Číslo smlouvy objednatele: DS202301010

Číslo smlouvy zhotovitele:

SMLOUVA O DÍLO

kterou uzavřely podle občanského zákoníku (zák. č. 89/2012 Sb. ve znění pozdějších předpisů)

dále uvedeného dne, měsíce a roku, níže uvedené smluvní strany:

Next Generation Security Solutions s.r.o.

se sídlem:	U Uranie 954/18, Praha 7, 170 00
zastoupené:	Václavem Novákem, MBA, jednatelem
IČO:	06291031
DIČ:	CZ06291031
Bankovní spojení:	[redacted]

jako **zhotovitel** na straně jedné

a

STATUTÁRNÍ MĚSTO LIBEREC

se sídlem:	nám. Dr. E. Beneše 1/1, 460 59 Liberec
zastoupené:	Ing. Jaroslavem Zámečníkem, CSc., primátorem
zastoupené ve věci smlouvy:	Ing. Zbyňkem Vavřinou, vedoucím odboru vnitřních věcí
zastoupené ve věci plnění smlouvy:	Jakubem Stodůlkou, vedoucí oddělení informatiky a řízení procesů
IČO:	00262978
DIČ:	CZ00262978
Bankovní spojení:	[redacted]

jako **objednatel** na straně druhé

1. PŘEDMĚT SMLOUVY

1.1 Zhotovitel pro Objednatele zajistí a předá následující dílo spočívající v dodání GAP analýzy specifikované dle nabídky od zhotovitele (specifikované v příloze č. 1 této smlouvy). Tato smlouva se týká části nabídky „**Etapa 1 – Posouzení stavu bezpečnosti informací**". Výstupem činnosti Zhotovitele bude zpráva z posouzení stavu bezpečnosti informací u Objednatele dle požadavků na poskytovatele regulované služby v režimu nižších povinností, která bude obsahovat:

1.1.1 kritéria a podmínky srovnávací analýzy,

1.1.2 shrnutí zjištění,

1.1.3 zhodnocení stavu bezpečnosti informací s uvedením neshod vůči požadovanému stavu a základnímu doporučeními k jejich odstranění,

1.1.4 doporučení k zavedení systému řízení bezpečnosti.

2. CENA DÍLA, TERMÍNY, PLATEBNÍ PODMÍNKY

2.1 Objednatel se zavazuje dílo převzít a zaplatit za ně dohodnutou odměnu.

2.2 Za dílo specifikované v článku 1.1 této Smlouvy se Objednatel zavazuje Zhotoviteli zaplatit odměnu v celkové výši 68 400 Kč bez DPH.

2.3 Faktura za realizaci díla bude vystavena po předání a akceptaci díla Objednatelem.

2.4 Termín pro splnění předmětu díla dle bodu 1.1 je stanoven nejpozději do 30. 9. 2023.

2.5 Cena díla zahrnuje veškeré náklady Zhotovitele nezbytné k řádnému, úplnému a kvalitnímu provedení díla dle čl. 1.1 Smlouvy.

2.6 K ceně uvedené v čl. 2.2 této smlouvy bude připočtena sazba DPH odpovídající platným a účinným právním předpisům České republiky.

2.7 Splatnost faktur je 14 dnů ode dne jejich doručení Objednateli.

2.8 Nedodrží-li Objednatel termín splatnosti, je Zhotovitel oprávněn požadovat smluvní úrok z prodlení ve výši 0,01 % z dlužné částky za každý kalendářní den.

2.9 Nedodrží-li Zhotovitel termín splnění předmětu díla, je Objednatel oprávněn požadovat smluvní úrok z prodlení ve výši 0,2 % z ceny příslušné části díla vč. DPH, se kterou je zhotovitel v prodlení, za každý kalendářní den.

3 ZÁVĚREČNÁ UJEDNÁNÍ A DOLOŽKY

3.1 Tato smlouva a vztahy z ní vyplývající se řídí právem České republiky.

3.2 Smlouva se sjednává na dobu určitou a to do ukončení veškerých činností spojených se zajištěním plnění předmětu smlouvy, nejpozději do data podpisu akceptačního protokolu.

3.3 Smluvní strany jsou povinny vzájemně spolupracovat při plnění předmětu této Smlouvy a jsou povinny poskytnout si vzájemně dostupnou součinnost nezbytnou k tomu, aby mohl být naplněn předmět této Smlouvy – tj. vytvoření plně funkčního díla pro Objednatele dle podmínek této Smlouvy, bez vad a nedodělků.

3.4 Smluvní strany jsou povinny neprodleně si vzájemně sdělovat informace, které mohou mít vliv na plnění závazků vyplývajících z této Smlouvy.

3.5 Na hotové dílo dle čl. 1.1 je platná záruka 1 rok ode dne předání a převzetí díla bez vad a nedodělků.

3.6 Hotové dílo se předává na základě předání dokumentace a její akceptace pomocí písemného, oboustranně podepsaného protokolu.

