Prováděcí SMLOUVA

Zajištění BEZPEČNOSTNÍCH informačních auditů a poskytování penetračních testů

Smluvní strany:

**Česká republika – Ministerstvo zemědělství**

se sídlem: Těšnov 65/17, 110 00 Praha 1 – Nové Město,

IČO: 00020478

DIČ: CZ00020478

zastoupená: Ing. Petrem Kutálkem, ředitelem Odboru bezpečnostní politiky a krizového řízení

bankovní spojení: ČNB Praha 1, Na Příkopě 28

číslo účtu: 1226001/0710

(dále jen jako „**Objednatel**“ nebo „MZe“)

*Číslo výzvy: 04, číslo smlouvy DMS: ČJ. MZE-36533/2023-10023, číslo smlouvy: 940-2023-10023*

a

Deloitte Advisory s.r.o.

se sídlem: Italská 2581/67, Praha 2 Vinohrady

IČO: 275 82 167, DIČ: CZ275 82 187, Je plátcem DPH

společnost zapsaná v obchodním rejstříku vedeném Městským soudem v Praze,

spisová značka 113225 C

bankovní spojení: ING Bank N.V. Českomoravská 2420/15, 190 00 Praha 9 - Libeň, číslo účtu: 1000037000/3500

zastoupená: Pavel Šiška, na základě zmocnění ze dne 30. 11. 2020

(dále jen „Poskytovatel“)

*číslo smlouvy Poskytovatele:*

dnešního dne uzavřely na základě výzvy objednatele dle čl. 1 odst. 1.6. Rámcové smlouvy uzavřené mezi nimi dne 31. 10. 2019 tuto prováděcí smlouvu v souladu s ustanoveními § 1746 odst. 2, § 2358 a násl. a § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**“)

(dále jen „**Prováděcí smlouva**“).

