Smlouva o dílo

uzavřená ve smyslu ustanovení § 2586 a násl. zákona č. 89/2012 Sb.,
občanský zákoník (dále též „občanský zákoník“)

Jihočeský kraj
se sídlem: U Zimního stadionu 1952/2
370 76 České Budějovice
zastoupený: Ing. Petrem Vobejdou, vedoucím odboru informatiky
IČO: 70890650
DIČ: CZ70890650
bankovní spojení: 199783072/0300, ČSOB, a.s.

dále též „objednatel“

a

AEC a.s.
se sídlem Voctářova 2500/20a,
Libeň, 180 00 Praha 8
zastoupena: Ing. Tomášem Strýčkem, členem představenstva
IČO: 04772148
DIČ: CZ04772148
bankovní spojení: číslo účtu: 8176852 / 0800
zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, spisová zn: B 21326

dále též „zhotovitel“

společně též „smluvní strany“

uzavírají níže uvedeného dne tuto smlouvu o dílo.

1 Předmět smlouvy

1.1 Zhotovitel se touto smlouvou o dílo zavazuje provést na svůj náklad a nebezpečí pro objednatele dílo specifikované v příloze smlouvy (dále též „dílo“) a objednatel se zavazuje dílo převzít a zaplatit cenu.

2 Doba a místo dodání díla

2.1 Smlouva se uzavírá na dobu určitou, do úplného předání díla.

2.2 Dílo bude předáváno postupně, po etapách, v souladu s uvedeným harmonogramem předání díla. Výchozím dnem „T“ je den účinnosti smlouvy.

Etapy plnění	Termín
Zahájení penetračního testování	T
Předání výsledků penetračního testování	do T + 30
Připomínkování výsledků penetračního testování ze strany Příjemce	do T + 37
Odstranění připomínek k výsledkům penetračního testování ze strany Poskytovatele	do T + 44
Předání výsledků penetračního testování Příjemci k odstranění zjištěných nedostatků	do T + 51
Příjemce odstraní nahlášené nedostatky	do T + 81
Provedení ověření nápravných opatření realizovaných Příjemcem	do T + 95
Předání Předávacího protokolu Příjemci	do T + 102

Připomínkování Předávacího protokolu ze strany Příjemce	do T + 109
Odstranění připomínek k Předávacímu protokolu ze strany Poskytovatele	do T + 116
Vysvětlení pojmů, závěrů, návrhů řešení nalezených nedostatků	do T + 116
Dodání Vulnerability management software dle přílohy č. 1, písm. b)	do T + 116
Školení nástroje software Vulnerability management software	do T + volitelné, kdykoliv

2.3 O předání díla bude sepsán protokol podepsaný oprávněnými zástupci smluvních stran. Budou-li zjištěny vady díla nebo jeho části již při jeho přejímání, je třeba takovou skutečnost uvést do protokolu. Zhotovitel je povinen zjištěné vady odstranit, a to ve lhůtě 10 dnů od jejich zachycení v protokolu. Po dobu odstraňování vad neběží objednateli lhůta k placení. Odstraňování závad nezbavuje zhotovitele povinnosti dokončit další plnění v řádných termínech

2.4 Místem plnění a dodání díla je sídlo objednatele.

2.5 Objednatel nabývá vlastnické právo převzetím bezvadného díla.

3 Cena a platební podmínky

3.1 Cena byla stanovena na základě nabídky zhotovitele, a činí celkem 333 300,- Kč bez DPH. Sazba DPH bude k ceně za dílo připočtena v souladu s příslušnými právními předpisy. Přesný rozpis ceny za jednotlivá plnění je uveden v následující tabulce.