3.7 Smluvní strany jsou oprávněny zveřejnit veškerý obsah této smlouvy, budou-li o to požádány dle zákona č. 106/99 Sb.

3.8 Měnit či doplňovat tuto Smlouvu je možné pouze formou písemných, vzestupně číslovaných dodatků.

3.9 Tato Smlouva je vyhotovena ve dvou (2) stejnopisech s platností originálu, přičemž každá ze Smluvních stran obdrží po jednom (1) vyhotovení.

3.10 Smluvní strany prohlašují, že si tuto Smlouvu přečetly, s jejím zněním souhlasí a na důkaz pravé a svobodné vůle připojují níže své podpisy.

3.11 Smluvní strany berou na vědomí, že tato smlouva bude zveřejněna v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

3.12 Smluvní strany berou na vědomí, že jsou povinny označit údaje ve smlouvě, které jsou chráněny zvláštními zákony (obchodní, bankovní tajemství, osobní údaje, …) a nemohou být poskytnuty, a to šedou barvou zvýraznění textu. Neoznačení údajů je považováno za souhlas s jejich uveřejněním a za souhlas subjektu údajů.

3.13 Smlouva nabývá účinnosti nejdříve dnem uveřejnění v registru smluv v souladu s § 6 odst. 1 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

3.14 Smluvní strany berou na vědomí, že plnění podle této smlouvy poskytnutá před její účinností jsou plnění bez právního důvodu a strana, která by plnila před účinností této smlouvy, nese veškerou odpovědnost za případné škody takového plnění bez právního důvodu, a to i v případě, že druhá strana takové plnění přijme a potvrdí jeho přijetí.

Přílohy: 1. Nabídka Zhotovitele ze dne 24. 2. 2023

V Liberci dne:

V Praze dne:

_____

Za Objednatele

Ing. Zbyněk Vavřina
Vedoucí odboru vnitřních věcí

_____

Za Zhotovitele

Václav Novák, MBA
jednatel

NABÍDKA NA:

„PODPORU PŘI ZAVEDENÍ POŽADAVKŮ NA POSKYTOVATELE REGULOVANÉ SLUŽBY V REŽIMU NIŽŠÍCH POVINNOSTÍ“

STATUTÁRNÍ MĚSTO LIBEREC

V PRAZE DNE:

24. ÚNORA 2023

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00
Tel.: 237 836 950
sales@ngss.cz | www.ngss.cz

1. Identifikační údaje uchazeče

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
Bankovní spojení:	301607295/0300
Statutární orgán:	Václav Novák, MBA, jednatel
Webové stránky:	www.ngss.cz
Kontaktní osoby:	**Antonín Šefčík** Lead consultant +420 601 307 992 asefcik@ngss.cz **Ing. Jaromír Žák** Ředitel +420 602 382 317 jzak@ngss.cz

2. Obsah

STATUTÁRNÍ MĚSTO LIBEREC

Jakub Stodůlka

nám. Dr. E. Beneše 1/1

460 01, Liberec

Vážený pane Stodůlko,

Jménem společnosti Next Generation Security Solutions s.r.o. (dále také „NGSS“) si Vám dovolujeme předložit nabídku na poskytnutí služeb k zavedení požadavků kybernetické bezpečnosti na poskytovatele regulované služby v režimu nižších povinností u statutárního města Liberec (dále jen „úřad“), které vycházejí z požadavků směrnice NIS 2 a návrhu nového zákona o kybernetické bezpečnosti a návrhů navazujících vyhlášek.

Cílem je zajistit zavedení požadavků kybernetické bezpečnosti dle požadavků směrnice NIS2 do prostředí úřadu. Požadavky NIS2 budou realizovány zavedením systému řízení bezpečnosti informací v souladu s požadavky připravované vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (dále také „Vyhlášky“). Nabízíme Vám realizovat práce zahrnující realizaci celého procesu rozděleného do období 2 let:

1. Provedení **srovnávací analýzy současného stavu kybernetické bezpečnosti** vůči požadavkům vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (dále jen Vyhláška).
2. **Provedení hodnocení aktiv a přijetí bezpečnostních opatření** k určení možných rizik a návrhu jejich pokrytí.
3. **Implementace vybraných bezpečnostních opatření** zahrnuje návrh postupů, jejich popis v bezpečnostní dokumentaci a rozpracování do návrhu záznamů systému řízení bezpečnosti informací.
4. **Zavedení postupů kontinuity činností** zahrnuje návrh plánu kontinuity činností a navazujícího plánu obnovy v oblasti IT.
5. **Provedení interního auditu a přezkoumání zajišťování minimální úrovně kybernetické bezpečnosti** uzavírá celý cyklus zavedení systému řízení bezpečnosti informací. Audit bude proveden jako vzorový.

K upřesnění nebo vysvětlení nabídky a zapracování případných připomínek Vám nabízím jednání ať již vzdáleně, nebo ve Vaší společnosti.

