

Otevřená výzva k podání nabídek

Veřejná zakázka malého rozsahu

(nejedná se o zadávací řízení podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek)

Název zakázky	Školení kyberbezpečnosti
Předmět zakázky	Zakázka na služby
Typ zakázky	Zakázka malého rozsahu (nejedná se o zadávací řízení podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek). Jedná se o veřejnou zakázku dle §27, písm. a) a dle §31 zákona o zadávání veřejných zakázek.
Datum vyhlášení	22. 10. 2025
Zadavatel	Astronomický ústav AV ČR, v. v. i. Fričova 298, 251 65 Ondřejov IČO 67985815 DIČ CZ67985815 ISDS 49qnh3h Zadavatel je veřejná výzkumná instituce – právnická osoba, jejímž zřizovatelem je Akademie věd České republiky, organizační složka státu.
Kontaktní osoba zadavatele ve věcech zadávací dokumentace	Email: [REDACTED] Tel: [REDACTED]
Lhůta pro podávání nabídek a zadávací lhůta	Nabídky je možné podávat do 2.11. 2025 23:59 hodin Nabídky doručené po tomto termínu nebudou otevřeny a hodnoceny. Zadavatel stanovuje zadávací lhůtu, tj. dobu, po kterou jsou účastníci zadávacího řízení svými nabídkami vázáni, na 30 dnů. Tato lhůta začíná běžet okamžikem skončení lhůty pro podání nabídek a končí 30. den nebo v den, kdy zadavatel uzavře Smlouvu s vybraným dodavatelem. Výsledky zadávacího řízení budou oznámeny písemně všem účastníkům, kteří podali nabídku, ve lhůtě 5 pracovních dnů ode dne rozhodnutí o výsledku zadávacího řízení zadavatelem na email uvedený v nabídce. Po ukončení zadávacího řízení uzavře zadavatel s vybraným účastníkem zadávacího řízení smlouvu upravující realizaci služby. Zadavatel si vyhrazuje právo jednat po vybrání nejvhodnější nabídky o konečném znění Smlouvy v těch bodech, které neznamenaají změnu zadávacích podmínek. Zadavatel si vyhrazuje právo neuzavřít Smlouvu s žádným účastníkem.
Způsob podání nabídky	Nabídky je možné podat v elektronické podobě prostřednictvím portálu zadavatele https://www.vhodne-uverejneni.cz/profil/67985815

	e-mailem na adresu [redacted] nebo datovou schránkou 49qnh3h.
Předpokládaná hodnota zakázky	Celková předpokládaná hodnota veřejné zakázky roky je 500.000 Kč bez DPH. Předpokládaná hodnota zakázky v sobě zahrnuje veškeré náklady dodavatele na realizaci zakázky včetně dopravy a dalších nezbytných výdajů.
Lhůta a místo dodání	<u>Lhůta dodání:</u> Předpokládaná doba zahájení plnění veřejné zakázky je: 30 dní od účinnosti smlouvy. <u>Místo plnění:</u> Astronomický ústav AV ČR, v. v. i., Fričova 298 251 65 Ondřejov

Popis předmětu zakázky	Zajištění školení kybernetické bezpečnosti pro administrativní zaměstnance
Věcné vymezení předmětu	Zajištění školení kybernetické bezpečnosti pro administrativní zaměstnance včetně zajištění ubytování, stravování a prostor a techniky pro školení. Obsah školení: Školení bude probíhat 1 x ročně v rozsahu 2 dny (2x min. 6 hodin) po dobu 5 let (11/2025-06/2029). Přesný rozsah školení bude pro každé školení jiný a bude upřesněn vždy mezi objednatelem a dodavatelem na základě objednávky. Tematicky musí školení vždy vycházet z osnovy, kterou uchazeči přikládají k nabídce, pokrývat přehled běžných kybernetických hrozeb, které jsou relevantní při výkonu administrativní agendy středního podniku (úseky účetnictví, personalistiky, správa dokumentů, obsluha datové schránky, elektronická pošta), a metody jejich minimalizace a prevence. Kromě teoretické části musí být část školení věnována specifickým ukázkám a praktickým příkladům běžně používaných vektorů kybernetických útoků. Konkrétní témata jsou předmětem nabídky a jejího hodnocení. Forma školení bude ústní prezentace lektora doplněná obrazem, praktické ukázky, scénáře nebo ukázky k zamyšlení/procvičení. Ubytování a stravování: Uchazeč nabídne pro každé školení zajištění ubytování a stravování po dobu školení v hotelovém zařízení standardu *** nebo vyšším s ubytováním v jednolůžkových nebo dvoulůžkových pokojích vybavených vlastním sociálním zařízením a minibarem a dále stravování ve formě oběd+večeře a snídaně+oběd (snídaně formou bufetu, oběd a večeře buď servírované nebo formou bufetu vždy o min. dvou chodech). Ubytování musí dále splňovat: - kapacita ubytovacího zařízení: min. 20 osob - datové připojení s minimální rychlostí 50 Mb/s - dojezdová vzdálenost z Ondřejova do hotelu je maximálně 90 minut - hodnocení na serveru booking.cz lepší než 8,5 - konferenční místnost pro 20 osob Konkrétní výběr termínu školení a výběr ubytovacího zařízení se provede před každým školením v součinnosti s objednatelem s přihlédnutím k jeho provozním podmínkám. Výběr musí odpovídat rámcové nabídce na zajištění ubytování. Školení bude realizováno v období duben-červen, v roce 2025 pak v období listopad-prosinec. Předpokládá se cca 15 účastníků.

