objednateli seznam podkladových materiálů nezbytných pro poskytnutí Služeb dle této Smlouvy;
   d) zajistit ochranu od Objednatele převzatých podkladových materiálů a k jejich ochraně zavázat také veškeré své zaměstnance či spolupracovníky, kteří s těmito materiály přijdou či by mohli přijít do styku. Poskytovatel se zejména zavazuje neposkytovat podkladové materiály Objednatele ani výstupy plnění nikomu, s výhradou případů poskytnutí předchozího písemného souhlasu Objednatele;
   e) umožnit Objednateli průběžnou kontrolu kvality poskytovaných Služeb dle potřeb Objednatele;
   f) zachovávat mlčenlivost o všech skutečnostech, o kterých se dozví při poskytování Služeb dle této Smlouvy či v souvislosti s nimi. Tato povinnost Poskytovatele trvá i po ukončení této Smlouvy.
   g) zajistit řádné a včasné plnění finančních závazků svým poddodavatelům, kdy za řádné a včasné plnění se považuje plné uhrazení (vyjma případných sjednaných pozastávek) poddodavatelem vystavených a doručených faktur za plnění poskytnutá k plnění veřejné zakázky, a to vždy do 30 kalendářních dnů od obdržení platby ze strany Objednatele za konkrétní plnění. Poskytovatel se zavazuje přenést totožnou povinnost do dalších úrovní dodavatelského řetězce a zavázat své poddodavatele k plnění a šíření této povinnosti též do nižších úrovní dodavatelského řetězce. Objednatel je oprávněn požadovat předložení smlouvy uzavřené mezi Poskytovatelem a jeho poddodavatelem k nahlédnutí. Poskytovatel je povinen do 5 pracovních dnů předložit Objednateli požadované dokumenty.

2. Objednatel je povinen:
   a) předat Poskytovateli vyžádané podkladové materiály, nezbytné k řádnému splnění povinností Poskytovatele dle této Smlouvy;
   b) poskytnout Poskytovateli nezbytnou součinnost k poskytnutí Služeb dle této Smlouvy, zejména zajistit Poskytovateli spolupráci s příslušnými zaměstnanci Objednatele;
   c) umožnit po předchozí dohodě Poskytovateli přístup do svých objektů za účelem realizace předmětu plnění dle této Smlouvy.

3. Smluvní strany jsou povinny:
   a) při plnění této Smlouvy úzce spolupracovat, zejména si poskytovat úplné, pravdivé a včasné informace potřebné k řádnému plnění svých povinností, přičemž v případě změny podstatných okolností, které mají nebo mohou mít vliv na plnění Smlouvy, jsou Smluvní strany povinny o takové změně informovat druhou Smluvní stranu bezodkladně, nejpozději však do 3 pracovních dnů po zjištění takové změny;
   b) plnit řádně a včas své povinnosti tak, aby nedocházelo k prodlení s jejich plněním. Pokud se některá ze Smluvních stran dostane do prodlení s plněním svých povinností, je povinna písemně oznámit bez zbytečného odkladu druhé Smluvní straně důvod prodlení a předpokládaný termín a způsob jeho odstranění.

Článek V.
Sankce

1. V případě porušení povinnosti Poskytovatele dle čl. IV odst. 1 písm. a) až e) této Smlouvy, je Objednatel oprávněn požadovat po Poskytovateli zaplacení smluvní pokuty ve výši 5 000 (pěttisíc) Kč za každé jednotlivé porušení, a to i opakovaně.

2. V případě prodlení Poskytovatele s potvrzením požadavků Objednatele ve lhůtě uvedené v čl. II odst. 2 této Smlouvy nebo v případě prodlení Poskytovatele s provedením požadavků Objednatele ve lhůtě dohodnuté podle čl. II odst. 2 této Smlouvy, je Objednatel oprávněn požadovat po Poskytovateli zaplacení smluvní pokuty ve výši 1 000 Kč za každý i započatý den prodlení.

3. V případě porušení povinnosti mlčenlivosti a ochrany osobních údajů Objednatele specifikovaných v čl. VI této Smlouvy je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 100 000 (sto tisíc) Kč za každé jednotlivé porušení, a to i opakovaně.

4. V případě, že Poskytovatel využije poddodavatelů a Objednatel si vyžádá doklady o uzavřených smlouvách nebo provedených platbách poddodavatelů, přičemž Poskytovatel Objednateli uvedené doklady neposkytne ve lhůtě uvedené v čl. IV odst. 1 písm. g) Smlouvy, je Objednatel oprávněn požadovat po Poskytovateli zaplacení smluvní pokuty ve výši 500 Kč (slovy: pět set korun českých), za každý i započatý den prodlení.

5. V případě, že Poskytovatel využije poddodavatelů a Objednatel z dokladů uvedených IV odst. 1 písm. g) Smlouvy zjistí, že Poskytovatel řádně a včas neplní finanční závazky vůči svým poddodavatelům dle čl. IV odst. 1 písm. g) Smlouvy, je Kupující oprávněn požadovat po Prodávajícím zaplacení smluvní pokuty ve výši 1 000,- Kč za každý takto zjištěný případ.

6. V případě porušení povinností Poskytovatele v rámci kybernetické bezpečnosti specifikovaných v čl. VII této Smlouvy je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 100 000 (sto tisíc) Kč za každé jednotlivé porušení, a to i opakovaně.

7. V případě prodlení Objednatele se zaplacením dohodnuté ceny za poskytnutí řádně akceptovaných Služeb dle čl. II a III této Smlouvy je Poskytovatel oprávněn požadovat po Objednateli zaplacení úroku z prodlení ve výši 0,01 % (slovy: jedna setina procenta) z dlužné částky za každý i započatý den prodlení.

8. Vznikem povinnosti platit smluvní pokutu, ani jejím skutečným zaplacením nezaniká povinnost Smluvních stran splnit povinnost, jejíž plnění bylo zajištěno smluvní pokutou.

9. Smluvní sankce dle tohoto článku jsou splatné do 30 dnů ode dne doručení výzvy k jejich úhradě povinné straně.

10. Zaplacením smluvní pokuty a úroku z prodlení není dotčen nárok Smluvních stran na náhradu škody nebo odškodnění v plném rozsahu ani povinnost Poskytovatele řádně poskytnout plnění.

11. Žádná ze Smluvních stran není povinna zaplatit smluvní pokutu či náhradu škody, pokud prokáže, že porušení povinností bylo způsobeno okolnostmi dle § 2913 odst. 2 občanského zákoníku.