S pozdravem
Antonín Šefčík, lead consultant

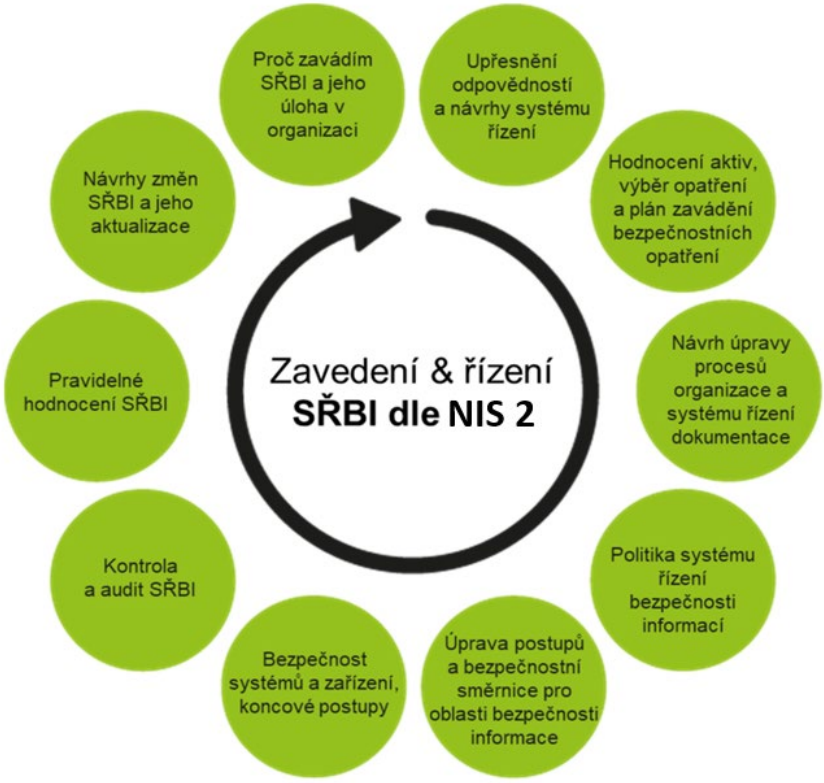
3. Předmět plnění

Cílem je zvýšit zabezpečení informací u úřadu zavedením systému řízení bezpečnosti informací na základě požadavků návrhu Vyhlášky. Pojem systém řízení bezpečnosti informací (ve zkratce „SŘBI“) se používá jako synonymum pro pojem zajišťování minimální úrovně kybernetické bezpečnosti užívaný ve Vyhlášce.

V oblasti zavedení požadavků na poskytovatele regulované služby v režimu nižších povinností u úřadu je potřebné realizovat:

- **posouzení stavu bezpečnosti informací** u úřadu dle kritérií návrhu Vyhlášky včetně zpracování záznamu s uvedením neshod a doporučení,
- provedení identifikace a **hodnocení aktiv** a přijetí bezpečnostních opatření;
- návrh bezpečnostních postupů a jejich zapracování do **bezpečnostní dokumentace** s důrazem na vytvořením směrnic netechnické a technické bezpečnosti a uživatelské bezpečnostní směrnice a zpracování **dílčích postupů a jejich zdokumentování**,
- návrh **postupů zajištění kontinuity činností** a zpracování příslušné dokumentace,
- provedení **interní auditu** a provedení **Přezkoumání zajišťování minimální úrovně kybernetické bezpečnosti**.

Grafické znázornění zavedení a řízení systému řízení bezpečnosti informací (SŘBI) je uvedeno zde:



Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

3.1. Etapa 1: Posouzení stavu bezpečnosti informací

Posouzení stavu bezpečnosti informací zahrnuje prověření stavu bezpečnosti skrze srovnávací analýzu spolu s návrhem dalšího postupu při odstranění zjištěných neshod.

Posouzení stavu by mělo ukázat silné stránky a slabiny ochrany informací. Pro porovnání stavu bezpečnosti budou použity vybrané požadavky na poskytovatele regulované služby v režimu nižších povinností.

Posouzení stavu bude provedeno v Liberci v sídle úřadu.

Srovnávací analýza zahrnuje dvě části:

- První část tvoří vlastní prověření stavu bezpečnosti spolu s návrhem dalšího postupu při odstranění zjištěných neshod;
- Druhou část pak tvoří návrh deklaratorní Politiky systému řízení bezpečnosti informací (dále také „SŘBI“), která bude tvořit základní dokument pro zavedení a provoz kybernetické bezpečnosti.

Posouzení stavu bezpečnosti informací ověří úroveň zabezpečení informací zpracovávaných úřadem. V rámci posouzení stavu bude posuzována zejména úroveň zavedení:

- organizačních bezpečnostních opatření,
- technických bezpečnostních opatření.

Vlastní prověření pak probíhá formou:

- prostudování předané dokumentace,
- posouzení stavu na místě, a to:
  - rozhovory s odpovědnými osobami (respondenty),
  - náhledem do informačních systémů,
  - prohlídkou vstupů do prostor úřadu a prostor, kde jsou informace zpracovávány a ukládány spolu s prohlídkou serveroven a technologických místností,
- vypracování závěrečné zprávy, která bude předána k připomínkám úřadu.