Záruka																								
Hodnotící kritéria	Způsob hodnocení nabídek Základním kritériem pro hodnocení veřejné zakázky je ekonomická výhodnost nabídky. Ekonomická výhodnost nabídek bude hodnocena na základě nejvýhodnějšího poměru nabídkové ceny a kvality. Zadavatel stanovil následující dílčí kritéria hodnocení a jejich váhu: <table><tr><th>Označení kritéria</th><th>Název kritéria</th><th>Váha</th></tr><tr><td>K1</td><td>Nabídková cena (bez DPH)</td><td>30 %</td></tr><tr><td>K2</td><td>Obsah školení</td><td>30 %</td></tr><tr><td>K3</td><td>Lektor / pedagog</td><td>10 %</td></tr><tr><td>K4</td><td>Ubytování – počet hvězdiček</td><td>20 %</td></tr></table> Hodnotící kritérium K1 – Nabídková cena V rámci tohoto dílčího kritéria Zadavatel stanoví tato subkritéria: <table><tr><th>Označení subkritéria</th><th>Název subkritéria</th></tr><tr><td>S1</td><td>Cena za provedení 1 školení v uvedeném rozsahu včetně všech nákladů na dopravu, stravování a ubytování školitele, zajištění technických prostředků a školících prostor v Kč bez DPH</td></tr><tr><td>S2</td><td>Cena za ubytování účastníků školení za osobu a den v Kč bez DPH (max. přípustná cena 2050 Kč/osoba/noc)</td></tr><tr><td>S3</td><td>Cena za stravování účastníků školení za osobu a den v Kč bez DPH (max. přípustná cena 780 Kč/osoba/den)</td></tr></table> Uchazeč uvede nabídkovou cenu u každého subkritéria S1, S2, S3 samostatně, celková cena vzorového dvoudenního školení pak bude vypočtena jako součet školení, 1x ubytování, 2x strava. $K1 = S1 + S2 + S3 \times 2$ Hodnocení bude provedeno dle následujícího vzorce: Nejnižší nabídková cena K1 / hodnocená cena K1 $\times$ 30% Hodnotící kritérium K2 – Obsah školení V rámci tohoto kritéria bude Zadavatel hodnotit především tematický obsah, kvalitu, relevanci a praktický přínos obsahu školení pro účastníky vzorového školení kyberbezpečnosti v rozsahu 12 hodin. Za tím účelem uchazeč předloží rámcový obsah školení, tj. popis okruhů, kterých se školení bude týkat, z něhož bude zřejmá tematická náplň a který bude naplňovat shora uvedené rámcové předpoklady. Součástí hodnocení je povinný ukázkový záznam školení v délce alespoň 30 minut. Bodová stupnice (1–5 bodů): 5 bodů – obsah je komplexní, prakticky využitelný, pokrývá všechny požadavky Zadavatele s vysokou přidanou hodnotou. 4 body – obsah je velmi kvalitní, splňuje všechny požadavky, avšak méně inovativní nebo méně prakticky zaměřený.	Označení kritéria	Název kritéria	Váha	K1	Nabídková cena (bez DPH)	30 %	K2	Obsah školení	30 %	K3	Lektor / pedagog	10 %	K4	Ubytování – počet hvězdiček	20 %	Označení subkritéria	Název subkritéria	S1	Cena za provedení 1 školení v uvedeném rozsahu včetně všech nákladů na dopravu, stravování a ubytování školitele, zajištění technických prostředků a školících prostor v Kč bez DPH	S2	Cena za ubytování účastníků školení za osobu a den v Kč bez DPH (max. přípustná cena 2050 Kč/osoba/noc)	S3	Cena za stravování účastníků školení za osobu a den v Kč bez DPH (max. přípustná cena 780 Kč/osoba/den)
Označení kritéria	Název kritéria	Váha																						
K1	Nabídková cena (bez DPH)	30 %																						
K2	Obsah školení	30 %																						
K3	Lektor / pedagog	10 %																						
K4	Ubytování – počet hvězdiček	20 %																						
Označení subkritéria	Název subkritéria																							
S1	Cena za provedení 1 školení v uvedeném rozsahu včetně všech nákladů na dopravu, stravování a ubytování školitele, zajištění technických prostředků a školících prostor v Kč bez DPH																							
S2	Cena za ubytování účastníků školení za osobu a den v Kč bez DPH (max. přípustná cena 2050 Kč/osoba/noc)																							
S3	Cena za stravování účastníků školení za osobu a den v Kč bez DPH (max. přípustná cena 780 Kč/osoba/den)																							

- **3 body** – obsah je dobrý, pokrývá většinu požadavků, ale chybí vyšší přidaná hodnota nebo aktuální témata.
- **2 body** – obsah splňuje jen částečně, chybí zásadní oblasti nebo praktické využití.
- **1 bod** – obsah nevhodný, nesplňuje základní požadavky.

Hodnotící kritérium K3 – Lektor / pedagog

V rámci tohoto kritéria bude Zadavatel hodnotit odbornost, zkušenosti, interaktivitu a schopnost lektora srozumitelně vysvětlit probíranou látku podle ukázkového videa.

Bodová stupnice (1–5 bodů):

- **5 bodů** – velmi zkušený odborník s více než 5letou praxí v oboru kybernetické bezpečnosti a více než 3letou lektorskou praxí; interaktivní, výborné reference.
- **4 body** – zkušený lektor, splňuje všechny požadavky, interaktivní přístup, dobré reference.
- **3 body** – lektor se základní zkušeností, méně interaktivní, splňuje minimální požadavky.
- **2 body** – lektor s omezenou praxí, projev málo interaktivní, nižší přínos.
- **1 bod** – lektor bez doložené praxe nebo s nevyhovující kvalifikací.

Hodnotící kritérium K4 – Ubytování (počet hvězdiček)

V rámci tohoto kritéria bude hodnocen oficiální počet hvězdiček ubytovacího zařízení.

Bodová stupnice (1–5 bodů):

- **5 bodů** – 5 hvězdiček
- **4 body** – 4 hvězdičky
- **3 body** – 3 hvězdičky
- **2 body** – 2 hvězdičky
- **1 bod** – 1 hvězdička

Výsledné hodnocení nabídek

Každé nabídce bude přidělen bodový zisk v jednotlivých dílčích kritériích. Výsledné hodnocení bude stanoveno jako vážený součet bodů dle stanovených vah.

Za ekonomicky nejvýhodnější bude považována nabídka s nejvyšším celkovým bodovým hodnocením.

V případě rovnosti výsledného bodového hodnocení bude o pořadí rozhodovat vyšší počet bodů v kritériu K2 – Obsah školení; pokud by i tento počet bodů byl shodný, rozhodne hodnocení kritéria K1 – nabídková cena; pokud by i tento počet bodů byl shodný, rozhodne hodnocení kritéria K3 – pedagog; pokud by i tento počet bodů byl shodný, rozhodne hodnocení kritéria K4 – ubytování; pokud by i tento počet bodů byl shodný, rozhodne los.