1. ÚVODNÍ USTANOVENÍ
   1. Tato Prováděcí smlouva se uzavírá jako prováděcí smlouva k rámcové smlouvě RÁMCOVÁ SMLOUVA O POSKYTOVÁNÍ SLUŽEB uzavřené Objednatelem a Poskytovatelem dne 31. 10. 2019, číslo smlouvy: 596-2019-10023, číslo sml. DMS 55513/2019-MZE-10023 (dále jen “**Rámcová smlouva**”)**.**
   2. Práva a povinnosti stran při poskytování plnění dle této Prováděcí smlouvy se řídí ustanoveními této Prováděcí smlouvy a ustanoveními Rámcové smlouvy.
   3. Ustanovení Rámcové smlouvy mají v případě rozporu přednost před ustanoveními této Prováděcí smlouvy, ledaže by se jednalo o nepodstatnou změnu v podmínkách Rámcové smlouvy ve smyslu § 222 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“).
2. PŘEDMĚT SMLOUVY
   1. Poskytovatel se na základě této Prováděcí smlouvy zavazuje poskytnout Objednateli služby uvedené v příloze č. 1 této Prováděcí smlouvy.
   2. Objednatel se zavazuje zaplatit za řádně poskytnuté služby cenu v souladu s podmínkami Rámcové smlouvy.
   3. Celkový rozsah služeb poskytovaných na základě této Prováděcí smlouvy nepřekročí 282 člověkohodin.
   4. Poskytovateli uzavřením této Prováděcí smlouvy nevzniká právo na čerpání plnění v předpokládaném rozsahu stanoveném v příloze č. 1 Rámcové smlouvy.
3. DOBA A MÍSTO PLNĚNÍ
   1. Místem plnění této Prováděcí smlouvy se sjednává: budova Ministerstva zemědělství na adrese Těšnov 65/17, 110 000 Praha 1 – Nové Město nebo vzdálený přístup k testovanému systému.
   2. Služby budou poskytovány v době stanovené v harmonogramu uvedeném v příloze č. 2 této Prováděcí smlouvy.
   3. Termín pro potvrzení výzvy v souladu s ustanovením 1.8 Rámcové smlouvy je pět pracovních dní.
4. OSTATNÍ UJEDNÁNÍ
   1. Objednatel je oprávněn pozastavit poskytování plnění dle této Prováděcí smlouvy svým jednostranným písemným oznámením doručeným Poskytovateli, a to bez jakýchkoliv sankcí. Pozastavení plnění se stává účinným třetím dnem následujícím po doručení oznámení o pozastavení plnění Poskytovateli. Právo Poskytovatele na úhradu ceny řádně poskytnutého plnění do doby pozastavení plnění tím není dotčeno.
5. TRVÁNÍ SMLOUVY
   1. Tato Prováděcí smlouva nabývá účinnosti doručením přijetí návrhu na její uzavření smluvní straně, která návrh na uzavření Prováděcí smlouvy učinila, a potvrzením výzvy v souladu s odst. 1.6 Rámcové smlouvy. V případě, že však tato Prováděcí smlouva splňuje podmínky pro její uveřejnění v registru smluv dle zákona č. 340/2015 Sb., ve znění pozdějších předpisů, nabude Prováděcí smlouva účinnosti dnem jejího uveřejnění v registru smluv.
   2. Tato Prováděcí smlouva se uzavírá na dobu určitou, a to do na dobu šesti měsíců ode dne nabytí její účinnosti.
   3. Objednatel je oprávněn odstoupit od této Prováděcí smlouvy za podmínek uvedených v odst. 8.6 a 8.7 Rámcové smlouvy.
   4. Poskytovatel je dále oprávněn od této Prováděcí smlouvy odstoupit za podmínek stanovených příslušnými právními předpisy.
   5. Objednatel je oprávněn bez jakýchkoliv sankcí tuto Prováděcí smlouvu vypovědět bez udání důvodů, a to s měsíční výpovědní lhůtou, která začne běžet následujícím dnem po dni, kdy byla písemná výpověď doručena Poskytovateli.
6. ZÁVĚREČNÁ USTANOVENÍ
   1. Poskytovatel svým podpisem níže potvrzuje, že souhlasí s tím, aby obraz této Prováděcí smlouvy, včetně jejích příloh a případných dodatků a metadat k této Prováděcí smlouvě, byly uveřejněny v registru smluv v souladu se zákonem 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. Smluvní strany se dohodly, že podklady dle předchozí věty odešle za účelem jejich uveřejnění správci registru smluv Objednatel; tím není dotčeno právo Poskytovatele k jejich odeslání. Z důvodu uveřejnění této Prováděcí smlouvy v registru smluv, nepodléhá tato smlouva povinnosti uveřejnění na profilu zadavatele (Objednatele) s odkazem na ustanovení § 219 odst. 1 písm. d) ZZVZ. Poskytovatel tímto uděluje souhlas Objednateli k uveřejnění všech podkladů, údajů a informací uvedených v tomto odstavci a těch, k jejichž uveřejnění vyplývá pro Objednatele povinnost dle právních předpisů.
   2. Nedílnou součást této Prováděcí smlouvy tvoří tyto přílohy:

|  |  |
| --- | --- |
| Příloha č. 1: | Popis poskytovaných služeb |
| Příloha č. 2: | Harmonogram plnění |

* 1. Tato Prováděcí smlouva je uzavřena ve čtyřech stejnopisech, z nichž každá strana obdrží po dvou stejnopisech.

V Praze dne 19.6.2023 V Praze dne 15.6.2023

…..……………………………………………… …..………………………………………………

Česká republika - Ministerstvo zemědělství Deloitte Advisory s.r.o.

Ing. Petr Kutálek, XXX

ředitel Odboru bezpečnostní politiky a krizového řízení

Jednatel

Příloha č. 1

1. **Předmět plnění**

Předmětem plnění je poskytnutí komplexních penetračních testů, včetně souvisejících služeb, v prostředí Ministerstva zemědělství Poskytovatelem, s velkým důrazem na splnění podmínky nezávislosti.