Článek VI.
Ochrana důvěrných informací a zpracování osobních údajů

1. Smluvní strany se dohodly, že veškeré informace, které se Poskytovatel dozvěděl v rámci uzavírání a plnění této Smlouvy, tvořící její obsah, a informace, které Poskytovateli Objednatel sdělí nebo jinak vyplynou z plnění Smlouvy, musí být Poskytovatelem dle vůle Objednatele utajeny (dále jen „***důvěrné informace***"). Poskytovatel nesmí důvěrné informace Objednatele použít pro jiné účely než pro poskytnutí plnění dle této Smlouvy, nesmí je zveřejnit ani poskytnout jiné osobě. Uvedené ustanovení se nevztahuje na obsah Smlouvy, jejích příloh a případných dodatků.

2. Smluvní strany se dohodly, že Poskytovatel nesdělí důvěrné informace třetí osobě a přijme taková opatření, která znemožní jejich přístupnost třetím osobám. Ustanovení předchozí věty se nevztahuje na případy, kdy:
   a) má Poskytovatel opačnou povinnost stanovenou zákonem,
   b) se takové důvěrné informace stanou veřejně známými či dostupnými jinak než porušením povinností vyplývajících z tohoto článku, nebo
   c) Objednatel dá k zpřístupnění konkrétní důvěrné informace písemný souhlas.

3. Smluvní strany výslovně souhlasí s tím, že tato Smlouva bude uveřejněna v registru smluv bez jakýchkoliv omezení, a to včetně případných příloh a dodatků. Smluvní strany prohlašují, že skutečnosti uvedené v této Smlouvě nepovažují za obchodní tajemství ve smyslu ustanovení platných právních předpisů a udělují svolení k jejich užití a uveřejnění bez stanovení jakýchkoliv dalších podmínek či omezení.

4. V souvislosti s plněním této smlouvy Smluvními stranami bude docházet i ke zpracování osobních údajů ve smyslu Nařízení Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „***Nařízení***") a zákona č. 110/2019 Sb., o zpracování osobních údajů v platném znění (dále jen „***Zákon***").

5. Objednatel jakožto správce osobních údajů (dále v tomto článku označen jen jako „***správce***"), tímto pověřuje ve smyslu článku 28 Nařízení Poskytovatele jako zpracovatele osobních údajů (dále v tomto článku označena jen jako „***zpracovatel***") zpracováním osobních údajů poskytnutých správcem a zaměstnanci nebo potenciálními zaměstnanci správce pro účel plnění povinností vyplývajících z této Smlouvy.

6. Správce i zpracovatel postupují při své činnosti týkající se nakládání s osobními údaji ve smyslu Zákona a Nařízení. Zpracovatel zpracovává osobní údaje v rozsahu a v souladu s Nařízením a v rozsahu stanoveném touto Smlouvou. Zpracovatel zpracovává osobní údaje pouze na základě doložených pokynů správce.

7. Další povinnosti zpracovatele jsou následující:
   a) Zpracovatel osobních údajů zpracovává osobní údaje v rozsahu nezbytném pro plnění účelu podle této Smlouvy, a to pouze po nezbytně nutnou dobu;
   b) Zpracovatel nesmí s poskytnutými osobními údaji jakkoliv nakládat nad rámec účelu, za kterým mu byly poskytnuty, v rámci tohoto účelu pak zpracovatel musí s osobními údaji nakládat jen v rozsahu nezbytně nutném;
   c) Zpracovatel se zavazuje přijmout taková technická a organizační opatření k zabezpečení osobních údajů, aby nemohlo dojít k neoprávněnému, nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů;

d) Zpracovatel zajistí informovanost a školení svých zaměstnanců pracujících s osobními údaji. Především zajistí, aby jeho zaměstnanci pracující s osobními údaji byli v souladu s platnými právními předpisy vázáni povinností mlčenlivosti ve smyslu Nařízení a poučeni o možných následcích pro případ porušení této povinnosti;

e) Zpracovatel není oprávněn zapojit do zpracování žádného dalšího zpracovatele bez předchozího písemného souhlasu správce;

f) Zpracovatel poskytne správci nezbytnou spolupráci, součinnost a informace (i) potřebné k vyřízení jakékoli stížnosti nebo žádosti subjektu údajů týkající se jejich osobních údajů nebo dozorového orgánu ochrany osobních údajů (ii) v souvislosti se zmírňováním a nápravou incidentů v oblasti zabezpečení osobních údajů a porušení zabezpečení údajů (jako např. ztráta, krádež, vymazání, zveřejnění nebo poškození osobních údajů), (iii) za účelem opravy, změny, přenesení nebo vymazání osobních údajů nebo (iv) za účelem plnění jakýchkoliv jiných povinností správce podle Nařízení;

g) Zpracovatel ohlásí správci jakékoliv porušení zabezpečení osobních údajů bez zbytečného odkladu poté, co porušení zjistí a ohlášení případně doplní o informace požadované správcem;

h) Zpracovatel v souladu s rozhodnutím správce všechny osobní údaje vrátí správci po ukončení zpracování, a vymaže existující kopie, pokud právo EU nebo české právo nepožaduje uložení daných osobních údajů;

i) Zpracovatel poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v článku 28 Nařízení, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje. Zpracovatel neprodleně informuje správce v případě, že podle jeho názoru určitý pokyn porušuje Zákon nebo Nařízení nebo jiné předpisy EU, České republiky nebo jiného členského státu EU týkající se ochrany osobních údajů.

8. Smluvní ujednání o zpracování osobních údajů ve smyslu tohoto článku se uzavírá na dobu trvání této Smlouvy.

9. Další vzájemná práva a povinnosti Smluvních stran, práva a povinnosti Smluvních stran vůči třetím osobám a veřejným orgánům v souvislosti se zpracováním osobních údajů, vyplývajících ze Zákona nebo Nařízení, nejsou shora uvedeným dotčeny.

10. Z tohoto ujednání o zpracování osobních údajů neplynou pro Smluvní strany žádné finanční závazky, odměna za zpracování osobních údajů je již zahrnuta v odměně Poskytovatele stanovené dle čl. III této Smlouvy.

Článek VII.
Kybernetická bezpečnost a související povinnosti Poskytovatele

1. Poskytovatel se zavazuje při plnění postupovat v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (zákon o kybernetické bezpečnosti) (dále též „***ZoKB***"), jakož i v souladu se souvisejícími prováděcími předpisy a oprávněnými požadavky Objednatele.