Jednotlivé oblasti jsou rozděleny následovně:

- **Organizační opatření:**
  - zajišťování minimální úrovně kybernetické bezpečnosti,
  - povinnosti vrcholového vedení,
  - bezpečnostní role,
  - řízení bezpečnostní politiky a dokumentace,
  - řízení aktiv
  - řízení dodavatelů,
  - bezpečnost lidských zdrojů,

- řízení změn, akvizice, vývoje a údržby,
- řízení přístupů,
- zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
- řízení kontinuity činností,

- **Technické opatření:**
  - fyzická bezpečnost,
  - bezpečnost komunikačních sítí,
  - správa a ověřování identit,
  - řízení přístupových oprávnění
  - detekce kybernetických bezpečnostních událostí včetně:
    - jejich hlášení,
    - naplnění informační povinnost poskytovatele regulované služby,
    - procesu reakce na protiopatření, výstrahy nebo varování,
  - zaznamenávání bezpečnostních a relevantních provozních událostí,
  - aplikační bezpečnost,
  - kryptografické algoritmy,
  - zajišťování dostupnosti regulované služby a
  - zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv.
- **Naplnění registračních a evidenčních povinností** vůči:
  - Portálu NÚKIB a
  - Evidencím NÚKIB.

Výstupy:

- **Zprava z posouzení stavu bezpečnosti informací u úřadu dle požadavků na poskytovatele regulované služby v režimu nižších povinností**, která bude obsahovat:
  - kritéria a podmínky srovnávací analýzy,
  - shrnutí zjištění,
  - zhodnocení stavu bezpečnosti informací s uvedením neshod vůči požadovanému stavu a základnímu doporučeními k jejich odstranění,
  - doporučení k zavedení systému řízení bezpečnosti.

3.2. Etapa 2: Provedení hodnocení aktiv a rizik a přijetí bezpečnostních opatření

Cílem etapy je zjistit nároky na dostupnost, důvěrnost a integritu u zpracovávaných informací u úřadu.

> Proces **hodnocení aktiv** zahrnuje identifikaci a ohodnocení aktiv (informací a prostředků a osob podílejících se na jejich zpracování) a následný výběr bezpečnostních opatření a zpracování plánu jejich zavedení.

V úvodu etapy jsou určeni a poučeni Garanti aktiv[1] a následně jsou s nimi provedeny rozhovory k ohodnocení procesů/informací za které jsou garanti odpovědni. Rozhovory řídí konzultanti společnosti NGSS.

Provedení hodnocení rizik bude provedeno **ve třech na sebe navazujících fázích**:

1. Příprava hodnocení aktiv.
2. Provedení hodnocení aktiv.
3. Výběr opatření k zabezpečení informací.

3.2.1. Příprava hodnocení aktiv

Cílem této fáze je připravit provedení hodnocení aktiv s důrazem na zpracování metodiky identifikace a hodnocení aktiv v závislosti na podmínkách úřadu a upřesnění hodnocených aktiv.

> **Popis postupu přípravy hodnocení rizik:**
>
> - určení osob, se kterými bude provedeno dotazování,
> - provedení prvotního rozhovoru k upřesnění primárních aktiv,
> - návrh primárních aktiv a návrh rozhovorů k hodnocení aktiv,
> - návrh, projednání a schválení metodiky hodnocení aktiv a rizik.

Výstupy fáze:

- **Metodika identifikace a hodnocení aktiv;**
- **Registr aktiv** (evidence aktiv).

[1] Garant aktiva je bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnost aktiva (zejména informací, ale i podpůrná aktiva). Garant aktiva má metodickou a provozní znalost daného aktiva, zodpovídá za klasifikaci informací a definování bezpečnostních požadavků na ochranu jemu svěřených aktiv.

Next Generation Security Solutions s.r.o.

U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

3.2.2. Provedení hodnocení aktiv

Cílem etapy je zjistit důležitost informací z hlediska nároků na dostupnost, důvěrnost a integritu úřadu.

Proces **hodnocení aktiv** zahrnuje ohodnocení aktiv (informací a prostředků a osob podílejících se na jejich zpracování), následný výběr bezpečnostních opatření a zpracování plánu jejich zavedení.

Popis postupu provedení hodnocení aktiv je následující:

- provedení ohodnocení aktiv,
- doplnění **Registru aktiv**,
- prvotní výběr bezpečnostních opatření,
- zpracování **Zprávy o hodnocení aktiv**.

V závěru etapy bude zpracována zpráva o hodnocení aktiv shrnující zjištění z výše uvedených činností.

Množství potřebných rozhovorů a odpovědných osob bude upřesněn na základě informací zjištěných v předešlé fázi, nejvýše se počítá s provedením 20 rozhovorů.

Výstupy fáze:

- Doplnění dokumentu **Registr aktiv;**
- **Zpráva o hodnocení aktiv.**

3.2.3. Výběr opatření k zabezpečení informací

Cílem fáze je vybrat bezpečnostní opatření k zabezpečení zpracovávaných informací a popsat způsob jejich zavedení.

Popis postupu výběru bezpečnostních opatření je následující:

- dokončení výběru bezpečnostních opatření,
- zpracování přehledu bezpečnostních opatření,
- zpracování plánu zavádění bezpečnostních opatření.