Požadavky na prokázání splnění základní a profesní kvalifikace účastníka zadávacího řízení	Účastník zadávacího řízení, aby prokázal splnění kvalifikace potřebné k realizaci této veřejné zakázky malého rozsahu, musí doložit: podepsané čestné prohlášení, které tvoří přílohu této výzvy k podání nabídek. Požadavky na základní způsobilost dodavatele jsou uvedeny v § 74 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek. Profesní způsobilost je uvedena v § 77 odst. 1 a 2 písm. a) zákona č. 134/2016 Sb., o zadávání veřejných zakázek. Doklady, které prokazují profesní způsobilost: a) výpis z obchodního rejstříku nebo jiné obdobné evidence, b) doklad, že je oprávněn podnikat v rozsahu odpovídajícímu předmětu veřejné zakázky, pokud jiné právní předpisy takové oprávnění vyžadují. Zadavatel si může v průběhu zadávacího řízení vyžádat předložení originálů nebo úředně ověřených kopií dokladů, které prokazují základní a profesní způsobilost. Technická kvalifikace V souladu s ustanovením § 79 odst. 2 písm. b) Zákona požaduje zadavatel uvést a předložit v rámci čestného prohlášení o splnění kvalifikace seznam školení kybernetické bezpečnosti poskytnutých dodavatelem za poslední 3 roky před zahájením zadávacího řízení včetně uvedení ceny a doby jejich poskytnutí a identifikace objednatel. (příloha č. 2). V souladu s § 73 odst. 6 Zákona stanovuje toto: Zadavatel požaduje, aby součástí seznamu školení byly alespoň 3 realizovaná školení, každá v minimální hodnotě 15 000 Kč bez DPH. Zadavatel v souladu s § 79 odst. 2 písm. d) zákona požaduje, aby dodavatel předložil osvědčení o vzdělání a odborné kvalifikaci lektorů vztahující se k požadované službě, přičemž lektori podílející se na poskytování předmětu plnění musí disponovat minimálně 3letou praxí v oboru kybernetické bezpečnosti a minimálně 2letou praxí v lektorování uvedených specializovaných témat, stanovených ve Věcném vymezení předmětu plnění. Dodavatel předloží: a) kopie dokladů o vzdělání a odborné kvalifikaci lektorů, b) čestné prohlášení o požadované délce praxe c) ukázkovou nahrávku školení v délce alespoň 30 minut. Účastník zadávacího řízení, který nesplní doložení kvalifikace v požadovaném rozsahu, bude zadavatelem vyloučen z účasti v zadávacím řízení.
Požadavek na uvedení kontaktní osoby účastníka zadávacího řízení	Účastník zadávacího řízení je povinen ve své nabídce uvést kontaktní osobu ve věci zakázky, její telefon a e-mailovou adresu.

Požadavek na písemnou formu nabídky	Při podání nabídek musí účastník zadávacího řízení vyplnit všechny přílohy této Výzvy. Účastník zadávacího řízení může podat pouze jednu nabídku na tuto veřejnou zakázku. Předložená nabídka musí být vypracována výhradně v českém jazyce včetně všech příloh a dokumentů. Pokud některý z požadovaných dokumentů nebo jejich kopii má účastník zadávacího řízení k dispozici pouze v jazyce jiném než českém, předloží v nabídce úřední překlad tohoto dokumentu do českého jazyka. Povinnost připojit k dokladům úředně ověřený překlad do českého jazyka se nevztahuje na doklady ve slovenském a anglickém jazyce. Účastník zadávacího řízení v nabídce uvede své identifikační údaje - obchodní firma nebo název, sídlo dle výpisu z obchodního rejstříku, adresu pro doručování pošty, IČ, DIČ, jméno osoby oprávněné jednat jménem či za účastníka zadávacího řízení, telefonické spojení, příp. e-mailovou a webovou adresu. Zadavatel nepřipouští variantní řešení nabídky.
Obchodní a platební podmínky	Faktura je splatná do 14 dnů od data jejího doručení.
Povinnost uchovávat doklady a umožnit kontrolu	Účastník zadávacího řízení se zavazuje, že umožní provedení kontroly veškerých dokladů souvisejících s plněním zakázky všem subjektům oprávněným k výkonu kontroly projektu, a to po dobu danou právními předpisy ČR k jejich archivaci (zákon č. 563/1991 Sb., o účetnictví, a zákon č. 235/2004 Sb., o dani z přidané hodnoty). Dodavatel je osobou povinnou spolupůsobit při výkonu finanční kontroly dle § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, v platném znění. Dodavatel se zároveň zavazuje, že umožní provedení stejné kontroly i u případného subdodavatele.
Další podmínky pro plnění zakázky:	Zadavatel je oprávněn před uzavřením smlouvy kdykoli zrušit zadávací řízení zejména za předpokladu, že: • nastanou skutečnosti, za kterých nelze požadovat, aby v řízení pokračoval; • vybraný dodavatel zadávacího řízení, popř. účastník zadávacího řízení druhý v pořadí, odmítl uzavřít smlouvu nebo neposkytl zadavateli k jejímu uzavření dostatečnou součinnost. O zrušení zadávacího řízení je zadavatel povinen písemně informovat do 5 pracovních dnů od přijetí rozhodnutí o zrušení všechny zadavateli známé účastníky zadávacího řízení a zájemce, kteří podali nabídku v řádném termínu, s uvedením důvodu. Zadavatel neposkytuje náhradu nákladů vynaložených účastníku zadávacího řízení na účast v zadávacím řízení na danou veřejnou zakázku. Přestože se v některých ustanoveních zadavatel odvolává na zákon č. 134/2016 Sb., o zadávání veřejných zakázek, nejedná se o veřejnou zakázku vedenou v režimu tohoto zákona.
Podmínky poskytnutí zadávací dokumentace	Účastník je oprávněn požadovat po zadavateli dodatečné informace k zadávacím podmínkám. Žádost musí být písemná a doručena prostřednictvím elektronického portálu: https://www.vhodne-uverejneni.cz/profil/67985815 datovou schránkou nebo na e-mail [redacted] Dodatečné informace zadavatel poskytne všem účastníkům, a to na dotazy

	vznesené nejpozději 4 pracovní dny před koncem lhůty pro podání nabídek. Nedílnou součástí této výzvy jsou přílohy: Příloha č. 1 – Vzor krycího listu nabídky Příloha č. 2 - Vzorová čestná prohlášení
Další podmínky	Zadavatel si vyhrazuje právo zadávací řízení před jeho ukončením zrušit.