	Cena bez DPH v Kč	**Výše DPH v Kč**	**Cena s DPH v Kč**
Penetrační testování dle přílohy č. 1, písm. a): webové stránky Jihočeského kraje: www.kraj-jihocesky.cz	44 400	9 324	53 724
Penetrační testování dle přílohy č. 1 písm. a): extranet Jihočeského kraje: priv.kraj-jihocesky.cz	88 800	18 648	107 448
Vysvětlení pojmů, závěrů, návrhů řešení nalezených nedostatků	11 100	2 331	13 431
Dodání Vulnerability management software dle přílohy č. 1, písm. b)	189 000	39 690	228 690
Školení nástroje software Vulnerability management software	V ceně licence	V ceně licence	V ceně licence
Celková nabídková cena za dílo v Kč	333 300	69 993	403 293

3.2 Cena je konečná a zahrnuje veškerá náklady spojené s provedením díla.

3.3 Cena bude uhrazena na základě daňového dokladu (faktury) vystavené zhotovitelem, a to po dokončení díla a jeho převzetí objednatelem. Objednatel nebude poskytovat zálohy. Splatnost faktury je 14 dnů ode dne jejího doručení objednateli.

3.4 Vystavená faktura bude mít náležitosti daňového dokladu dle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, v souladu s § 435 občanského zákoníku. Faktura musí dále obsahovat:

a) číslo smlouvy,
b) předmět plnění a jeho přesnou specifikaci ve slovním vyjádření (nestačí pouze odkaz na číslo uzavřené smlouvy),
c) označení banky a čísla účtu, na který musí být zaplaceno,
d) lhůtu splatnosti faktury,
e) datum uskutečnitelného zdanitelného plnění shodné s datem předání plnění objednateli,
f) název, sídlo, IČO a DIČ příjemce a poskytovatele včetně údajů o zápisu do OR,
g) jméno osoby, která fakturu vystavila, včetně kontaktního telefonu.

3.5 Jestliže nebude faktura obsahovat veškeré údaje, nebo pokud v ní nebudou správně uvedené údaje, je objednatel oprávněn vrátit ji ve lhůtě 5 pracovních dnů od jejího převzetí zhotoviteli s uvedením chybějících náležitostí nebo nesprávných údajů. V takovém případě se přeruší doba splatnosti a nová lhůta splatnosti počne běžet doručením opravené faktury objednateli.

4 Záruka a odpovědnost za vady

4.1 Zhotovitel je povinen provést dílo tak, aby bylo bez vad a nedodělků, a v takovém stavu a kvalitě, která umožňuje jeho řádné převzetí a užívání objednatelem.

4.2 Zhotovitel prohlašuje, že zaručuje dohodnuté vlastnosti díla, a to po dobu 24 měsíců.

4.3 Objednatel není povinen dílo nebo jeho část převzít, pokud dílo obsahuje vady, a to zejména:

- dílo neodpovídá požadované specifikaci,
- dílo obsahuje vady, které ztěžují nebo znemožňují jeho plánované užívání.

4.4 Objednatel je povinen reklamovat zjištěné vady díla písemně u zhotovitele, a to bez zbytečného odkladu poté, co je zjistil. Uplatněním reklamace se staví záruční doba na reklamované dílo či jeho část.

4.5 Zhotovitel je povinen v záruční době rozhodnout o oprávněnosti reklamace nejpozději následující pracovní den po dni nahlášení vady zboží objednatelem. Vada bude odstraněna na místě určeném objednatelem, a to nejpozději do 10 pracovních dnů od uznání oprávněnosti reklamace.

4.6 U reklamovaného díla, u kterého byla reklamace uznána, a které bylo opraveno, běží nová záruční doba ode dne předání díla objednateli.

5 Smluvní pokuta a úrok z prodlení

5.1 Dojde-li k prodlení zhotovitele s řádným a včasným dodáním díla, je objednatel oprávněn účtovat zhotoviteli smluvní pokutu ve výši 0,05 % z ceny díla vč. DPH za každý i započatý den prodlení zhotovitele. Případné odstoupení od smlouvy nemá vliv na povinnost zhotovitele zaplatit smluvní pokutu.

5.2 Je-li zhotovitel v prodlení s odstraněním reklamované vady, je objednatel oprávněn účtovat zhotoviteli úrok z prodlení ve výši 0,05 % z celkové ceny za dílo za každý i započatý den prodlení.