V rámci fáze bude posouzeno, zda jsou existující bezpečnostní opatření dostatečná, a bude proveden výběr dalších opatření. Bude provedeno určení, která opatření budou realizována a tato opatření budou uvedena v **Přehledu bezpečnostních opatření**. Následně bude zpracován **Plán zavedení bezpečnostních opatření**, který na základní úrovni popíše způsob implementace vybraných opatření. V Plánu budou zohledněny i výsledky srovnávací analýzy stavu bezpečnosti.

Výstupy fáze:

- **Přehled bezpečnostních opatření** obsahuje uvedení vybraných a nevybraných opatření z vyhlášky včetně zdůvodnění;
- **Plán zavedení bezpečnostních opatření** obsahuje záznam vybraných opatření s uvedením:
  - cílů a přínosů vybraných bezpečnostních opatření,
  - potřebných zdrojů pro jednotlivá bezpečnostní opatření,
  - osob zajišťujících prosazování jednotlivých bezpečnostních opatření,
  - termínů zavedení jednotlivých bezpečnostních opatření,
  - způsobu realizace bezpečnostních opatření.

3.3. Etapa 3: Implementace vybraných bezpečnostních opatření

Cílem etapy je zavést navržená opatření k ochraně informací do praxe.

Implementace vybraných bezpečnostních opatření bude zahrnovat realizaci opatření zejména k:

- pokrytí zjištěných rizik,
- odstranění neshod zjištěných srovnávací analýzou stavu bezpečnosti,
- pokrytí možných zranitelností.

Vlastní implementace SŘBI je velmi rozsáhlou činností. Zavedení funkčního, pravidelně zlepšovaného systému pak může být i v řádu roků. Implementace by měla probíhat v jednotlivých oblastech Vyhlášky. Důraz by měl být, vedle vlastních technologických úprav a implementace bezpečnostních a monitorovacích nástrojů, zaměřen především na:

- bezpečnou činnost dodavatelů,
- činnost uživatelů,
- správu kybernetických bezpečnostních incidentů a událostí,
- zajištění kontinuity činností.

Vlastní kontinuitu činností řešíme v samostatné etapě, neboť se jedná o rozsáhlou a komplikovanou činnost.

V rámci implementace navrhujeme zpracovat především:

- bezpečnostní postupy a pokyny pro uživatele, včetně způsobu jejich podpory a monitoringu,
- návrh a upřesnění opatření:
  - zaměřených na řádný a bezpečný provoz prostředků pro zpracování informací, služeb a procesů s tím souvisejících,
  - zaměřených na ochranu a kontrolu přístupu k informacím, službám a procesům,
  - pravidel a postupů pořizování, vývoje a údržby systémů k prosazení bezpečnosti informací do celého životního cyklu užívaných systémů od fáze návrhu, vývoje, testování až po vlastní provoz a údržbu,
- návrh řešení bezpečnostních incidentů a zavést evidenci bezpečnostních incidentů,
- Plán rozvoje bezpečnostního povědomí a realizovat jej včetně proškolení vybraných zaměstnanců po určených kategoriích a zpracování záznamu o školení,
- zavedení opatření v oblastech:
  - netechnické bezpečnosti s důrazem na:
    - činnost bezpečnostního managementu,
    - zapracování bezpečnostních požadavků SŘBI do smluv s třetími stranami,
    - označování dokumentů,

- formalizace odesílání zařízení ICT do opravy a jejich likvidace,
- zabezpečení přenosných prostředků ICT,
- vytvoření registru právních požadavků,
- zjištění ochrany osobních údajů a autorského práva,
- provádění porovnání technické shody,

- ICT s důrazem na:
  - formalizaci provozních postupů ICT,
  - formalizaci řízení přístupu k prostředkům ICT,
  - formalizaci změnového řízení a zavádění nových prostředků ICT,
  - kryptografickou ochranu prostředků ICT.

Úroveň politiky a směrnic zpracuje NGSS ve spolupráci s úřadem, pro úroveň záznamů předá NGSS vzory záznamů, poučí úřad, jak záznamy zpracovat a úřad si doplní záznamy za kontroly NGSS.

Výstupy:

Vzhledem k potřebám úřadu **doporučujeme nevytvářet množství jednotlivých politik a dokumentů, ale vytvořit základní směrnice navazující na Bezpečnostní politiku SŘB**I. Tyto dokumenty budou zahrnovat obsah všech politik vyžadovaných vyhláškou o Je též možné zapracovat potřebné požadavky do již stávajících dokumentů. Návrh a hierarchie dokumentů je následující:

Typ dokumentu	Návrh dokumentu úřadu	Požadavek vyhlášky
Vrcholový dokument	• **Politika zajišťování minimální úrovně kybernetické bezpečnosti**	• Politika zajišťování minimální úrovně bezpečnosti
Dokumenty navazující na politiku	• **Směrnice netechnické bezpečnosti**	• Politika organizační bezpečnosti • Politika řízení bezpečnostní politiky a dokumentace • Politika řízení aktiv • Politika řízení dodavatelů • Politika bezpečnosti lidských zdrojů • Politika zvládání kybernetických bezpečnostních událostí a incidentů • Politika řízení kontinuity činností • Politika fyzické bezpečnosti
Dokumenty navazující na politiku	• **Směrnice technické bezpečnosti**	• Politika řízení změn, akvizice, vývoje a údržby • Politika řízení přístupu • Politika bezpečnosti komunikační sítě • Politika pro zaznamenávání událostí

Next Generation Security Solutions s.r.o.