V Ondřejově



Michal Bursa
Astronomický ústav AV ČR, v. v. i.

NABÍDKA VE VĚCI:

**„ŠKOLENÍ
KYBERBEZPEČNOSTI“**

ASTRONOMICKÝ ÚSTAV AV ČR, v.v.i.

2. listopadu 2025

Číslo nabídky NAB-25-226

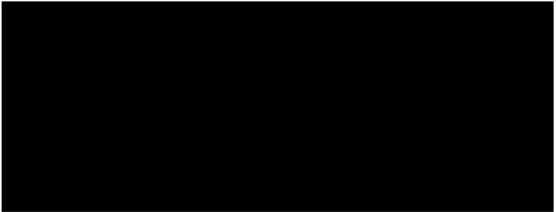
1. Identifikační údaje dodavatele

Next Generation Security Solutions s.r.o.	
Sídlo společnosti:	U Uranie 954/18, Holešovice, 170 00 Praha 7
IČ:	06291031
DIČ:	CZ06291031
Spisová značka	C 279627 vedená u Městského soudu v Praze
Právní forma:	Společnost s ručením omezeným
Statutární orgán:	Mgr. Ondřej Dedek, jednatel
Webové stránky:	www.ngss.cz
ID datové schránky:	se7ns8g
Telefon:	+420 237 836 950
Bankovní spojení:	
Plátce DPH:	ANO
Nespolehlivý plátce:	NE
Malý či střední podnik:	ANO
Kontaktní osoba:	
Vázanost nabídkou	po dobu zadávací lhůty, 30 dnů od data lhůty pro podání nabídek

2. Obsah

1.	Identifikační údaje dodavatele.....	2
2.	Obsah	3
3.	Krycí list nabídky.....	4
4.	Čestné prohlášení.....	5
5.	Seznam lektorů.....	7
6.	Obsah školení.....	8
6.1.	Ukázka formy školení.....	9
6.2.	Čestné prohlášení o požadované délce praxe	10
7.	NGSS tým.....	11
8.	Naše zkušenosti	15
9.	Informace o společnosti	17

3. Krycí list nabídky

Účastník zadávacího řízení (obchodní firma nebo název)	Next Generation Security Solutions s.r.o.
Sídlo (v případě fyzické osoby místo podnikání) (celá adresa včetně PSČ)	U Uranie 954/18, Holešovice, 170 00 Praha 7
Právní forma	Společnost s ručením omezeným
Identifikační číslo	06291031
Daňové identifikační číslo	CZ0629131
Zástupce / zástupci účastníka zadávacího řízení (vč. telefonu a e-mailové adresy)	Mgr. Ondřej Dedek, jednatel odedek@ngss.cz 774 416 033
Cena za provedení školení v uvedeném rozsahu v Kč bez DPH	215.000, - Kč bez DPH v definovaném rozsahu na 5 let
Cena za ubytování účastníků školení za osobu a den v Kč bez DPH	2.000, - Kč bez DPH / osoba / noc
Cena za stravování účastníků školení v Kč bez DPH	750,- Kč bez DPH / osoba / den
Délka praxe školitele v oboru kyberbezpečnosti (roky)	7 let
Délka lektorské praxe školitele (roky)	4 roky
Počet hvězdiček vzorového ubytování	4****
Podpis oprávněné osoby <i>Mgr. Ondřej Dedek, jednatel</i>	

4. Čestné prohlášení

o splnění kvalifikačních předpokladů

Prohlašuji, že jako dodavatel předmětné veřejné zakázky:

„Školení kyberbezpečnosti“

splňuji tyto kvalifikační předpoklady, neboť jsem dodavatelem, který:

- a) nebyl v zemi svého sídla v posledních 5 letech před zahájením zadávacího řízení pravomocně odsouzen pro trestný čin uvedený v příloze č. 3 ZVZ nebo obdobný trestný čin podle právního řádu země sídla dodavatele; k zahlázeným odsouzením se nepřihlíží. Je-li dodavatelem právnická osoba, musí tuto podmínku splňovat tato právnická osoba a zároveň každý člen statutárního orgánu. Je-li členem statutárního orgánu dodavatele právnická osoba, musí tuto podmínku splňovat tato právnická osoba, každý člen statutárního orgánu této právnické osoby a osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele. Účastní-li se zadávacího řízení pobočka závodu zahraniční právnické osoby, musí tuto podmínku splňovat tato právnická osoba a vedoucí pobočky závodu. Účastní-li se zadávacího řízení pobočka závodu české právnické osoby, musí tuto podmínku splňovat tato právnická osoba, každý člen statutárního orgánu této právnické osoby, osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele a vedoucí pobočky závodu.
- b) nemá v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek,
- c) nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění,
- d) nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti,
- e) není v likvidaci, nebylo proti němu vydáno rozhodnutí o úpadku, nebyla proti němu nařízena nucená správa podle jiného právního předpisu nebo v obdobné situaci podle právního řádu země sídla dodavatele.
- f) (ani jeho skutečný majitel) není uveden mezi osobami, na něž je uvalena sankce uplatnitelná podle zákona č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů.¹
- g) v souladu s nařízením Rady (EU) č. 833/2014 nemá ve své vlastnické struktuře právnickou osobu, subjekt nebo orgán usazený v Rusku, který je z více než 50 % ve veřejném vlastnictví nebo pod veřejnou kontrolou,
- h) splňuje profesní způsobilost, kterou zadavatel požadoval v zadávací dokumentaci.

Účastník prokazuje splnění základní způsobilosti v rozsahu dle § 74 zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZZVZ“) a profesní způsobilosti podle § 77 odst. 1 a § 77 odst. 2 písm. a) ZZVZ, v souladu s § 228 odst. 1 a 2 ZZVZ ve spojení s § 45 odst. 4 ZZVZ, a to předložením odkazu na výpis ze Seznamu kvalifikovaných dodavatelů vedený v informačním systému veřejné správy.

Výpis z SKD účastníka je k dispozici na adrese:

<https://skd.nipez.cz/ISVZ/Ciselniky/Seznam.aspx?type=1&vt=2&data=ZmNJQyUzZDA2MjkxMDMxJTI2>

¹ Sankce EU proti Rusku a Bělorusku možno ověřit na: www.mcribis.cz

i) realizoval v posledních 3 letech následující zakázky:

Školení kybernetické bezpečnosti, každá v minimální hodnotě 15 000 Kč bez DPH.