5.3 Výše uvedenými ustanoveními není dotčeno právo na náhradu škody.

6 Komunikace mezi stranami

6.1 Ve věcech odborných, technických a převzetí díla jsou určeny následující kontaktní osoby.

Na straně objednatele:

Bc. Radek Hauser, tel.: 386 720 194, e-mail: hauser@kraj-jihocesky.cz
Bc. Aleš Velek DiS., tel.: 386 720 508, e-mail: velek@kraj-jihocesky.cz

Na straně zhotovitele:

Za oblast penetračních testů:

Ing. Filip Zvařič, tel.: 602 281 310, e-mail: filip.zvaric@aec.cz

Za oblast Nessus Professional a VMS:

Ing. David Pecl, tel.: 732 689 554, e-mail: david.pecl@aec.cz

7 Ukončení smlouvy

7.1 Tuto smlouvu je možné ukončit dohodou stran.

7.2 Objednatel je oprávněn od smlouvy odstoupit, pokud zhotovitel nedodá řádně a včas plnění dle této smlouvy, anebo bude z jeho postupu zřejmé, že dílo řádně a včas dodáno nebude, a dále v případě, když probíhá insolvenční řízení proti majetku zhotovitele, v němž bylo vydáno rozhodnutí o úpadku, nebo insolvenční návrh byl zamítnut proto, že majetek zhotovitele nepostačuje k úhradě nákladů insolvenčního řízení, nebo byl konkurs zrušen proto, že majetek zhotovitele byl zcela nepostačující.

7.3 Odstoupení musí být písemné a je účinné okamžikem doručení druhé straně. V takovém případě se smlouva ruší od počátku.

8 Závěrečná ujednání

8.1 Smlouva může být měněna pouze písemnými dodatky.

8.2 Smlouva je vyhotovena ve 2 stejnopisech, kdy každá ze stran obdrží 1 vyhotovení.

8.3 Zhotovitel bere na vědomí, že smlouva bude uveřejněna v registru smluv zřízeného podle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů. Zhotovitel prohlašuje, že tato smlouva neobsahuje údaje, které tvoří předmět jeho obchodního tajemství podle § 504 občanského zákoníku.

8.4 Smlouva nabývá platnosti dnem podpisu a účinnosti dnem zveřejnění v registru smluv. Zveřejnění zajistí objednatel.

8.5 Strany prohlašují, že si tuto smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují své podpisy.

8.6 Součástí této smlouvy jsou následující přílohy:

- Příloha č. 1- specifikace předmětu díla
- Příloha č. 2- bezpečnostní pravidla pro dodavatele

V Českých Budějovicích dne

V Praze dne 10. 3. 2021

Digitálně podepsal Ing. Tomáš Strýček
Datum: 2021.03.10 13:58:14 +01'00'

Za objednatele

Ing Petr Vobejda, vedoucí odboru informatiky

Za zhotovitele

Ing. Tomáš Strýček, člen představenstva

Příloha č. 1- specifikace předmětu díla:

a) Penetrační testy webových aplikací

Předmětem zakázky je realizace jednorázových penetračních testů webových aplikací provozovaných na adresách www.kraj-jihocesky.cz a priv.kraj-jihocesky.cz. Účelem testů je odhalovat případné zranitelnosti ve výše uvedených aplikacích a zajistit tak jejich bezpečnost v souladu s bezpečnostní strategií a dalšími dokumenty zadavatele.

Penetrační testy budou realizovány formou blackbox testů provedených z vnějšího prostředí. Testovacímu týmu budou před provedením testu předány přístupové údaje k aplikaci priv.kraj-jihocesky.cz svázané s platným neprivilegovaným uživatelským účtem. Žádné jiné informace týkající se aplikací, jejich vnitřní logiky nebo použitých technologií nebudou testovacímu týmu předem předány.

Testy budou realizované v předem dohodnutých termínech a časech z předem dohodnutých IP adres.

Testy budou realizovány v souladu s některou z obecně uznávaných metodik penetračního testování (OSSTMM, OWASP testing guide, apod.) a budou primárně zaměřeny na odhalování zranitelností dle platné verze OWASP Top 10. Využito při tom bude automatizovaných nástrojů i manuálního testování.

Součástí realizace penetračních testů budou i nápravná opatření. Uchazeč bude poskytovat součinnost při realizaci nápravných opatření. Faktickou realizaci bude provádět zadavatel či dodavatel příslušné oblasti. Dodavatel zajistí ověření realizace nápravného opatření.