2. Poskytovatel bere na vědomí, že Dílo/Služby/Dodávky mohou souviset s užitím, správou, či rozvojem tzv. významného informačního systému ve smyslu ustanovení § 2 písm. d) ZoKB. Objednatel však požaduje zabezpečení způsobem stanoveným pro významné informační systémy. Stane-li se Dílo/Služby/Dodávky v budoucnu významným informačním systémem, zavazuje se Objednatel písemně o této skutečnosti Poskytovatele informovat; Smluvní strany pro tento případ sjednávají, že povinnosti podle ZoKB a provádějících předpisů vůči Národnímu

úřadu pro kybernetickou a informační bezpečnost provádí Objednatel. Poskytovatel má v tomto případě postavení Významného dodavatele a vztahují se na něj rovněž všechny povinnosti stanovené v tomto článku pro Poskytovatele.

3. Poskytovatel se zavazuje podstoupit audit/kontrolu k plnění všech relevantních povinností, ke kterým se Poskytovatel smluvně zavázal. Typicky půjde o kontrolu způsobu plnění dohodnutých bezpečnostních opatření, způsobu řízení Poskytovatele, způsobu nakládání s daty, způsobu identifikace a hlášení kybernetických bezpečnostních incidentů apod. Možnost neakceptace tohoto ustanovení může být nahrazena předaným výstupem auditu ISO 27001 u Poskytovatele.

4. Kontrola zavedení a užití bezpečnostních opatření a procesů:

   a) Poskytovatel se na výzvu zavazuje umožnit Objednateli provedení kontroly v rozsahu zavedení a realizace bezpečnostních opatření, jejichž zavedení a užití je vyžadováno ZoKB, prováděcími předpisy k tomuto zákonu nebo vnitřními předpisy Objednatele. Výzva na Dodavatele bude zaslána minimálně 1 měsíc před první takovou kontrolou. Kontrola dle smluvního vztahu popřípadě další kontroly budou prováděny v intervalu maximálně 12 – ti měsíců. Poskytovatel v této věci poskytne Objednateli, nebo jím určené třetí straně, nutnou součinnost. Z kontroly vyhotoví Objednatel dokument s názvem Zápis z kontroly Poskytovatele.

   b) Při těchto kontrolách bude vždy přihlédnuto rozsahu plnění podle Smlouvy.

   c) Pokud bude během kontroly zjištěno, že Poskytovatel nesplňuje povinné náležitosti, tj. bezpečnostní organizační a technická opatření nejsou zavedena nebo užita, nebo jsou zavedena či užita v nedostatečném rozsahu, je tato skutečnost zapsána do Zápisu z kontroly Poskytovatele. Objednatel v Zápisu z kontroly Poskytovateli stanoví závazný termín pro jejich nápravu. Při určení tohoto termínu bude vždy přihlédnuto k povaze bezpečnostního opatření, které není zavedeno či užito, nebo je zavedeno či užito v nedostatečném rozsahu.

   d) Všechny náklady ZoKB a náklady související s kontrolami, plněním požadavků ZoKB, řešením kybernetických bezpečnostních incidentů či přijetím definovaných bezpečnostních opatření jsou vždy na vrub Poskytovatele jako podnikatelské riziko a není možno je jakkoli přikládat na vrub Objednatele.

5. V případě Kybernetického bezpečnostního incidentu (dále též „KBI“) vzniklého na Dílu/Službě/Dodávce se Poskytovatel zavazuje tento KBI neprodleně oznámit Objednateli, a následně pracovat na jeho odstranění s cílem uvést Dílo/Služby/Dodávky do stavu s užitím, správou, či rozvojem významného informačního systému ve smyslu ustanovení § 2 písm. d) ZoKB bez rizika vzniku KBI. Poskytovatel informuje Objednatele o odstranění nahlášeného KBI a sepíše akceptační protokol, který bude obsahovat, mimo jiné, popis závady, případně důvod jejího vzniku, způsob odstranění závady, přičemž Objednatele bude ve věcech kybernetické bezpečnosti zastupovat Manažer kybernetické bezpečnosti Objednatele. Poskytovatel se zavazuje umožnit Objednateli provést kontrolu procesu odstraňování KBI a vypořádat se s případnými připomínkami Objednatele k procesu odstraňování KBI.

6. Seznam vyžadovaných bezpečnostních opatření se může měnit buď v souvislosti se změnou povahy a rozsahu plnění podle smlouvy nebo v návaznosti na povinnosti Objednatele vyplývající z ustanovení § 13 ZoKB. Pokud Národní bezpečnostní úřad Objednateli uloží povinnost, v návaznosti na výskyt kybernetické bezpečnostní události či incidentu, zavést či užívat určité bezpečnostní opatření, má Poskytovatel povinnost toto bezpečnostní opatření zavést či užívat, nebo Objednateli poskytnout nutnou součinnost.

7. Jmenovitě se může jednat o tyto kontrolované oblasti a bezpečnostní opatření v prostředí Poskytovatele nebo související s Předmětem plnění dle Smlouvy:

   - Existenci a rozsah bezpečnostních politik a bezpečnostní dokumentace;

- Zavedení procesů organizační bezpečnosti včetně zavedení bezpečnostních rolí;
- Zavedení procesů řízení Poskytovatele;
- Zavedení procesů bezpečnosti lidských zdrojů včetně doložení stavu bezpečnostního povědomí pracovníků Poskytovatele a plán jeho dalšího rozvoje;
- Zavedení procesů a nástroje pro řízení přístupu;
- Zavedení procesů zvládání kybernetických bezpečnostních událostí a incidentů včetně nasazení nástroje pro detekci kybernetických bezpečnostních událostí a nasazení nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí;
- Zavedení procesů a nasazení nástroje pro řízení změn včetně zpracování incidentů, servisních požadavků, problémů či změnových požadavků;
- Zavedení procesů řízení kontinuity činností;
- Nasazení nástroje a souvisejících procesů pro zajištění úrovně dostupnosti informací (zálohování, plán a principy testování obnovy dat);
- Způsob vzdáleného připojení do vnitřní sítě a jeho zabezpečení;
- Nasazení nástroje a procesů pro správu a ověřování identit pracovníků Poskytovatele
- (koncových uživatelů i administrátorů) včetně nasazení nástroje a souvisejících procesů pro řízení přístupových oprávnění;
- Nasazení nástroje pro záznam činnosti uživatelů a administrátorů;
- Zavedení procesů pro pravidelné ověření, jestli daný pracovník Poskytovatele disponuje právě těmi právy, která jsou nutná pro jeho pracovní zařazení;
- Nasazení a provoz nástroje pro ochranu před škodlivým kódem, antivirové kontroly na zařízeních Poskytovatel použitých pro plnění předmětu této Smlouvy a implementace antimalwaru a antispywaru a antivirové kontroly na koncových zařízeních včetně navazujících procesů;
- Zavedení kryptografických prostředků a způsob jejich aplikace;
- Zajištění fyzické bezpečnosti objektů, z kterých Poskytovatel realizuje dodávku pro Objednatele.