Významná zakázka č. 1

Název zakázky	Školení kybernetické bezpečnosti
Rozsah předmětu zakázky	Školení kybernetické bezpečnosti pro koncové uživatele
Finanční objem zakázky	19.000, - Kč
Datum realizace zakázky	20. 5. 2025
Identifikace objednatele	Nakladatelství C. H. Beck, s. r. o. / IČ: 24146978

Významná zakázka č. 2

Název zakázky	Školení kybernetické bezpečnosti
Rozsah předmětu zakázky	Školení kybernetické bezpečnosti pro koncové uživatele
Finanční objem zakázky	42.500, - Kč
Datum realizace zakázky	10. 3. 2025
Identifikace objednatele	Kamýk Daunen s.r.o. / IČ: 25691104

Významná zakázka č. 3

Název zakázky	Školení kybernetické bezpečnosti
Rozsah předmětu zakázky	Školení kybernetické bezpečnosti pro koncové uživatele
Finanční objem zakázky	35.000, - Kč
Datum realizace zakázky	10. 1. 2024
Identifikace objednatele	Progresus invest holding core a.s. / IČ: 13995758

Dodavatel, případně osoba oprávněná jednat za dodavatele, podpisem tohoto prohlášení bere na vědomí, že případné nepravdivé prohlášení může vést k uvedení zadavatele v omyl a tím i ke vzniku materiální i nemateriální škody na straně zadavatele, stejně tak možnosti vystavení se postihu za protiprávní jednání i trestněrelevantního charakteru uvedením nepravdivých či zkreslených údajů v rámci tohoto prohlášení.

Společnost: **Next Generation Security Solutions s.r.o.**
 Zastoupena: Mgr. Ondřejem Dedkem, jednatelem
 Se sídlem: U Uranie 954/18, Holešovice, 170 00 Praha 7
 IČO: 06291031

V Praze dne 2. listopadu 2025

5. Seznam lektorů

Lektoři podílející se na poskytování předmětu plnění musí disponovat minimálně 3letou praxí v oboru kybernetické bezpečnosti a minimálně 2letou praxí v lektorování uvedených specializovaných témat, stanovených ve Věcném vymezení předmětu plnění.

Seznam techniků je uveden v následující tabulce:

Jméno a příjmení	Délka praxe v oboru kybernetické bezpečnosti	Délka praxe v lektorování uvedených specializovaných témat
g [REDACTED]	7 let	4 roky
[REDACTED]	10 let	6 let

Za každého lektora dodavatel dále předkládá:

- a) kopie dokladů o vzdělání a odborné kvalifikaci lektorů
- b) čestné prohlášení o požadované délce praxe
- c) ukázkovou nahrávku školení v délce alespoň 30 minut

6. Obsah školení

Zajištění školení kybernetické bezpečnosti pro administrativní zaměstnance včetně zajištění ubytování, stravování a prostor a techniky pro školení.

1. **Obecný úvod** – co je kyberbezpečnost, problematika a rozsah;
2. **Hrozby** – co nám a organizaci hrozí;
3. **Zvyšování bezpečnostního povědomí**
 - a. bezpečné chování v online prostředí
 - b. bezpečné používání práce na dálku a mobilita
 - c. klasifikace a sdílení dat
 - d. specifické povinnosti vedoucích pracovníků
4. **Jak se bránit a předcházet rizikovým situacím:**
 - a. Phishing a nevyžádané emaily,
 - b. Podvodné WWW stránky,
 - c. Správné používání hesel,
 - d. Fyzická bezpečnost,
 - e. Sociální inženýrství;
 - f. Zaměření kybernetická rizika u specifické agendy Objednatele:
 - i. Úsek účetnictví
 - ii. Personalistika
 - iii. Správa dokumentů
 - iv. Obsluha datových schránek
 - v. Elektronická pošta
5. **Případná specifická interní bezpečnostní pravidla organizace.**
6. **Praktické příklady a ukázky vektorů kybernetických útoků**
7. **Kazuistika kybernetické bezpečnosti**
8. **Ochrana osobních údajů – manažerský přehled (GDPR)**
 - a. Hlavní právní základy zpracování osobních údajů, fotografií a audio-video
 - b. Role a součinnost **DPO × manažer/architekt KB**
 - c. zásady minimalizace, pseudonymizace/šifrování, auditní stopa
9. **Legislativní rámec KB a regulace služeb dle nového zákona o KB**
 - a. Nový Zákon o kybernetické bezpečnosti
 - b. pojem poskytovatel regulované služby
 - c. rozdělení režimů vyšších/nížších povinností
 - d. princip samoidentifikace a registrace regulované služby.
 - e. Předmět a princip regulace dle směrnice NIS2
 - f. Politika AI, AI z pohledu rizik KB
 - g. AI Act - Evropský akt o umělé inteligenci

Volitelným návazným krokem po školení může být **dodání dokumentu Základy bezpečného chování na internetu**, který shrnuje podávané informace a uživatelům je nadále k dispozici.

Školení realizuje certifikovaný specialista se zkušenostmi z oboru bezpečnosti informací.

6.1. Ukázka formy školení

Příklad ukázkového záznamu v oblasti školení – **Zvyšování bezpečnostního povědomí:**

- <https://www.youtube.com/watch?v=jqi1S6ME4go>
- <https://www.youtube.com/watch?v=qRDRsVkeCLc>
- https://www.youtube.com/watch?v=o7tcQdA_9H8

6.2. Čestné prohlášení o požadované délce praxe

Společnost **Next Generation Security Solutions s.r.o.** tímto čestně prohlašuje, že uvedení lektori disponují minimálně 7letou praxí v oboru kybernetické bezpečnosti a minimálně 4letou praxí v lektorování uvedených specializovaných témat, stanovených ve Věcném vymezení předmětu plnění.