Součástí testů nebude vyhledávání zranitelností v síťové ani jiné infrastruktuře, virtualizačních platformách ani dalším SW vybavení serverů provozujících uvedené aplikace, které s provozem daných aplikací přímo nesouvisí. Součástí testů nebude testování odolnosti aplikací vůči útokům typu DoS (DDoS), testování fyzické bezpečnosti serverů, ani testy užívající phishing nebo jiné sociotechnické postupy.

Výsledky testů budou vždy shrnuty v závěrečné zprávě. Ta bude obsahovat:

1) soupis všech kroků provedených v rámci testů a jejich výsledků,
2) detailní popis odhalených zranitelností včetně konkrétního postupu umožňujícího jejich využití a ohodnocení jejich nebezpečnosti a doporučení pro jejich odstranění.

Očekávané výstupy:

- Závěrečná zpráva
- Výsledky testů zaznamenané do standardizovaných šablon pro jednotlivé identifikované a testované systémy
- Sumarizace zjištění pro vedení organizace
- Detailní technická zpráva s popisem hlavních zranitelností spolu s odhadem úsilí na jejich odstranění
- CD/DVD dokumentující všechny akce vykonané v síťovém prostředí (kompletní záznam síťové komunikace)
- Výsledky ověření realizace nápravných opatření

Kvalifikační předpoklady:

- Vysoká kompetence v řízení informační bezpečnosti – organizace musí být držitelem certifikace ISO 27 001
- Vysoká kompetence k zvládání kybernetických bezpečnostních incidentů – organizace musí mít udělen minimálně stupeň Accredited organizací Trusted Introducer
- Odborná kompetence v oblasti penetračního testování – alespoň jeden z členů testovacího týmu, který bude penetrační testy realizovat, musí být držitelem alespoň jedné z certifikací CEH, GPEN, OPST nebo OSCP

b) Software pro správu chyb zabezpečení (Vulnerability management software)

Předmětem je dodání vulnerability management software za účelem plnění požadavků vyhlášky č. 82/2018 Sb. v souladu s bezpečnostní strategií a dalšími dokumenty zadavatele.

Řešení musí splňovat následující požadavky:

- On-premise deployment
- Řešení založené na jediné instanci (skener kombinovaný s managementem)
- Neomezený počet skenovaných IP adres
- Podpora IPv4, IPv6 i hybridních sítí
- Podpora autentizovaných (Windows a UNIX/Linux) bezagentských skenů a neautentizovaných skenů
- Podpora skenování webových aplikací
- Podpora skenování síťových zařízení
- Užívání pluginů pro testování jednotlivých zranitelností
- Konfigurovatelné reporty s podporou exportu do formátů PDF, HTML a CSV
- Podpora zasílání e-mailových notifikací s výsledky testů
- Poskytování doporučení pro odstranění nalezených zranitelností
- Podpora auditování konfigurace dle ISO, NIST, COBIT/ITIL a případně dalších standardů
- Ohodnocení závažnosti zranitelností dle CVSS
- Prioritizace zranitelností dle jejich využitelnosti s pomocí útočných frameworků (Metasploit, Core Impact, apod.)

Součástí dodávky řešení bude i zajištění jeho podpory od výrobce, včetně pravidelných updatů, na dobu 36 měsíců.

Výrobce řešení musí zdarma poskytovat on-demand e-learningová školení související s dodaným řešením.

Příloha č. 2- bezpečnostní pravidla pro dodavatele

Cílem těchto bezpečnostních pravidel je snižování kybernetických rizik a zvyšování účinnosti bezpečnostních opatření chránící Aktiva KÚ JK, ke kterým mají přístup Dodavatelé.

A.1 Základní odpovědnosti Dodavatele

Dodavatel řešení:

a) Je povinen dodržovat požadavky na bezpečnost informací v souladu s platnými zákony ČR.
b) Odpovídá za své řešení/dodávku/správu tak, aby respektovalo požadavky na bezpečnost KÚ JK, zabránilo bezpečnostním incidentům a stavu kybernetického nebezpečí.
c) Odpovídá za dodávku a implementaci řešení v požadované kvalitě i z pohledu bezpečnosti.
d) Ručí za trvalé zachování mlčenlivosti všech svých pracovníků i po ukončení smluvního vztahu s úřadem.