8. Ostatní bezpečnostní požadavky jsou uvedeny v Příloze č. 2 této Smlouvy – „Ostatní všeobecné bezpečnostní požadavky ZP MV ČR“.

Článek VIII.
Doba trvání Smlouvy a zánik závazku

1. Tato Smlouva je sjednána na dobu určitou ode dne nabytí účinnosti Smlouvy po dobu **12 (dvanáct) měsíců**.

2. Závazkový vztah založený mezi oběma Smluvními stranami touto Smlouvou zaniká, nastane-li některá z níže uvedených právních skutečností:
   a) uplynutí doby, na kterou byla Smlouva sjednána,
   b) před uplynutím dohodnuté doby trvání Smlouvy v případě, že celkový objem plnění dle této Smlouvy, tj. cena poskytnutých Služeb dle čl. I této Smlouvy dosáhne objemu Objednatelem vyčleněných finančních prostředků uvedených v čl. III odst. 2 této Smlouvy. O této skutečnosti se Objednatel zavazuje Poskytovatele neprodleně informovat.

3. Závazkový vztah dle této Smlouvy lze ukončit dohodou Smluvních stran v písemné formě, přičemž účinky zrušení Smlouvy nastanou k okamžiku stanovenému v takovéto dohodě.

4. Obě Smluvní strany jsou oprávněny Smlouvu písemně vypovědět i bez udání důvodu. Výpovědní doba činí dva (2) měsíce a počíná běžet od prvního dne měsíce následujícího po měsíci, ve kterém byla výpověď doručena druhé Smluvní straně. Uplynutí výpovědní doby má za následek ukončení závazkového vztahu dle této Smlouvy.

5. V případě, že jedna ze Smluvních stran podstatně poruší povinnosti z této Smlouvy, může druhá Smluvní strana od Smlouvy odstoupit. Pro účely této Smlouvy se podstatným porušením Smlouvy rozumí zejména:

   a) opakované prodlení Poskytovatele i přes písemné upozornění Objednatele s poskytnutím Služby ve sjednaných termínech;

   b) poskytování Služby v rozporu s Přílohou č. 1 této Smlouvy,

   c) opakované neposkytnutí součinnosti ze strany Objednatele, znemožňující Poskytovateli poskytnout Služby dle článku I této Smlouvy;

   d) prodlení Objednatele s úhradou řádně a oprávněně vystavené Faktury Poskytovateli za poskytnuté plnění, přesahující třicet (30) kalendářních dnů;

   e) porušení jakéhokoliv ustanovení článku VI této Smlouvy.

   f) porušení jakéhokoliv ustanovení článku VII této Smlouvy,

   g) porušení závazku Poskytovatele k dodržování veškerých obecně závazných právních předpisů vztahující se k vykonávané činnosti vůči svým pracovníkům dle podmínek uvedených v čl. I této Smlouvy a byl orgánem veřejné moci pravomocně uznán vinným ze spáchání přestupku, správního deliktu či jiného obdobného právního jednání.

6. Objednatel je dále oprávněn odstoupit od této Smlouvy v případě, že:

   a) Poskytovateli bude rozhodnutím správce daně přidělen status nespolehlivého plátce,

   b) vůči Poskytovateli bylo zahájeno insolvenční řízení nebo vstoupil do likvidace.

7. Odstoupením od Smlouvy závazek ze Smlouvy zaniká ke dni doručení projevu vůle jedné Smluvní strany směřujícího k odstoupení od Smlouvy druhé Smluvní straně. Účinky odstoupení se řídí příslušnými ustanoveními občanského zákoníku.

8. Zánik účinnosti Smlouvy se nedotýká zejména nároku na náhradu škody, smluvní pokuty a povinnosti mlčenlivosti.

Článek IX.
Uveřejňovací povinnost

1. Poskytovatel prohlašuje, že si je vědom toho, že Objednatel jako povinný subjekt dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále jen „***zákon o registru smluv***"), je povinen uveřejnit v Registru smluv, jehož správcem je Ministerstvo vnitra, tuto Smlouvu, včetně jejích případných změn a dodatků, za splnění podmínek k uveřejnění dle zákona o registru smluv, a s uveřejněním Smlouvy v plném znění souhlasí.

2. Objednatel se zavazuje Smlouvu, uveřejnit ve lhůtě do 15 dnů od jejího uzavření v Registru smluv. Poskytovatel je povinen po uplynutí této lhůty, nejpozději do 20 dnů ode dne, kdy byla Smlouva uzavřena, v Registru smluv ověřit, zda Objednatel Smlouvu, řádně uveřejnil, a pokud se tak nestalo, je povinen Smlouvu, uveřejnit sám a o této skutečnosti informovat Objednatele.

3. Poskytovatel prohlašuje, že si je vědom toho, že Objednatel, jako zadavatel veřejné zakázky, jež je předmětem této Smlouvy, je povinen, v souladu s ustanovením § 219 odst. 3 ZZVZ, uveřejnit na svém profilu výši skutečně uhrazené ceny za plnění Smlouvy, v souladu s podmínkami a ve lhůtách stanovených ZZVZ včetně všech případně dalších povinností Objednatele stanovených ZZVZ.

Článek X.
Závěrečná ustanovení

1. Tato Smlouva nabývá platnosti dnem podpisu poslední ze Smluvních stran a účinnosti dnem uveřejnění Smlouvy v Registru smluv dle čl. IX odst. 2 této Smlouvy. Za den uzavření Smlouvy se považuje podpis Smlouvy druhou Smluvní stranou.

2. Smluvní strany se dohodly, že jejich práva a povinnosti založené touto Smlouvou se řídí obsahem Smlouvy. V otázkách neupravených touto Smlouvou se řídí obecně závaznými právními předpisy, zejména pak občanským zákoníkem. Smluvní strany se ve smyslu § 1 odst. 2 občanského zákoníku odchylují od ustanovení § 2050 občanského zákoníku, jehož režim se pro vztahy Poskytovatele a Objednatele dle této Smlouvy nepoužije.

3. Obě Smluvní strany se zavazují o případných změnách kontaktních údajů neprodleně informovat druhou Smluvní stranu.

4. Veškeré změny nebo dodatky k této Smlouvě mohou být činěny pouze písemně se souhlasem obou Smluvních stran. Smlouva a práva a povinnosti z ní vzniklá jsou závazná i pro případné právní nástupce Smluvních stran.