V Praze dne 2. 11. 2025

.....
Mgr. Ondřej Dedek, jednatel

7. NGSS tým

Lead Consultant

Antonín se v uplynulých dvaceti letech podílel na projektech zavádění ISMS spolu se zaváděním opatření v oblastech managementu bezpečnosti informací, ohodnocení aktiv, klasifikace dokumentů a informací, řízení fyzické bezpečnosti a bezpečnosti prostředí, bezpečnosti lidských zdrojů, řízení právních vztahů z hlediska bezpečnosti a krizového a havarijního plánování. V posledních patnácti letech projektově řídil projekty zavádění ISMS a implementaci bezpečnosti v informačních a komunikačních systémech. Je držitelem certifikátů Lead auditor ISMS dle ISO/IEC 27001, Lead auditor SMS dle ISO/IEC 20000 a je držitelem certifikátu PRINCE2 pro oblast projektového řízení.

Information Security Consultant

Ondřej je certifikovaný manažer informační bezpečnosti s certifikacemi M-BI a CISM. Dále působí jako architekt IT řešení se znalostmi v oblasti serverů, storage, virtualizace, zálohování a bezpečnosti, je držitelem certifikace TOGAF. Podílí se na významných projektech v oblasti ochrany před kybernetickými útoky a pracuje na projektech bezpečnosti informací formou auditu, analýzy a zpracování dat. Věnuje se také školení odborných rolí v oblasti bezpečnosti informací.

Security Consultant

Barbora je absolventkou státní univerzity bezpečnostně právního zaměření a v naší společnosti spolupracuje na různých projektech z oblasti bezpečnosti informací. Provádí audity bezpečnosti informací/ kybernetické bezpečnosti, identifikaci a hodnocení aktiv a rizik, navrhuje organizační opatření k ošetření rizik a zabývá se ochranou osobních údajů. Je držitelkou certifikace CRISC (Certified in Risk and Information Systems Control) a M-BI (Manažer bezpečnosti informací).

Lead Consultant

Martin je absolventem Technické univerzity v Liberci. Již 5 let se zabývá systémy řízení bezpečnosti informací. V naší společnosti se podílí na konzultační činnosti pro oblasti organizačních opatření – povinnosti vrcholového vedení, organizace lidských zdrojů, bezpečnostní dokumentace, řízení aktiv, analýzy rizik a v oblastech technických opatření – fyzická bezpečnost, řízení identit a přístupových oprávnění, řízení událostí a incidentů bezpečnosti informací. Společnosti, ve kterých se podílel na zavádění systému bezpečnosti informací úspěšně procházejí certifikačními a kontrolními audity. Je držitelem certifikátu Manažer ISMS dle ISO 27001.

Senior Security Consultant

Daniel má dlouholeté zkušenosti se správou a bezpečností počítačových sítí. Zároveň je expertem v oblasti ochrany osobních údajů, je držitelem certifikátu Certificate EU GDPR DPO. Dále je držitelem certifikátu Lead auditor ISMS dle ISO/IEC 27001. Pracuje na projektech bezpečnosti informací a ochrany osobních údajů s důrazem na technické a analytické činnosti.

Senior Security Consultant

Miroslav má téměř 30 let zkušeností v ICT, kybernetické bezpečnosti a ochraně osobních údajů, z toho dvě dekády v justici. Zaměřuje se zejména na veřejnou správu, zdravotnictví, školství a sociální služby. Jeho klíčovou specializací je edukace v oblasti kybernetické bezpečnosti, ochrany osobních údajů a legislativy ICT. Věnuje se ISMS, analýze rizik, bezpečnostní dokumentaci a zavádění opatření dle legislativy, zejména po transpozici NIS2. Je interním doktorandem na Katedře informačních technologií ČZU v Praze. Je držitelem certifikací ITIL4, PRINCE2, IPMA, ITSM, DevOps a dalších.

Security consultant

Šimon se zaměřuje na management kybernetické bezpečnosti a ve své práci zohledňuje mnohaleté zkušenosti z působení v bankovním sektoru. Vystudoval management na Univerzitě Karlově v Praze a v NGSS se podílí na různých projektech spojených s hodnocením aktiv, zaváděním opatření ISMS, řešením ochrany osobních údajů, analýzami rizik či bezpečnostními audity. Je držitelem certifikátu BCM manager dle normy ISO 22301 a Manažer ISMS.

Security Consultant

Ivo při výkonu své práce zohledňuje zkušenosti ze správy a zabezpečení počítačových sítí, které propojuje s poznatky získanými během studia na právnické fakultě Západočeské univerzity v Plzni. V naší společnosti se zaměřuje zejména na projekty v oblasti informační bezpečnosti, na identifikaci a hodnocení aktiv a rizik a na ochranu osobních údajů, přičemž klade důraz na technické a analytické činnosti.

Security Consultant

Lukáš se zaměřuje na technickou stránku auditů a hodnocení zabezpečení informačních systémů. Odborné zkušenosti získal při práci v našem bezpečnostním operačním centru (SOC), především jako hlavní analytik (úroveň L2). V současnosti se věnuje konzultační činnosti, zaměřuje se zejména na technické hodnocení zabezpečení při plnění požadavků norem jako ISO/IEC 27001 nebo NIS 2. Je absolventem kurzu Manažer bezpečnosti informací a držitelem certifikací CySA+ a CISSP.

Security Consultant

Roman absolvoval bezpečnostně právní studia, kde se setkal s kybernetickou bezpečností a ochranu informací. Disponuje několikaletými zkušenostmi v oblasti ochrany osobních údajů, kde se specializoval na implementaci a dodržování právních rámců týkajících se zpracování a zabezpečení osobních údajů. Postupně rozšířil své zaměření i na kybernetickou bezpečnost. Jeho profil doplňují zkušenosti s řízením IT projektů, které nasbíral v prostředí finančního sektoru.

Advokát

Nikola je advokátka s mnohaletou generální praxí. Věnuje se mj. závazkovému právu, tedy přípravě a řešení smluv z nejrůznějších oblastí a zajišťuje konzultace z oblasti problematiky ochrany osobních údajů a kybernetické bezpečnosti.

Senior Project Manager

Jana v uplynulých 25 letech řídila projekty většího rozsahu v oblasti budování informačních systémů a dodávek technologií pro zdravotnické záchranné služby či krizové řízení městských částí. Zákazníkům ze státní sféry pomáhala budovat centrální projektové kanceláře a řídila kolektiv servisních a projektových manažerů. Pracuje na projektech týkající se kybernetické bezpečnosti veřejných institucí, dodávek infrastruktury a specializovaných SW pro zákazníky. Její doménou je systémová integrace. Jana je držitelkou certifikátů Prince2 Practitioner, ITIL 4 Foundation a P3.Express.