Dodavatel je povinen akceptovat použití prostředků bezpečnostního auditu, které mohou být útvarem IT využity k sledování aktivit v prostředí ICT/IS či aktivity procházejících přes toto prostředí.

A.2 Ochrana Aktiv

Dodavatel se před vlastním **přístupem** k datům a informacím KÚ JK musí zavázat mlčenlivostí. Tzn., že platí povinnost Dodavatele se zavázat a také povinnost pracovníků KÚ JK (prioritně ve smlouvě, prohlášením Dodavatele, formulářem, …) zavázat Dodavatele a nezpřístupnit data a informace Dodavateli dříve, než dojde k jeho závazku mlčenlivosti (tj. podpisu NDA – Non Disclosure Agreement či CA – Confidentiality Agreement).

A.3 Přístup k ICT/IS

Přihlášení Dodavatele do sítě KÚ JK musí podléhat kontrole přístupu na základě autorizace po předchozí autentizaci, včetně autentizace přes VPN v případě užití VPN klienta. Přihlašovací proces do VPN a do Windows domény poskytuje základní bezpečnostní funkce – nikdy se nezobrazuje vkládané heslo a heslo není nikde přenášeno a ukládáno v nezašifrované formě. Přístup ke službám ICT/IS je vždy zajištěn přes proces autentizace, autorizace a bezpečnostního auditu.

A.4 Ochrana před škodlivým softwarem

Dodavatel je povinen:

a) Centrálně organizovat zabezpečení svých koncových stanic v připojeních do své infrastruktury (např. řízení personálních firewallů, antivirového SW atd.) a to minimálně na úrovni standardů KÚ JK. Standardy KÚ JK se řídí zákonem č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a zejména vyhláškou č. 82/2018 Sb. Vyhláška o kybernetické bezpečnosti a dále bezpečnostními doporučeními NCKB pro administrátory v aktuálně platné verzi. Dodavatel by měl v přiměřené míře splňovat požadavky uvedených dokumentů.
b) Obsahem antivirové ochrany jsou taková opatření technického a administrativního charakteru, která vedou k detekci a následnému odstranění infiltrujícího software u všech prostředků provozovaných v rámci infrastruktury Dodavatele.
c) Dodavatel musí na své straně definovat zásady bezpečného užívání Internetu a s těmito zásadami seznámit veškerý personál užívající ICT prostředky infrastruktury Dodavatele.
d) Dodavatel musí na pracovních stanicích v jeho odpovědnosti zajistit bezpečné nakonfigurování prohlížečů obsahu Internetu (např. www prohlížeče).

A.5 Řízení bezpečnostních rizik

Dodavatel je povinen zajistit, že:

a) Hesla pracovníků Dodavatele nebudou zaznamenávána v otevřené podobě.
b) Vzájemnou spolupráci a komunikaci mezi Dodavatelem a KÚ JK při řešení ICT bezpečnostní rizik

A.6 Hlášení

Dodavatel je povinen KÚ JK hlásit:

a) nestandardní situace při práci v ICT/IS;
b) bezpečnostní události nad ICT/IS;
c) bezpečnostní slabiny v ICT/IS Objednatele.

A.7 Kontrola a audit Dodavatele

KÚ JK má obecné právo auditu prostředí Dodavatele za účelem ověření dodržování Bezpečnostních pravidel Objednatele či za účelem ověření zabezpečení dat a informací na ICT prostředcích Dodavatele, a to minimálně 1x za 12 měsíců.

A.8 Ošetření výjimek

Ve výjimečných případech je možno vyhlásit výjimku z dodržování bezpečnostních pravidel. Udělení výjimek ze stanovených pravidel se provádí na základě požadavku zaslaného manažerovi kybernetické bezpečnosti, který má právo výjimku udělit.

Schváleno: Bezpečnostní komise – Výbor pro řízení kybernetické bezpečnosti