5. Poskytovatel je dle 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.

6. Pokud by se kterékoli ustanovení vyplývající z této Smlouvy ukázalo jako neplatné či nevymahatelné nebo by se takovým po dobu trvání účinnosti této Smlouvy stalo, nemá taková skutečnost vliv na ostatní ustanovení Smlouvy. Smluvní strany se zavazují takové ustanovení nahradit platným ustanovením, které je svým obsahem původnímu ustanovení nejbližší.

7. Smluvní strany se dohodly, že spory, které by případně vznikly z této Smlouvy nebo v souvislosti s ní, jakož i otázky její platnosti či neplatnosti nebo jejího vzniku a zániku, budou přednostně řešeny dohodou Smluvních stran. Pokud nebudou vyřešeny dohodou Smluvních stran, budou řešeny příslušnými soudy České republiky, přičemž pro místní příslušnost je rozhodný obecný soud Objednatele.

8. Osobami pověřenými jednat za Smluvní strany během plnění dle této Smlouvy jsou:
   a) za stranu Objednatele:
      – pro podepisování předávacích protokolů:
      jméno: [redacted]
      e-mail:
      – pro řešení technických záležitostí:
      [redacted]

b) za stranu Poskytovatele:

– pro podepisování předávacích protokolů:

[redacted]

– pro řešení technických záležitostí:

[redacted]

9. Veškerá oznámení vyplývající z této Smlouvy budou, pokud není v této Smlouvě výslovně sjednáno jinak, předána osobně proti podpisu, potvrzujícímu jejich převzetí nebo zaslána doporučeně poštou na adresu druhé Smluvní strany uvedenou v záhlaví Smlouvy. Písemnost se považuje za doručenou, i když se adresát o uložení nedozvěděl, a to 5. (slovy: pátým) dnem po jejím odeslání. To platí i v případě, že nebyla doručena na změněnou adresu bydliště nebo sídla, pokud ji příslušná Smluvní strana druhé Smluvní straně písemně neoznámí.

10. Tato Smlouva byla vyhotovena ve dvou vyhotoveních, z nichž každá ze Smluvních stran obdrží po jednom.

11. Nedílnou součástí této Smlouvy jsou následující přílohy:
    Příloha č. 1 – Popis předmětu plnění,
    Příloha č. 2 – Ostatní všeobecné bezpečnostní požadavky ZP MV ČR.

12. Smluvní strany prohlašují, že si tuto Smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.

V Praze dne ……

Kupující: [redacted]

……

Zdravotní pojišťovna ministerstva vnitra České republiky,
MUDr. David Kostka, MBA,
generální ředitel

V Praze dne ……

Poskytovatel: [redacted]

……

ALP Security, s.r.o.
Aleš Vokál, jednatel

Příloha č. 1 Smlouvy – Popis předmětu plnění:

Předmětem plnění je poskytování služeb spočívající zejména v:

1. Provádění vnějších penetrační testů představujících simulaci napadení systémů útočníkem. Cílem testů je zjistit, jak snadno identifikovatelný cíl informační systémy Objednatele představují, jaké informace lze získat o zvenčí dostupných systémech, jak detekovat zranitelnosti, které mohou být zneužity k získání neautorizovaného přístupu k citlivým systémovým zdrojům, a navrhnout doporučení k jejich odstranění.

   Vnější penetrační testy budou provedeny ze sídla Poskytovatele vůči testovaným z vnějšku dostupným systémům bez ohledu na jejich místo provozu (cloud, jiný Poskytovatel, in-house). Seznam IP adres a identifikace webové aplikace budou dodány před zahájením vlastního testování Objednatelem.

   Podrobný postup vnějších penetračních testů je uveden v článku „Postup testování".

2. Provádění vnitřních penetrační testů realizovaných z prostředí vnitřní LAN sítě Objednatele. Cílem penetračních testů je prověření bezpečnosti systému v rámci jeho provozního prostředí a provozu vnitřní sítě bez destrukčního dopadu. Penetrační test se může skládat z:
   a) testů k získání informací, identifikace funkčních systémů;
   b) všeobecných testů zranitelnosti;
   c) testů týkajících se charakteristiky infrastruktury systému;
   d) testů existence backdoors;
   e) testů autentizace a schémat pro kontrolu přístupu;
   f) kontroly operačních systémů;
   g) testů aplikačních chyb a vad v systému;
   h) testů nedostatečného provozního zabezpečení;
   i) testování slabých míst zahrnující body selhání, s cílem způsobit odmítnutí služeb webových aplikací;
   j) odposlech komunikace se systémem;
   k) odchycení a přesměrování této komunikace;
   l) zneužití odchycených informací a komunikace směrem k aplikačním službám (serverům);
   m) testů přístupu přes wi-fi síť Objednatele.

3. Vypracování písemných zpráv o stavu technické bezpečnosti prověřovaných webových aplikací a IT infrastruktury Objednatele vypracované Poskytovatelem, které Poskytovatel Objednateli předá v dohodnutém elektronickém formátu. Požadavky na zpracování písemné zprávy jsou uvedeny v článku „Obsah a struktura zprávy z testů".

Postup testování

Testování se bude skládat z následujících fází. V případě potřeby budou dohodnuty individuální postupy testování v závislosti na typu webové aplikace, popřípadě IT infrastruktury.

- Identifikace cíle;
- Identifikace aktivních služeb;
- Identifikace zranitelností;
- Získání přístupu;
- Eskalace privilegií a ovládnutí cíle;
- Reakce na testy.

Penetračními testy, které jsou předmětem plnění, není pouze provádění automatizovaných (vulnerability) skenů.

Pro testování budou využity především následující metodiky a doporučení týkající se bezpečnosti informačních systémů. Metodiky mohou být interně přizpůsobeny.

- Doporučení OWASP (Open Web Application Security Project), která se zaměřují na pomoc organizacím při identifikaci bezpečnostních hrozeb webových aplikací;
- Standard OSSTMM (Open Source Security Testing Methodology Manual) – metodologie pro testování bezpečnosti;
- Doporučení organizace IETF (Internet Engineering Task Force) – organizace vydávající RFCs tzv. standardy internetu;
- Doporučení organizace NIST (např. NIST SP 800-44 Guidlines on Securing Public Web Servers);
- Common Criteria (ISO/IEC 15408) – standard pro hodnocení úrovně bezpečnosti systémů;
- Materiály a doporučení ISACA (Information Systems Audit and Control Association) určené certifikovaným auditorům informačního systému (CISA);
- Normy pro řízení bezpečnosti IS/ICT, řízení kvality projektu a provádění auditů:
  - normy řady ISO/IEC 27000 pro oblast řízení bezpečnosti informačních systémů;
  - BS 7799-3 Směrnice pro řízení rizik souvisejících s informační bezpečností;
  - ČSN EN ISO 19011:2002 – Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu;
  - ČSN ISO 10006 – Management jakosti – Směrnice jakosti v managementu projektu.

