Smlouva O Dílo

uzavřená dle § 2586 a násl. zákona č. 89/2012 Sb. (občanský zákoník)

mezi:

Objednatel (dále také „FNO“)			
Název:	Fakultní nemocnice Ostrava		
Sídlo:	17. listopadu 1790, 708 52 Ostrava-Poruba		
IČ:	00843989	**DIČ:**	CZ00843989
Bankovní spojení:	ČNB Ostrava, 66332761/0710		
Zřizovací listina MZ ČR ze dne 25.11.1990 č.j. OP-054-25.11.90			
Zastoupená:	Foltýn Petr, Bc.		
Kontaktní osoba:	Janáček Robert, Ing.	robert.janacek@fno.cz	

a

Zhotovitelem			
Název:	Next Generation Security Solutions s.r.o.		
Sídlo:	U Uranie 954/18, Praha-Holešovice, 17000		
IČ:	06291031	**DIČ:**	CZ06291031

I.

Základní ustanovení

Zhotovitel se zavazuje provést na svůj náklad a nebezpečí níže uvedený předmět plnění a Objednatel se zavazuje ho převzít a zaplatit sjednanou cenu.

II.

Předmět, doba a místo plnění

Předmětem plnění této smlouvy je:

Posouzení stavu kybernetické bezpečnosti, stanovení rozsahu a provedení hodnocení rizik dle specifikace uvedené v poptávce, která tvoří přílohu této smlouvy.

Datem ukončení plnění této smlouvy: 31.3.2019

Místem plnění této smlouvy je sídlo Objednatele.

III.

Cena a platební podmínky

1. Cena bez DPH je sjednána ve výši: 469 000,00 Kč.
2. K ceně bude DPH připočteno v zákonné výši.
3. Cena je splatná na základě Zhotovitelem vystavené faktury, která musí obsahovat náležitosti daňového dokladu dle zákona č. 235/2004 Sb., o dani z přidané hodnoty.
4. Faktura je splatná do 30 dnů od jejího doručení.
5. Faktura, včetně všech souvisejících dokumentů (kopie Objednatelem potvrzeného akceptačního protokolu nebo dodacího listu …), bude zaslána na emailovou adresu: **efakturace1@fno.cz** a to tak, že všechny přílohy jsou ve formátu pdf a faktura je jako první v pořadí ze všech příloh.

6. V případě, že faktura bude obsahovat nesprávné nebo neúplné náležitosti, je Objednatel oprávněn ji vrátit Zhotoviteli. Ten ji podle charakteru nedostatků buď opraví, nebo vystaví novou. U této nové nebo opravené faktury běží nová lhůta splatnosti.

IV.
Sankční ustanovení

1. Objednatel se zavazuje při prodlení se zaplacením faktury zaplatit Zhotoviteli úrok z prodlení ve výši stanovené předpisy občanského práva.
2. Zhotovitel se zavazuje při nedodržení smluveného termínu plnění zaplatit Objednateli smluvní pokutu ve výši 0,05% z celkové ceny neakceptovaného nebo neodebraného plnění za každý den prodlení.
3. Dohodnutou smluvní pokutu zaplatí Zhotovitel vedle škody, která vznikne Objednateli porušením povinností, na něž se vztahuje smluvní pokuta.

V.
Záruční podmínky

1. Objednatel není povinen předmět plnění převzít, pokud vady samy o sobě nebo ve spojení s jinými budou bránit jeho řádnému užívání.
2. Zhotovitel ručí za kvalitu předmětu plnění dle této smlouvy po dobu 24 měsíců od data předání předmětu plnění bez vad objednateli.
3. Případné reklamace zajistí Zhotovitel odstranit na vlastní náklady do 30 dnů od jejich uplatnění.

VI.
Ostatní ujednání

VII.
Závěrečná ustanovení

1. Veškeré změny a doplňky této smlouvy je možné činit písemně, a to formou číslovaných dodatků.
2. Tato smlouva je sepsána ve dvou vyhotoveních, každá strana obdrží jedno.
3. Veškeré právní vztahy touto smlouvou neupravené se řídí ustanoveními občanského zákoníku a ostatních obecně závazných právních předpisů.
4. Tato smlouva nabývá platnosti podpisem obou smluvních stran a účinnosti nejdříve dnem zveřejnění v registru smluv.
5. V souladu se zákonem č. 340/2015 Sb., o registru smluv v platném znění, Zhotovitel souhlasí s uveřejněním plného znění smlouvy, včetně všech jejich změn a dodatků.

V Ostravě, dne: 4.1.2019

Za Objednatele
FAKULTNÍ NEMOCNICE OSTRAVA
17. listopadu 1790/5, 708 52 Ostrava-Poruba
Tel.: +420 597 371 111, Fax: +420 596 917 340

V Ostravě, dne: 11.1.2019

Za Zhotovitele
NGSS Next Generation Security Solutions
U Uranie 954/18, 17000 Praha 7

Posouzení stavu kybernetické bezpečnosti, stanovení rozsahu a provedení hodnocení rizik

Obsahem poptávky je posouzení shody procesů a činností prováděných Fakultní nemocnicí Ostrava (dále jen FNO) s požadavky na bezpečnost definovaných v obecné normě a vyhláškou č. 82/2018 Sb., a návrh postupu implementace opatření k eliminaci zjištěných nedostatků.