U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

		• Politika nasazení, používání a údržby nástrojů pro detekci kybernetických bezpečnostních událostí • Politika aplikační bezpečnosti, řízení zranitelností a patch management • Politika používání kryptografie • Politika dlouhodobého ukládání, zálohování a obnovy
Dokumentace pro uživatele	• **Bezpečnostní uživatelská směrnice**	• Politika bezpečného chování uživatelů, administrátorů a osob zastávajících bezpečnostní role • Politika bezpečného používání mobilních zařízení

Vzory potřebných **záznamů** a další dokumentace s důrazem na **Plán rozvoje bezpečnostního povědomí**, **Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků**, **Evidence technických aktiv, která již nejsou výrobcem podporována**, **Spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory** a **Stanovení fyzického bezpečnostního perimetru**.

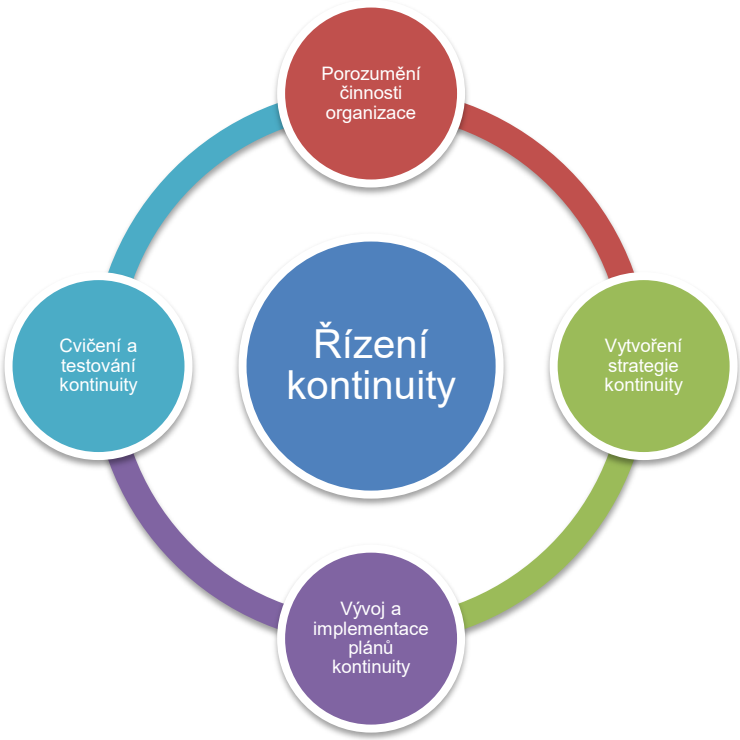
Next Generation Security Solutions s.r.o.

U Uranie 954/18, Praha 7, 170 00 | sales@ngss.cz | www.ngss.cz

3.4. Etapa 4: Zavedení postupů kontinuity činností

Cílem etapy je vytvořit proces řízení kontinuity činností u úřadu.

Klíčovým principem řízení kontinuity činností je snaha určit kritické prvky úřadu, a to z hlediska klíčových služeb, které úřad poskytuje, a z hlediska požadavků zainteresovaných stran, zejména klientů. Po jejich identifikaci je třeba zajistit kontinuitu jejich provozu vytvořením plánů kontinuity a obnovy.



Etapa obsahuje tyto činnosti:

- stanovení **cílů řízení kontinuity činností**,
- zpracování a projednání částí směrnice netechnické bezpečnosti, ve kterých bude ustanoven proces řízení kontinuity činností včetně rozdělení rolí a způsobu naplnění stanovených cílů,
- provedení **analýzy dopadu** s cílem určení parametrů zajištění kontinuity činností (minimální úrovně poskytovaných služeb, doby obnovení chodu a body obnovení dat) a stanovení priorit obnovy,
- vytvoření plánu kontinuity pro identifikované kritické činnosti,
- vytvoření plánu obnovu pro identifikovaná kritická aktiva,
- zavedení procesu prověřování a testování kontinuity činností.