Obsah a struktura písemné zprávy z testů

Výstupem každého testu je zpráva o stavu technické bezpečnosti prověřovaného systému a IT infrastruktury, která je rozdělena na část manažerského shrnutí a na detailní zprávu. Výstupy jsou standardně dodávány i na elektronickém médiu spolu s výstupy z použitých nástrojů a případnými doplňujícími informacemi k testům (např. screenshoty z průběhu testů).

1. Manažerské shrnutí

Pro účely managementu organizace je vypracována speciální hodnotící zpráva s cílem podchytit a stručně a srozumitelně popsat zjištěné výsledky testování a analýz.

Cílem manažerského shrnutí bude podat stručné informace o průběhu testu, ohodnotit bezpečnost webových aplikací a IT infrastruktury, tak i jednotlivých zkoumaných oblastí, a popsat nejdůležitější doporučovaná bezpečnostní opatření, která budou podrobně popsána v detailní zprávě.

2. Detailní zpráva

Obsahem detailní zprávy jsou konkrétní zjištění související s jednotlivými zkoumanými oblastmi. Detailní zpráva obsahuje následující informace:

- cíl a rozsah testu;
- popis předmětu testu;
- stanovení stupnice a metodiky hodnocení – kategorizace zjištěných zranitelností a jejich přehledné značení v rámci dokumentu;
- postup provedeného testu včetně nástrojů a technik použitých v jednotlivých fázích;
- popis zjištění z jednotlivých fází testu;
- popis nalezených zranitelnosti, každá v členění uvedeném níže;
- doporučení pro odstranění identifikovaných slabin a zranitelných míst;
- závěrečné zhodnocení provedeného testu a hodnocení aktuálně dosažené úrovně bezpečnosti testovaných aplikací.

Všechny identifikované zranitelnosti jsou popsány v následující struktuře:

a) Hodnocení/kategorizace zranitelnosti – veškeré nalezené problémy a zranitelnosti jsou rozděleny do pěti kategorií podle závažnosti:

kriticky závažná chyba (KRITICKÁ) – CRITICAL

Jako kritické chyby jsou označeny nedostatky, které byly při testech zneužity a vedly (mohou vést) k přímé kompromitaci testovaného systému.

závažné chyby (VYSOKÁ) – HIGH

Jako závažné klasifikujeme chyby, které bezprostředně umožňují kompromitaci systému, či jeho nedostupnost. U těchto chyb existuje velmi vysoká pravděpodobnost zneužití. Jejich okamžitá náprava je nutná.

středně závažné chyby (STŘEDNÍ) – MEDIUM

Do této kategorie spadají chyby, jejichž využití k potenciálnímu útoku na informační systém je technologicky náročnější na realizaci, nebo které umožňují průnik do systému pouze v případě splnění několika určitých navzájem souvisejících podmínek. Jejich závažnost nelze podceňovat s ohledem na potenciálně hrozící zneužití.

méně závažné chyby (NÍZKÁ) – LOW

Tato kategorie zahrnuje méně závažné chyby, které napomáhají napadení systému. Např. poskytují potenciálnímu útočníkovi informace, jež lze uplatnit v rámci útoku na informační systém – organizace o svém informačním systému prozrazuje více, než je nezbytně nutné. Ve většině případů se jedná pouze o konfigurační opomenutí apod.

(INFORMATIVNÍ) – INFO

Informativní kategorie označuje vše, co lze zjistit o systémech a sítích, aniž by bylo možné jakýmkoliv způsobem zabránit úniku těchto informací. Tyto údaje nejsou většinou příliš důležité pro vedení vlastního útoku, ale mnohdy mohou napomoci útočníkovi při dokreslení či doplnění celkového obrazu o cíli potenciálního napadení.

b) Klasifikace dle schopnosti útočníka – skill, neboli schopnosti útočníka, je klasifikace, která popisuje nároky kladené na schopnosti a znalosti útočníka pro realizaci daného útoku:

   - Pro identifikaci a případné zneužití zranitelnosti postačují základní znalosti a schopnosti uživatele – útočníka. Ke zneužití může dojít také neúmyslnou chybou nebo náhodným jednáním.
   - Středně obtížná náročnost s využitím automatizovaných nástrojů. Technicky zdatní útočníci, kteří s větší mírou využívají manuální metody útoku, případně převzaté skripty.
   - Velmi znalí a zkušení útočníci, kteří k útokům používají úzce specializované a sofistikované nástroje. Jedná se o přesně cílené útoky.

c) Zjištění – popis zranitelného místa/nálezu včetně popisu kde a jakým způsobem byla zranitelnost identifikována.

d) Riziko – popis rizik plynoucích z možného zneužití zranitelného místa včetně možných scénářů zneužití (kdo a za jakých podmínek může zranitelnost zneužít a jaké jsou možné dopady tohoto zneužití), posouzení dopadu rizika na produkční prostředí.

e) Doporučení – doporučení vedoucí k odstranění nalezených nedostatků, případně návrhy na zvýšení bezpečnosti stávajících bezpečnostních mechanismů a opatření. Tato doporučení se mohou týkat procesních změn, konfigurace zařízení (hardening systémů), návrhu nových bezpečnostních mechanismů pro zvýšení stávající úrovně bezpečnosti, doporučení pro uživatelská PC pro zvýšení bezpečnosti atd.

f) Přílohy (výstupy z použitých nástrojů, printscreeny, důkazy apod.).

Příloha č. 2 Smlouvy – Ostatní všeobecné bezpečnostní požadavky ZP MV ČR:

I. Úvod

Účelem je definovat závazné obecné bezpečnostní požadavky pro Poskytovatele, jejichž předmětem plnění pro Objednatele je (výhradně či jako součást předmětu plnění jiné služby) vývoj, implementace a/nebo servis software či hardware (dále také jen „***SW***" či „***HW***"), a/nebo kteří v souvislosti s plněním pro Objednatele přistupují do informačního a komunikačního systému Objednatele (dále také jen „***systém ICT***"), a/nebo kteří v rámci poskytovaného plnění pro Objednatele zpracovávají, a/nebo přenášejí a/nebo ukládají a/nebo archivují jakákoli data a informace Objednatele a/nebo jeho zákazníků (dále také jen „***Bezpečnostní požadavky***"). Účelem tohoto dokumentu je současně definovat požadavky na Poskytovatele dle platné právní úpravy, především pak dle ustanovení § 5 odst. 2 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a § 7 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), přičemž zohledňuje také ostatní související platné právní předpisy týkající se dané problematiky.