Dále v návaznosti na posouzení shody procesů stanovení rozsahu připravovaného systému řízení bezpečnosti informací a provedení hodnocení rizik, kterým jsou informace ve FNO vystaveny.

Doba plnění se předpokládá po dobu 3 měsíců od počátku účinnosti smlouvy. V rámci posouzení stavu požadujeme zpracovat:

- Posouzení stavu bezpečnosti informací ve FNO
- Stanovení rozsahu a cílů systému řízení bezpečnosti informací
- Hodnocení rizik bezpečnosti informací
- Návrh plánu zvládání rizik

Provedení posouzení stavu bezpečnosti informací ve FNO

V rámci provedení posouzení požadujeme realizovat Srovnávací analýzu stavu bezpečnosti k posouzení úrovně stavu ochrany informací v prostředí FNO. Jako kritéria srovnávací analýzy požadujeme použít požadavky vyhlášky č. 82/2018 Sb. Srovnávací analýza v oblasti zajištění kybernetické bezpečnosti prověří stav v oblastech organizačních a technických opatření, bezpečnostní politiky a bezpečnostní dokumentace v následujícím rozsahu:

- Organizační opatření:
  - Systém řízení bezpečnosti informací
  - Řízení rizik
  - Bezpečnostní politika
  - Organizační bezpečnost
  - Stanovení bezpečnostních požadavků pro dodavatele
  - Řízení aktiv
  - Bezpečnost lidských zdrojů
  - Řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému
  - Řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému
  - Akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systém
  - Zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních Incidentů
  - Řízení kontinuity činností
  - Kontrola a audit
- Technická opatření:
  - Nástroj pro ochranu integrity komunikačních sítí
  - Nástroj pro ověřování identity uživatelů
  - Nástroj pro řízení přístupových oprávnění
  - Nástroj pro ochranu před škodlivým kódem

- Nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů
- Nástroj pro detekci kybernetických bezpečnostních událostí
- Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- Aplikační bezpečnost
- Kryptografické prostředky
- Nástroj pro zajišťování úrovně dostupnosti informací
- Bezpečnost průmyslových a řídicích systémů

- Bezpečnostní politika a bezpečnostní dokumentace

Jako výstup požadujeme zpracovat dokument „Zpráva ze srovnávací analýzy stavu bezpečnosti informací ve FNO". Dokument musí tvořit přehledová zpráva o stavu bezpečnosti v porovnání k relevantním požadavkům vyhlášky č. 82/2018 Sb. Zpráva musí, mimo zhodnocení stavu, obsahovat návrh úprav bezpečnostních procesů ve FNO a návrh opatření k odstranění zjištěných neshod.

Stanovení rozsahu a cílů systému řízení bezpečnosti informací

Stanovení rozsahu požadujeme provést tak, aby byl vymezen rozsah pokrývaných aktiv, pokrývané organizační části a určeny hranice a aplikovatelnost systému řízení bezpečnosti informací. Cíle požadujeme stanovit ve formě dlouhodobých úkolů s návrhem odpovědností, termínů a hodnotících kritérií k zavedení systému řízení bezpečnosti informací.

Jako výstup požadujeme zpracovat dokument „Rozsah a cíle systému řízení bezpečnosti informací FNO". Dokument musí obsahovat popis pro jaké informace a informační systémy je ISMS zaváděno, vymezení základních skupin aktiv, pokrývaných organizačních celků a návrh organizace bezpečnosti informací. Dokument dále uvede hranice a závislosti navrhovaného systému řízení bezpečnosti informací.

Provedení hodnocení rizik bezpečnosti informací

Hodnocení rizik bezpečnosti informací požadujeme provést tak, aby byla určena rizika informací (a návazně informačních systémů, osob a prostředí) zpracovávaných v rámci FNO. Požadujeme posouzení rizik hrozících z hlediska použitého hardware, software ale i lidského faktoru s ohledem na neúmyslné chyby či přímo krádeže dat.

V rámci hodnocení rizik požadujeme provést činnosti vyžadované vyhláškou č. 82/2018 Sb., a to zejména:

- Určení a schválení metodiky pro identifikaci a hodnocení aktiv
- Určení a schválení metodiky pro identifikaci a hodnocení rizik
- Určení respondent pro provedení identifikace a ohodnocení aktiv a rizik a naplánování rozhovorů
- Provedení identifikace a zaevidování aktiv a určení odpovědných garantů
- Provedení ohodnocení aktiv z hlediska zajištění jejich dostupnosti, důvěrnosti a integrity
- Provedení identifikace hrozeb, zranitelností a dopadů
- Provedení hodnocení rizik
- Provedení určení, od jaké úrovně budou rizika považována za závažná a budou činěna opatření pro jejich redukci