Enterprise Security Architect

Daniel je expertem v oblasti bezpečnosti informací s více než dvacetiletou praxí v oblastech implementace a provozu systémů řízení bezpečnosti informací, poradenských službách k ochraně dat, řízení rizik, designu bezpečnostní architektury a auditu.

Information Security architect

Stanislav je zkušený konzultant, auditor a manažer s dlouholetou (30+) praxí v oblasti praktické administrace IT systémů, návrhů IT řešení (IT design) a řízení IT služeb (ITSM). Posledních 15 let se věnuje výhradně oblasti informační bezpečnosti v oblastech architektury, auditu, návrhů bezpečnostních řešení, zajištění compliance, implementace ISMS, risk managementu, bezpečností cloudových služeb apod. Je držitel mnoha uznávaných a aktuálně platných mezinárodních certifikátů (CISA, CISSP, CRISC, CCSP, TOGAF, ITIL, PRINCE2) a členem odborných organizací ISACA a ISC2.

Senior Security Architect

Viktor se zaměřuje na inovace a provozně funkční informační a komunikační technologickou a kybernetickou bezpečnost se zahrnutím business požadavků. Celou profesní kariéru se zabývá praktickými technickými aspekty sledování a vyhodnocování aktivit, jak zařízení, tak lidských uživatelů na všech dostupných vrstvách informačního prostoru. Aktuálně se podílí na praktickém provozu, konzultacích a koncepčním rozvoji rozsáhlých exponovaných prostředí jak v oblasti státní správy, tak komerčního sektoru.

Základní pracovní životní pravidlo které ctí je: Vědět, naslouchat, analyzovat, řešit a následně doručovat potřebné hodnoty.

[REDACTED]

Security Architekt/Vedoucí týmu implementačních služeb

David je zkušeným specialistou bezpečnostních technologií s více než sedmiletou praxí v oblastech jako jsou SIEM, SOAR, Identity či ochrana dat. V uplynulých letech se podílel na mnoha významných projektech zavedení komplexních řešení bezpečnosti, od jejich návrhu po samotnou implementaci. Je držitelem certifikace CompTIA Security+ a nejvyšších certifikací pro jednotlivé technologie. Zároveň provádí presale našich produktů v oblasti IT bezpečnosti.

[REDACTED]

Security Specialist

Martin má dlouholeté IT zkušenosti v oblasti zavádění, správy, školení a prezentací collaboration a security produktů. Většinu své profesní kariéry působil na straně zákazníků jako správce a lektor produktů HCL Digital Solutions, IBM MaaS360 a Cisco Webex. Před několika lety přešel ze strany zákazníka na stranu dodavatele, kde se jeho činnosti rozšířili o další produkty v oblasti IT security a presale prezentace produktů. Martin je držitelem ocenění HCL Ambassador a IBM Champion a certifikací na produkty Safetica a IBM QRadar.

[REDACTED]

Security Specialist

Josef má dlouholeté zkušenosti se správou produktů Microsoft, specifických zákaznických systémů na platformách Windows a Linux, i uživatelskou podporou. V posledních několika letech se specializuje na implementaci a správu řešení v oblasti kybernetické bezpečnosti. Má za sebou řadu implementací zakázek produktových řešení pro významné zákazníky. Je členem týmu NESTOR Security Operations Center, který se stará o aktivní dohled, reakce na bezpečnostní incidenty a správu bezpečnostních produktů pro naše zákazníky. Je držitelem certifikací na produkty IBM QRadar, ESET, Safetica a Microsoft.

[REDACTED]

Security Analyst, Vedoucí týmu security operations center

Čeněk má dlouholeté zkušenosti v oblasti informačních a komunikačních technologií z několika společností, kde přišel do styku s různými technologiemi. V Oblasti IT Security pracuje již několik let a podílí se na analýze a vyhodnocování kybernetických bezpečnostních událostí. Upravoval a nastavoval korelační pravidla z SIEM řešení. Jeho odpovědností bylo mimo jiné také spravovat řešení Fidelis, provádět skenování zranitelností pomocí nástroje Nessus a následné vyhodnocení včetně reportu zjištěných zranitelností a návrhu na opatření. Zpracovával pravidelné bezpečnostní reporty a aktivně pracoval s nástroji ArcSight ESM, LogManagement, Elasticsearch, Kibana, Flowmon, Fidelis Network & Fidelis Endpoint, MISP a Privileged Access Management.

8. Naše zkušenosti

Níže uvádíme seznam vybraných organizací, ve kterých jsme prováděli nebo provádíme naše služby:

100 Towers Holding a.s.	Louda Auto a.s.
Accolade, s.r.o.	Masarykův ústav a Archiv AV ČR, v. v. i.
AKT plastikářská technologie Čechy, spol. s r.o.	Městská část Praha 2, 5, 9, 10, 11
BBH Tsuchiya s.r.o.	METAL TRADE COMAX, a.s.
Biotechnologický ústav AV ČR, v. v. i. (BIOCEV)	Mypa Tools s.r.o.
Centrum HiLASE	Nadace CERGE-EI
Constellium Extrusions Děčín, s.r.o.	Nemocnice Jablonec n. N.
CPI Services a.s.	OILES CZECH MANUFACTURING S. R. O.
Česká společnost pro jakost, z.s.	PAL Wiping Systems s.r.o.
Datron a.s.	Precision Tools Service Czech s.r.o.
Devizová burza a.s.	PRIMAPOL-METAL-SPOT s.r.o.
Emco spol. s r. o.	Randstad HR Solutions s.r.o.
Fakultní nemocnice Ostrava	S&G Consulting s.r.o.
Fakultní nemocnice u sv. Anny v Brně	Sage Automotive Interiors, Strakonice Fabrics, s.r.o.
FutureLife a.s.	Sellier & Bellot, a.s.
Fyzikální ústav AV ČR, v. v. i.	Siemens s.r.o.
GENNET, s.r.o.	Sodecia safety & interiors Leskovec, s.r.o.
GLOBAL ASSISTANCE a.s.	Státní fond životního prostředí České republiky
Globus ČR, v.o.s.	Statutární město Jablonec n. N.
Gutta ČR - Praha spol.s r.o.	Statutární město Liberec
Hlavní město Praha	Stokvis Promi, s.r.o.
INEP medical s.r.o.	Strojmetal Aluminium Forging, a.s.
Innovation Anywhere s.r.o.	ŠKODA ICT s.r.o.
INVENTI Group s.r.o.	ŠKODA TRANSPORTATION a.s.
Kamýk Daunen s.r.o.	TBG BETONMIX a.s.
Karvinská hornická nemocnice a.s.	TÜV NORD Czech, s.r.o.
KOITO CZECH s.r.o.	Univerzita Karlova
KONFORM – Plastic, s.r.o.	Orkla Foods Česko a Slovensko a.s.
Lesy České republiky, s.p.	voestalpine High Performance Metals CZ s.r.o.
Lesy hlavního města Prahy	Vojenská Zdravotní pojišťovna České republiky
Liberecká IS, a. s. (LIS)	