Primárním předmětem těchto služeb je zajištění odborných profesních služeb ICT dle konkrétních potřeb Objednatele v oblasti problematiky bezpečnostních informačních auditů a komplexních penetračních testů pro Objednatele, příp. celý resort MZe v souladu se závaznými standardy a principy Objednatele, zejména dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a norem ISO 27000. Jedná o následující činnosti, jejichž specifikace je uvedena v bodu 2. této přílohy.

1. **Specifikace předmětu požadovaného plnění:**

Budou provedeny **penetrační testy webu/portálu MZe „xxx“** s cílem ověřit technologickou a konfigurační bezpečnost daného portálu, a to s ohledem na:

* odolnost vůči manipulaci s obsahem
* odolnost vůči přístupu k autentizovanému obsahu
* možné dlouhodobé nedostatky přetrvávající na technologii
* možné nedostatky nesprávnou (nevhodnou) implementací technologie

Předmětem testů je ověření webu MZe „xxx“ včetně jeho testovací varianty („xxx“) a identifikace jeho případných závažných zranitelností, které by mohly vést k ohrožení požadovaných parametrů jeho provozu nebo k jeho neoprávněnému způsobu použití/zneužití. Spolu s identifikací zranitelností bude ověřena též jejich reálná zneužitelnost či možnost jejich výskytu nebo uplatnění a vymezena hlavní účinná opatření k jejich eliminaci.

Penetrační testy budou typově primárně zaměřeny na technologickou a systémově–aplikační vrstvu portálu, a to především z hlediska přístupu z vnějšího prostředí MZe.

Penetrační testy budou zahrnovat:

* Externí penetrační test prostředí portálu „xxx“
* Externí penetrační retest prostředí portálu „xxx“
* Skenování známých zranitelností systému jako celku
* Provedení penetračních testů bude doplněno orientačním testem zdrojových kódů
* Zpracování zprávy z penetračních testů
* Případný retest po odstranění identifikovaných slabin a nedostatků.

Dále mohou být požadovány služby bezpečnostního posouzení realizačních záměrů a bezpečnostních kontrol v souvislosti s uvedeným posouzením, v závislosti na aktuálních potřebách zadavatele.

Bezpečnostní posouzení bude zahrnovat minimálně:

* Kontrola dokumentace k záměrům projektů a identifikace informačně-bezpečnostních aspektů
* Zhodnocení možných bezpečnostních rizik a soulad s Bezpečnostními politikami MZe
* Doporučení vedoucí k opatřením na minimalizaci rizika v souladu s identifikovanými bezpečnostními riziky, nebo k odstranění nekonzistencí vzhledem k BP
* Kontrola faktického stavu bezpečnostních aspektů po realizaci projektu
* Zpracování vyjádření k bezpečnostnímu posouzení nebo kontrole faktického stavu po realizaci
  1. **Výstup z penetračních testů**

Výstupem penetračních testů bude zpráva z penetračních testů zahrnující:

* Manažerský souhrn hlavních zjištění a doporučení
* Základní informace o provedeném bezpečnostním testu (časový rámec, cíl a rozsah, použité postupy a techniky)
* Souhrnné informace k průběhu provedených testů s důrazem na faktory ovlivňující jejich průběh a výsledek
* Popis bezpečnostních slabin a specifikace doporučených protiopatření s důrazem na úroveň rizik jednotlivých slabin a prioritu doporučovaných opatření.
  1. **Ochrana informací MZe a požadavky na součinnost**

Potřebné informace budou zjišťovány formou konzultací s určenými pracovníky Objednatele a Poskytovatele s tím, že v případě potřeby budou též zpřístupněny vybrané nutné informace a dokumenty (např. uživatelská dokumentace, popisy architektury řešení, konfigurací a nastavení použitých komponent, popisy komunikačních protokolů apod.). Maximální zatížení zaměstnanců Objednatele nepřekročí 8 člověkodnů pro jednotlivý systém.

Po dobu provádění bezpečnostních a penetračních testů budou v rámci součinnosti, Objednatelem zajištěny tyto technologické podmínky:

* Stabilita testovaných prostředí (zejména z hlediska konfigurace, prvků a verzí systémového a aplikačního vybavení)
* Dostatečná exkluzivita k provedení testů v tom smyslu, že nebudou prováděny jiné aktivity, které by s testováním byly kolizní (např. zátěžové testy, rekonfigurace apod.).
* Případné potřebné přístupy, role a účty nutné k testování.