- Provedení volby způsobu redukce rizika, kdy pro každé riziko s úrovní vyšší, než stanovená hranice musí být rozhodnuto o způsobu jeho zvládání (modifikace rizika, podstoupení rizika, vyhnutí se riziku, sdílení rizika a volba pokrytí rizik opatřeními)
- Identifikace pokrytí opatřeními, kdy opatření jsou přiřazena těm rizikům, jejichž hodnota je vyšší nebo rovna stanovené hranici. Opatření požadujeme použít z vyhlášky č. 82/2018 Sb., a přílohy A normy ČSN ISO/IEC 27001.
- Projednání a vydání souhlasu se zbytkovými riziky
- Zpracování a projednání zprávy o hodnocení rizik
- Zpracování prohlášení o aplikovatelnosti, které uvede jaká (a proč) opatření jsou vybrána k pokrytí zjištěných rizik

Jako výstupy požadujeme zpracovat následující dokumenty:

- „Metodika hodnocení aktiv a rizik" – dokument musí popisovat způsob provedení ohodnocení spolu s odpovědnostmi. Jeho cílem je upřesnit hodnoty a metriky, které budou používány při hodnocení aktiv a rizik.

- „Zpráva z hodnocení rizik" – Zpráva musí uvést identifikovaná aktiva, jejich hodnotu spolu se zjištěnými riziky.

- „Prohlášení o aplikovatelnosti" – dokument, který musí obsahovat přehled bezpečnostních opatření požadovaných vyhláškou, která nebyla aplikována, včetně odůvodnění a opatření, která byla aplikována včetně způsobu plnění.

Návrh plánu zvládání rizik

V návaznosti na Srovnávací analýzu a výsledky hodnocení rizik požadujeme zpracovat Plán zvládání rizik.

Plán musí dle požadavků vyhlášky č. 82/2018 Sb. obsahovat:

- cíle a přínosy bezpečnostních opatření pro zvládání jednotlivých rizik,
- určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik,
- potřebné finanční, technické, lidské a informační zdroje,
- termín jejich zavedení,
- popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a
- způsob realizace bezpečnostních opatření.

Plán požadujeme zpracovat formou přehledové tabulky s následujícím obsahem:

- Opatření – bezpečnostní opatření, vybrané z vyhlášky č. 82/2018 Sb., nebo z jiného zdroje
- Způsob realizace opatření – rozpad opatření do dílčích kroků
- Cíl/přínos – zdůvodnění zavedení jednoho či skupiny bezpečnostních opatření
- Vazba mezi opatřením a rizikem – uvedení, jaké riziko opatření pokrývá
- Odpovědná osoba – uvedení osoby či osob odpovědných za zavedení a provozování vybraných opatření
- Zdroje – uvedení zdrojů finančních, technických, lidských a informačních, které jsou vyčleněny pro zavedení a provozování vybraného opatření nebo skupiny opatření
- Termín – uvedení návrhu termínu, v němž budou vybraná opatření zavedena, případně více termínů, pokud budou opatření zaváděna postupně
- Hodnocení – způsoby hodnocení úspěšnosti zavedení jednotlivých bezpečnostních opatření

Jako výstup požadujeme zpracovat dokument Plán zvládání rizik" - dokument stanovující plán přijetí potřebných opatření k pokrytí zjištěných rizik a odstranění neshod zjištěných v rámci srovnávací analýzy

Požadavky na kvalifikaci účastníků

Dodavatel je povinen prokázat kvalifikaci v následujícím rozsahu:

1. předložení seznamu významných služeb realizovaných dodavatelem v posledních třech letech s uvedením jejich rozsahu a doby poskytnutí. Významné služby musí zahrnovat minimálně jednu významnou dodávku v oblasti rozdílové analýzy mezi současným stavem a požadavky v oblasti informační bezpečnosti a kontinuity provozu, přičemž jako významná je stanovena dodávka ve výši min. 300 000 Kč bez DPH a jednu významnou dodávku zahrnující provedení analýzy rizik ve výši min. 150 000 Kč bez DPH.

2. předložení seznamu realizačního týmu.

Dodavatel prokáže splnění tohoto kvalifikačního předpokladu předložením seznamu specialistů, jež se budou podílet na plnění této veřejné zakázky, bez ohledu na to, zda se jedná o zaměstnance dodavatele nebo osoby v jiném vztahu k dodavateli, z něhož bude vyplývat, že dodavatel má k dispozici tým odborníků sestávající z:

- Vedoucí týmu - mezinárodně uznávaný certifikát: ISMS Auditor (Lead Auditor) nebo CISA (Certified Information Systems Auditor®) nebo ekvivalent daného certifikátu od jiné akreditované autority
- Konzultant bezpečnosti IT - odborné zkušenosti s architekturou v oblasti serverů, storage, virtualizace, zálohování a bezpečnosti. Certifikace ITIL.
- Konzultant bezpečnosti - odborné zkušeností v oblasti certifikace IT/ICT např. CISSP, ISSMP, ISO 27001, ISO 20000