Výstupy:

- **Cíle řízení kontinuity činností** s uvedením cíle, odpovědnosti a součinnosti, termínů realizace, metriky k hodnocení naplnění cíle a termínů kontroly;
- **Metodika pro provedení analýzy dopadů –** dokument popisující metodu a výsledky analýzy dopadů;
- **Zpráva z hodnocení dopadů** – dokument shrnující hodnoty Recovery Point Objective (RPO), Recovery Time Objective (RTO), Maximum Tolerable Downtime (MTD) spolu s pořadím obnovy sužeb/IS a aplikací;
- **Plán kontinuity činností** pro identifikované kritické činnosti s předepsaným obsahem:
  - podmínky aktivace plánu,
  - specifikace osob, které se mají plánem řídit,
  - dočasná řešení a postupy pro zajištění kontinuity služby v případě realizace krizového scénáře;
- **Plán obnovy** pro identifikovaná kritická IT aktiva s předepsaným obsahem:
  - Umístění a popis záloh.
  - Postupy pro obnovení dat včetně pořadí činností, odpovědných osob, potřebného času a zdrojů.
  - Způsob ověření úspěšného obnovení dat ze zálohy.

3.5. Etapa 5: Provedení interního auditu a přezkoumání SŘBI

Cílem etapy je ověřit zavedení bezpečnostních procesů a opatření a připravit pracovníky úřadu na provedení případného certifikačního auditu SŘBI.

V této etapě zavedení SŘBI se provede kontrola zavedení SŘBI cestou interního auditu. Provedení interního auditu je mandatorní povinností pro naplnění požadavků Vyhlášky. Současně v této etapě doporučujeme provést vyškolení interních auditorů z řad zaměstnanců úřadu. Vyškolení interních auditorů a provedení vzorového auditu poskytne dodavatel.

V rámci etapy je potřebné provést:

- projednání způsobu provádění interních auditů SŘBI, upřesnění auditovaných oblastí a procesů SŘBI, jmenovaní auditorů,
- zpracování, projednání a vydání Programu interního auditu SŘBI a Plánu interního auditu SŘBI,
- zpracování a projednání materiálů školení interních auditorů SŘBI a provedení školení interních auditorů SŘBI,
- provedení interního auditu SŘBI:
    - příprava auditu – příprava auditních podkladů, upřesnění rámce a průběhu auditu a příprava jeho účastníků na straně úřadu,
    - provedení auditu – shromáždění relevantních informací z auditovaných oblastí, jejich posouzení, zpracování a schválení ve formě auditních záznamů a příprava závěrů auditu z auditovaných oblastí,
        - audit SŘBI bude proveden dle relevantních paragrafů vyhlášky o kybernetické bezpečnosti a oblastí uvedených v normě ČSN ISO/IEC 27001:2014,
        - důraz bude položen na posouzení stavu zavedení opatření SŘBI podle zpracované bezpečnostní dokumentace,
    - vyhodnocení auditu – bude zjištěna úroveň shody aktuálního stavu auditovaných oblastí se zvolenými kritérii auditu – požadavky Vyhlášky.

V závěru etapy bude provedeno roční přezkoumání SŘBI. Cílem je přezkoumat systém řízení bezpečnosti informací úřadu. Při provedení přezkoumání SŘBI se předpokládá především činnost pracovníků úřadu. Práce dodavatele bude spočívat v návrhu osnovy a následném posouzení zpracovaného přezkoumání.

Výstupy:

- Program interních auditů SŘBI – program na období 3 let;
- Plán interního auditu SŘBI – plán na jednotlivý audit;
- Zpráva z interního auditu SŘBI úřadu obsahující shrnutí zjištění, zhodnocení stavu bezpečnosti informací s uvedením neshod vůči požadovanému stavu;
- Přezkoumání zajišťování minimální úrovně kybernetické bezpečnosti obsahující vyhodnocení stavu SŘBI v předepsaném formátu:
    - vyhodnocení bezpečnostních opatření z předchozího přezkoumání zajišťování minimální úrovně kybernetické bezpečnosti,
    - identifikace změn a okolností, které mohou mít vliv na zajišťování minimální úrovně kybernetické bezpečnosti,
    - zpětná vazba o účinnosti řízení bezpečnosti informací,
    - posouzení stavu plánu zavádění bezpečnostních opatřeních,
    - posouzení dopadů kybernetických bezpečnostních incidentů na poskytované služby a kybernetickou bezpečnost,
    - posouzení změn, které mohou mít negativní dopad na zajišťování minimální úrovně kybernetické bezpečnosti,
    - identifikace možností pro neustálé zlepšování,
    - doporučení potřebných rozhodnutí, stanovení bezpečnostních opatření a osob zajišťujících výkon jednotlivých činností.

4. NGSS tým

Antonín Šefčík
Lead Consultant

V uplynulých dvaceti letech se podílel na projektech zavádění SŘBI 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 SŘBI a implementaci bezpečnosti v informačních a komunikačních systémech. Je držitelem certifikátů Lead auditor SŘBI dle ISO/IEC 27001, Lead auditor SMS dle ISO/IEC 20000 a je držitelem certifikátu PRINCE2 pro oblast projektového řízení.

Ondřej Salák
Senior Security Consultant

Ondřej je certifikovaný manažer informační bezpečnosti s certifikacemi M-BI a CISM. Dále působí jako architekt IT řešení se znalostmi a certifikacemi v oblasti serverů, storage, virtualizace, zálohování a bezpečnosti. Podílel se na významných projektech v oblasti ochrany před kybernetickými útoky. Je držitelem certifikátů TOGAF a ITIL. Pracuje na projektech bezpečnosti informací a ochrany osobních údajů formou analýzy a zpracování dat.