Testy budou prováděny takovým způsobem, aby byla minimalizována rizika jejich negativního dopadu na infrastrukturu a aplikace Objednatele, zejména:

* testy budou prováděny ve stanovených prostředích a ve stanoveném rozsahu
* automatizované nástroje (např. skenery zranitelností) budou nastaveny po dohodě s Objednatelem s akceptovatelnou mírou intenzity skenování. Nebudou prováděny činnosti, které by mohly závažným způsobem negativně ovlivnit provozovanou internetovou/intranetovou infrastrukturu bez předešlého souhlasu pověřených pracovníků MZe.

V případě zjištění závažné chyby může být, po dohodě s MZe, provedeno intenzivnější (s dopadem do dostupnosti) nebo invazivnější (s dopadem do stability) prověření. Pro tyto potřeby musí být vyhrazen samostatný termín nebo režim, po schválení Objednatelem. Pro vyloučení pochybností smluvní strany uvádí, že v souladu s článkem 4.4 rámcové smlouvy výše uvedené služby jsou služby, které budou evidovány ve Výkazech poskytnutých služeb předložených Poskytovatelem Objednateli po ukončení měsíce, ve kterém byly služby poskytovány. Za tímto účelem bude Poskytovatel předávat elektronicky týdenní předběžné souhrny těchto služeb jako podklad pro měsíční kontrolu skutečně provedených a poskytnutých služeb. Akceptace skutečně provedených a poskytnutých služeb se provádí na základě schválení výkazu poskytnutých služeb.

Příloha č. 2

**Harmonogram a termín plnění**

**Závazný harmonogram plnění**

Penetrační testy budou probíhat v předem stanovených termínech po vzájemné dohodě Objednatele a Poskytovatele, a to v rámci platnosti této Prováděcí smlouvy a jejího trvání.

Dohoda termínů provedení jednotlivých činností bude uskutečňována v rámci společných jednání. Z těchto jednání bude prováděn zápis, jež bude obsahovat závazné termíny pro uskutečnění jednotlivých dílčích činností. V případě nedodržení termínu realizace bude uplatněna sankce dle článku 9.1. Rámcové smlouvy.

Pro potřeby testů mohou být využívány pracovní doby v případě testovacího prostředí, produkční prostředí mimo provozní špičky, tedy v době v pracovních dnech a víkendech od 00 hodin do 6 hodin ráno. K ukončení služby dojde tři kalendářní měsíce po podpisu této Prováděcí smlouvy.

| Fáze | Název činnosti | (ČLH1) |  |
| --- | --- | --- | --- |
| 1 | Úvodní test v testovacím prostředí | 98 |  |
| 2 | Příprava zprávy z testu v testovacím prostředí | 16 |  |
| 3 | Retest nálezů z testovacího prostředí | 22 |  |
| 4 | Test po nasazení do produkce | 75 |  |
| 5 | Příprava zprávy z testu v produkci | 8 |  |
| 6 | Retest nálezů z produkčního prostředí | 22 |  |
| 7 | Quality Assurance | 41 |  |
|  | CELKEM | 282 |  |

předpokládaný počet hodin potřebných na straně poskytovatele k poskytnutí poptávaných služeb

V rámci harmonogramu je proveden návrh ČLH, a to v celkové výši maximálně 282, tedy celková fakturovaná částka v rámci této prováděcí smlouvy nepřesáhne jejich uvedený počet. Obecné ujednání: Fakturace bude probíhat s odkazem na čl. 4.4 Rámcové smlouvy o poskytování služeb.

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 16.6.2023 V Praze dne 15.6.2023

…..……………………………………………… …..………………………………………………

Česká republika - Ministerstvo zemědělství Deloitte Advisory s.r.o.

Ing. Petr Kutálek, XXX

ředitel Odboru bezpečnostní politiky a krizového řízení

Jednatel