II. Obecné požadavky

a) pokud Poskytovatel využívá při poskytování plnění subdodavatele, Poskytovatel se zavazuje zajistit dodržování Bezpečnostních požadavků rovněž ve smluvních vztazích se svými subdodavateli; přičemž tuto skutečnost se Poskytovatel zavazuje doložit Objednateli na vyžádání předložením příslušného smluvního vztahu uzavřeného s tímto subdodavatelem Poskytovatele, případně předložením čestného prohlášení o řádném naplňování této povinnosti;

b) nestanoví-li dohoda stran jinak, Poskytovatel jmenuje nejpozději do 3 dnů po uzavření smlouvy zodpovědnou kontaktní osobu pro potřeby zajištění plnění Bezpečnostních požadavků a související komunikace mezi smluvními stranami (dále také jen „Kontaktní osoba").

c) Pokud při plnění předmětu smlouvy dochází ke zpracování osobních údajů, Poskytovatel se zavazuje zajistit uzavření samostatných smluv ve smyslu příslušných ustanovení zákona č. 110/2019 Sb., o zpracování osobních údajů v platném znění (zejména pak jeho ustanovení §34 a §47) a Nařízení Evropského parlamentu a Rady (EU) 2016/679, 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);

d) dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů společnosti Objednatele resp. platné řídící dokumentace Objednatele či její části, pokud byl s takovými dokumenty nebo jejich částmi seznámen.

III. Bezpečnostní požadavky na vývoj SW

Poskytovatel se při poskytování plnění pro Objednatele zavazuje:

a) poskytovat Objednateli v termínech stanovených Objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje SW či po jeho předání;

b) k dodání systémové a provozní bezpečnostní dokumentace nejpozději do doby předání a převzetí SW způsobem uvedeným ve smlouvě, a to minimálně v rozsahu stanoveném v odst. 4 této přílohy;

c) že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování SW a/nebo které jsou specifikovány výslovně ve smlouvě (zejména, že SW nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.);

d) že pokud součástí plnění je i instalace operačního systému případně SW třetích stran, v průběhu jeho instalace budou použity nejnovější aktualizované verze těchto produktů;

e) že veškeré důvěrné informace[1] poskytnuté Objednateli při realizaci plnění nebudou uchovávány v nešifrovaném tvaru a budou chráněna vůči neautorizovanému přístupu, nebude-li mezi smluvními stranami v konkrétním případě dohodnuto jinak;

f) že v rámci poskytovaného plnění bude instalovat SW nebo jejich upgrade podle hardeningových bezpečnostních politik a v souladu s bezpečnostními standardy Objednatele (platí pro Poskytovatele, pokud byl s takovými bezpečnostními standardy seznámen);

g) že v produkčním prostředí systému ICT bude obsažen jen kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování systému ICT;

h) že před spuštěním SW v produkčním prostředí daného systému ICT provede kontrolu souladu daného SW s bezpečnostními požadavky hardeningových bezpečnostních politik a v případě zjištění nesouladu zajistí bez zbytečného odkladu soulad dodávaného SW s bezpečnostními požadavky hardeningových politik (platí pro Poskytovatele, pokud byl s takovými bezpečnostními standardy seznámen);

i) že bude instalovat nový SW nebo nové verze SW pouze na základě Objednatelem předem schválených migračních postupů[2];

j) že ověří integritu zdrojového kódu a předá zdrojový kód Objednateli bezpečnou formou zajišťující integritu zdrojového kódu, přičemž bude průběžně evidovat a bezpečné ukládat zdrojové kódy provozovaných aplikací, a to i v případě, že budou zdrojové kódy předávány Objednateli, přičemž při vývoji SW se Poskytovatel zavazuje, že:
   - zdrojový kód programů vyvíjených Poskytovatelem bude předmětem procesu řízení verzí;
   - zdrojový kód programů je zálohován a uložen mimo produkční prostředí a současně je stanoven postup, jak sestavit systém ze zdrojového kódu;
   - provádění konfiguračních změn je v souladu s procesem změnového řízení Objednatele;
   - konfigurační soubory jsou pravidelně průběžně zálohovány;
   - eviduje každou změnu konfigurace.

IV. Požadavky na systémovou a provozní bezpečnostní dokumentaci.

Nedílnou součástí poskytovaného plnění je zdokumentování všech bezpečnostních nastavení, funkcí a mechanismů formou zpracování bezpečnostní dokumentace. Poskytovatel se v rámci poskytovaného plnění pro Objednatele zavazuje předat Objednateli dokumentaci minimálně v následujícím nebo obdobném rozsahu:

- strategie obnovy,
- dokumentace skutečného provedení,
- popis autorizačního konceptu a oprávnění,
- zálohovací a archivační postupy,
- instalační a konfigurační postupy;
- bezpečností nastavení.

[1] Za důvěrné informace se ve smyslu této přílohy považují zejména identifikační údaje certifikátu, hesla, konfigurační soubory, systémové programy, kritické knihovny, obnovovací procedury apod.

[2] Migrační postup – soubor kroků definující převod dat mezi dvěma nebo více systémy ICT.

V. Fyzická ochrana a bezpečnost prostředí

a) Poskytovatel se zavazuje dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny komponenty systémů ICT anebo datové nosiče (dále také jen „Pracoviště").

b) Poskytovatel se zavazuje, že na Pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k systému ICT, který je předmětem plnění dle této smlouvy.