Reference našich klientů

„S firmou NGSS proběhla spolupráce na zavedení TISAX v naší firmě. Během zavádění byl celý tým vždy velmi ochotný, vstřícný, k dispozici kdykoliv. Díky velmi profesionálnímu přístupu jsme společnými silami jsme došli do úspěšného konce. V případě další spolupráce nebudeme váhat oslovit znovu. Jsme velmi spokojeni s Vaší prací a děkujeme.“

KONFORM-Plastic, s.r.o.

„Práci NGSS týmu bych ohodnotil jako profesionální, vstřícnou a schopnou se přizpůsobit potřebám a znalostem klienta. V začátcích projektu byl pro mě TISAX velkou neznámou, postupem času, po mnoha konzultacích, kontrolních dnech, interním auditu a nemálo návštěvách, jsem s podporou týmu NGSS v zádech získal potřebné znalosti, přehled a informace, které mi pomohly systém TISAX úspěšně implementovat. Zároveň bych velmi ocenil kvalitu a obsah vypracované a poskytnuté dokumentace, která byla základním kamenem pro získání certifikace.“

Sage Automotive Interiors, Strakonice Fabrics, s.r.o.,

„Děkujeme týmu NGSS za vynikající práci při podpoře zavedení nového systému hodnocení rizik a návrhu bezpečnostní architektury IT. Jejich spolupráce a konzultace při úpravách „Systému řízení bezpečnosti informací“ odpovídala našim představám. Jsme s jejich profesionálním přístupem, spoluprací a výsledky velmi spokojeni. Vyzdvihnout musíme proaktivní a lidský přístup kooperujících konzultantů. Proto bychom společnost NGSS dále doporučili jako spolehlivého partnera v oblasti informační bezpečnosti.“

Liberecká IS, a.s.

„Díky spolupráci se společností NGSS, jsme detailně zhodnotili stav bezpečnosti informací v kyberprostoru Masarykovy univerzity. Jejich odborný tým nám poskytl komplexní analýzu, doporučení a postupy pro zlepšení našich bezpečnostních opatření v souladu se Zákonem o kybernetické bezpečnosti a nejlepšími praxemi a postupy v oboru. Jsme velice vděční za profesionální přístup a spolehlivou a odbornou pomoc.“

– Divize IT služeb, Ústav výpočetní techniky Masarykovy univerzity (UVT MUNI),

„Konzultanty společnosti NGSS jsme poprvé využili v souvislosti s Kybernetickým zákonem a analýzou jeho dopadu na chod naší Městské části. Jelikož jsme s výsledky i přístupem byli spokojeni, neváhali jsme využít služeb i v oblasti zavádění normy ISO 27001 a především analýzy dopadu GDPR.“

Městská část Praha 2

9. Informace o společnosti

Next Generation Security Solutions s.r.o. (NGSS) je česká společnost poskytující služby specialistů v oblasti řízení a nastavování bezpečnostních procesů, implementace bezpečnostních služeb a projektového řízení. Společnost nabízí svým zákazníkům zcela ojedinělý koncept komplexního **technologicky nezávislého řešení** v oblasti řízení a správy bezpečnosti informací. Zakladateli a členy realizačního týmu jsou ti nejzkušenější konzultanti a techničtí specialisté, působící v oboru minimálně 15 a více let.

NGSS se specializuje na poskytování služeb vysoce odborných specialistů schopných prokázat se všemi významnými profesními certifikacemi, jako jsou **CISA, CRISC, CISM, CISSP, ISMS a SMS Lead Auditor, Manažer bezpečnosti informací, PRINCE 2, ITIL, TOGAF, CEH** a dalšími.

Komplexní a systémový postup našich konzultantů Vás dovede k souladu s **GDPR** a navrhne veškeré potřebné procesy a technologie využitelné zároveň v oblastech **Kybernetické bezpečnosti**.

Spolupracujeme s mnoha významnými zadavateli v oblasti odborných posudků, due dilligence, **bezpečnostních auditů**, přípravy zadávacích dokumentací, bezpečnostních **analýz**, nápravných opatření i **právního poradenství**.

Dalším významným pilířem našich služeb je služba **SOC** (security operations center), která zahrnuje mj. role pro **ISMS** podporu a poradenství, outsourcing role pověřence pro ochranu osobních údajů (**DPO – Data Privacy Officer**), produktově nezávislou analyticko-operativní schopnost při řešení incidentů na základě výstupů z nástrojů **SIEM**, atp.

V neposlední řadě jsou Vám naši odborníci připraveni poskytnout jednorázové služby **penetračního testování** informačních systémů a ICT infrastruktury, řešení pro zabezpečení před ztrátou dat **DLP** (Data Loss Prevention) a poradenství v oblasti nasazení a provozu systémů pro **šifrování dat**.

Nabízíme nástroj pro zajištění povinnosti řídit rizika dle standardu NIS2. Společnosti tak efektivně řídí bezpečnostní opatření jednoduchou a přehlednou formou díky systému [OMIS](#):

- Vybrané procesy informační bezpečnosti budou v souladu s nařízením NIS 2, TISAX, DORA i ISO 27001.
- Moderní a uživatelsky atraktivní aplikace, ze které mají uživatelé i vývojáři radost.
- Na jeden klik pořídíte elektronické dokumenty pro bezpečnostní auditory

Next Generation Security Solutions s.r.o.

U Uranie 954/18, Praha 7, 170 00

sales@ngss.cz | www.ngss.cz