Barbora Kvasnicová
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).

Daniel Uher
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 SŘBI dle ISO/IEC 27001. Pracuje na projektech bezpečnosti informací a ochrany osobních údajů s důrazem na technické a analytické činnosti.

Šimon Procházka
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 SŘBI, řešením ochrany osobních údajů, analýzami rizik či bezpečnostními audity. Je držitelem certifikátu BCM manager dle normy ISO 22301.

5. Nabídková cena

Popis	Cena bez DPH
Etapa 1 – Posouzení stavu bezpečnosti informací	68 400 Kč
Etapa 2 – Provedení identifikace a hodnocení aktiv	171 000 Kč
Etapa 3 – Implementace vybraných bezpečnostních opatření	159 600 Kč
Etapa 4 – Zavedení postupů kontinuity činností	228 000 Kč
Etapa 5 – Provedení interního auditu a přezkoumání SŘBI	68 400 Kč
Celkem	**695 400 Kč**

V případě potřeby je možné čerpat i individuální konzultace v ceně 1 600,- Kč/hod.

Splatnost faktur je 14 dní. Platnost této nabídky je 30 dní.

6. Navrhovaný harmonogram zpracování

Etapa	Název etapy	Termín (měsíce)
Etapa 1	Posouzení stavu bezpečnosti informací	04 – 05/2023
Etapa 2	Provedení identifikace a hodnocení aktiv	06 – 10/2023
Etapa 3	Implementace vybraných bezpečnostních opatření	11/2023 – 02/2024
Etapa 4	Provedení analýzy dopadů a zavedení postupů kontinuity	01 – 05/2024
Etapa 5	Provedení interního auditu a přezkoumání SŘBI	06/2024
Celkem za všechny etapy		04/2023 – 06/2024

Harmonogram je možné upravit po vzájemné dohodě mezi NGSS a úřadem.

7. Naše zkušenosti

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

- Univerzita Karlova
- Česká zemědělská univerzita v Praze
- Fakultní organizace Ostrava
- Fakultní organizace u sv. Anny v Brně
- Hlavní město Praha
- Městská část Praha 2
- Městská část Praha 9
- Městská část Praha 13
- Městská část Praha 18
- Město Český Dub
- Vojenská Zdravotní pojišťovna České republiky
- Ústav molekulární genetiky AV ČR
- Biologické centrum Vestec u Prahy (BIOCEV)
- Siemens s.r.o.
- Lesy České republiky, s.p.
- Globus ČR, k.s.
- Synthos S.A.
- RAMA BOHEMIA a.s.
- Formel D Česká republika s.r.o.
- euroAWK, s.r.o.
- Stokvis Promi, s.r.o.
- Mypa Tools s.r.o.
- KONFORM – Plastic, s.r.o.
- Strojmetal Aluminium Forging, a.s.
- Constellium Extrusions Děčín, s.r.o.
- ARRIVA TRANSPORT ČESKÁ REPUBLIKA a.s.
- TÜV NORD Czech, s.r.o.
- SPORTISIMO s.r.o.
- KOITO CZECH s.r.o.
- Auditor spol. s.r.o.
- Sumi Agro Czech s.r.o.
- Bisnode Česká republika, a.s.
- Datron a.s.
- voestalpine High Performance Metals CZ s.r.o.
- PRIMAPOL-METAL-SPOT s.r.o.

Reference našich klientů

„Společnost NGSS nám poskytuje službu bezpečnostního dohledu nad informačními systémy a odborné GDPR poradenství. Jelikož náplň protíná odpovědnosti Odboru bezpečnosti a Odboru informačních a komunikačních technologií, oceňujeme propojení těchto dvou světů a díky pravidelným společným prezentacím máme přehled o stavu naší bezpečnosti.“

Ing. Luděk Chaloupka, ředitel OIKT, Česká zemědělská univerzita v Praze

„Spolupráce s NGSS nám přináší průběžné informace o našem stavu bezpečnosti informací a o hrozících rizicích. Díky tomu jsme schopni na tato zjištění reagovat včas a předejít nechtěným událostem na úrovni procesní i kybernetické bezpečnosti.“

Ing. Martin Borovička, vedoucí oddělení ICT, Městská část Praha 9

„Spolupráci s NGSS jsme začali na projektu Analýza a implementace GDPR pro naši společnost. Oceňuji především osobní přístup, milou a rychlou komunikaci a perfektní znalost problematiky. Kdykoliv se na konzultanty můžu obrátit a pomohou mi zorientovat se v dané legislativě.“

Naděžda Ševůrková, Finanční ředitel, voestalpine High Performance Metals CZ s.r.o.

„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 analýz dopadu GDPR.“

Ing. Petr Štěpán, vedoucí odboru informatiky, Městská část Praha 2

8. 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, SŘBI a SMS Lead Auditor, 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 **SŘBI** 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 připravení 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**.

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Praha 7, 170 00
sales@ngss.cz | www.ngss.cz