VI. Řízení přístupu

a) Poskytovatel bere na vědomí, že přístup k systému ICT je možné povolit pouze fyzické identitě zaměstnance Poskytovatele / poddodavatele Poskytovatele zaevidované v registru identit Objednatele, a to na základě požadavku Poskytovatele na přístup.

b) Poskytovatel bere na vědomí, že zaměstnanec Poskytovatele musí prokazatelně souhlasit se zpracováním osobních údajů potřebných pro zřízení přístupu, v opačném případě Objednatel není povinen přístup k systému ICT zaměstnanci Poskytovatele povolit. Zaměstnanec Poskytovatele s přiděleným přístupem (fyzickým, logickým) k systému ICT musí prokazatelně souhlasit se zpracováním osobních údajů zpracovávaných během vyhodnocování údajů o pohybu a prováděných aktivitách v prostorách Objednatele (např.: monitoring pomocí řešení Security Incident and Event Monitoring), přičemž takový souhlas musí být proveden souhlasem písemným nebo digitálním formou emailu, není-li smluvními stranami dohodnuto jinak.

c) Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci Poskytovatele musí být řízeno principem nezbytného minima a není nárokové.

d) Poskytovatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Poskytovatele nebo subdodavatele Poskytovatele.

e) Poskytovatel se zavazuje, že ICT systém bude ověřovat identitu uživatelů, administrátorů a aplikací odpovídajícím způsobem dle nároků definovaných v §19 odst. 3 či 4, případně odst. 5 vyhlášky o kybernetické bezpečnosti.

f) Poskytovatel se zavazuje, že přístup do systému ICT prostřednictvím mobilní aplikace bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení VPN.

g) Poskytovatel se zavazuje, že před připojením koncového zařízení, mobilní koncového zařízení nebo aktivního síťového prvku jako síťové switche, WiFi access pointy, routery či huby do počítačové sítě zažádá o schválení připojení kontaktní osobu na straně Objednatele.

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

i) Poskytovatel se zavazuje, že nebude instalovat a používat tyto typy nástrojů:
   - Keylogger,
   - Sniffer,
   - Analyzátor zranitelností a Port Scanner,
   - Backdoor, rootkit a trojský kůň nebo jinou podobu malware.

j) Poskytovatel se zavazuje, že všechny ICT systémy Poskytovatele, které se připojují do síťové infrastruktury Objednatele, jsou a budou chráněny proti malware.

k) Poskytovatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části systému ICT programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci systému ICT nebo nelegální získání dat a informací.

l) Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli vyvarují se níže uvedeného jednání při připojení do síťové infrastruktury Objednatele/na stanicích připojovaných do síťové infrastruktury Objednatele/při poskytování plnění/apod:

- nenavštěvovali internetové stránky s eticky nevhodným obsahem[3];
- neukládali a/nebo nesdíleli data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;
- nestahovali, nesdíleli, neukládali, nearchivovali a/nebo neinstalovali datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem;
- neukládat a/nebo nesdíleli data a informace společnosti na nepovolených datových úložištích nebo médiích;
- nezasílali řetězové emaily.

m) Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě a/nebo systému ICT Objednatele, respektovali a dodržovali následující omezení:
Zařízení typu notebook/počítač musí mít:

- aplikovány bezpečnostní záplaty (operačního systému, internetového prohlížeče a Javy),
- nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu;

n) Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě a/nebo systému ICT Objednatele chránili autentizační prostředky a údaje k systémům ICT Objednatele. Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako bezpečnostní incident ve smyslu příslušné řídící dokumentace a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu). Poskytovatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Bezpečnostních požadavků nebude posuzován jako okolnost vylučující odpovědnost Poskytovatele za prodlení s řádným a včasným plněním předmětu smlouvy a nebude důvodem k jakékoli náhradě případné újmy Poskytovateli či jiné osobě ze strany Objednatele.

VII. Monitorování

a) Poskytovatel bere na vědomí, že veškerá aktivita Poskytovatele a jeho plnění realizované v systémovém prostředí Objednatele budou Objednatelem průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na obsah smlouvy a interních dokumentů Objednatele, se kterými byl Poskytovatel seznámen.

b) Poskytovatel se zavazuje, že záznamy/logy obsahující výsledky monitorování, úspěšná a neúspěšná přihlášení do ICT systému a záznamy o správě uživatelů je povinen na vyžádání a bez zbytečného odkladu předložit Objednateli, a to po celou dobu trvání smlouvy i o jejím ukončení.

VIII. Předání a převzetí plnění

a) Poskytovatel bere na vědomí, že nedodržení Bezpečnostních požadavků včetně požadavku na předání kompletní systémové a provozní dokumentace je vadou bránící převzetí předmětu smlouvy (je vadou kategorie A), přičemž Objednatel není do doby odstranění příslušné vady plnění povinen plnění převzít.

[3] Data a informace obsahující prvky extrémismu, terorismu, pornografie anebo podněcování k nesnášenlivosti a společenským předsudkům vztahujícím se ke společenské skupině identifikované na základě rasy, náboženství nebo víry, pohlaví, sexuální orientace, národnostní a etnické příslušnosti či jiné odlišnosti.

b) Poskytovatel odpovídá za to, že systémy ICT budou obsahovat nejnovější bezpečnostní aktualizace (patche)[4] po celou dobu smlouvy není-li ve smlouvě definováno jinak.

IX. Výměna informací

a) Pokud je předmětem smlouvy výměna informací mezi smluvními stranami, musí být mezi smluvními stranami uzavřena dohoda o ochraně předmětných informací, zejména při jejich výměně, uložení, archivaci a ukončení smlouvy.

b) Poskytovatel se zavazuje, že veškerý přenos dat a informací musí být dostatečně zabezpečen z pohledu bezpečnostní klasifikace Kupujícího a tedy požadavků na důvěrnost, integritu a dostupnost dat a informací.

c) Poskytovatel se zavazuje, že on-line transakce realizované prostřednictvím webových technologií budou chráněny SSL certifikáty.

X. Zvládání bezpečnostních incidentů[5]

Poskytovatel se při poskytování plnění pro Objednatele zavazuje, že:

a) neprodleně nahlásí bezpečnostní událost přes Kontaktní osobu Objednatele uvedenou ve smlouvě;

b) v případě vzniku bezpečnostní události a následného zvládání a vyhodnocování bezpečnostního incidentu a/nebo v případě podezření na bezpečnostní incident, poskytne Objednateli požadovanou součinnost (např.: poskytne logy a identifikační údaje (např. IP adresa, MAC adresa, HW typ, sériové číslo případně IMEI) dotyčného koncového zařízení nebo mobilního koncového zařízení zaměstnance Poskytovatele nebo zaměstnance poddodavatele podílející se na realizaci plnění, k analýze obsahu, případně bez zbytečného odkladu zrealizuje opatření požadovaná Objednatelem). provede analýzu příčin bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že Poskytovatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

Bezpečnostní událost: událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací[6].

Bezpečnostní incident: narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku bezpečnostní události.

[4] Aktualizace software na vyšší vývojovou verzi.

[5] Pojem bezpečnostní incident a bezpečnostní událost je ekvivalentní pojmům Kybernetická bezpečnostní událost / Kybernetický bezpečnostní incident, vydefinovaných zákonem č. 181/2014 Sb. o kybernetické bezpečnosti.

[6] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů