Smlouva o poskytování služeb ZKB

1. SMLUVNÍ STRANY

Objednatel:	**Město Břeclav**
se sídlem:	náměstí T. G. Masaryka 42/3, 690 02 Břeclav
zastoupený:	Ing. Zdeňkem Marešem, vedoucím odboru kanceláře tajemníka
IČO:	00283061
DIČ:	CZ00283061

(dále jen „**Objednatel**“)

a

Poskytovatel	**Next Generation Security Solutions s.r.o.**
se sídlem:	U Uranie 954/18, Holešovice, 170 00 Praha 7
zastoupený:	Mgr. Ondřejem Dedkem, jednatelem
IČO:	062 91 031
DIČ:	CZ06291031
zápis v OR:	spisová značka: C 279627 vedená u Městského soudu v Praze

(dále jen „**Poskytovatel**“)

(Objednatel a Poskytovatel dále také dohromady jen jako „**Smluvní strany**“)

uzavírají v souladu se zákonem č. 89/2012 Sb., občanský zákoník, v platném znění, tuto

Smlouvu o poskytování služeb

(dále jen „**Smlouva**“)

2. ÚVODNÍ USTANOVENÍ

2.1. Účelem této Smlouvy je u Objednatele zavedení požadavků kybernetické bezpečnosti na poskytovatele regulované služby v režimu nižších povinností, které vycházejí z požadavků SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (dále jen „směrnice NIS 2“) a zákona č. 264/2025, o kybernetické bezpečnosti, v platném znění (dále jen „**ZKB**“) a na něj navazujících vyhlášek či jejích návrhů.

2.2. Cílem je zajistit zavedení požadavků kybernetické bezpečnosti dle požadavků směrnice NIS2 do prostředí Objednatele (dále jen „kybernetická bezpečnost“). Požadavky NIS2 budou realizovány zavedením systému řízení bezpečnosti informací v souladu s požadavky aktuálního znění připravované Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, jak je přílohou této Smlouvy, a která by měla být přijata v souvislosti se změnou zákona o kybernetické bezpečnosti ve znění ZKB (dále také „**Vyhláška**“). Smluvní strany se dohodly, že v případě, že by znění Vyhlášky bylo odlišné od znění vyhlášky, která bude přijata a nabyde účinnosti v době trvání Smlouvy, budou Služby poskytnuty, případně upraveny (pokud by už Služby byly poskytnuté) tak, aby odpovídaly znění přijaté a účinné vyhlášky.

2.3. Poskytovatel potvrzuje, že disponuje odbornými znalostmi a zkušenostmi z oblasti kybernetické bezpečnosti, stejně jako dalšími odbornými znalostmi z oblasti IT a bezpečnosti tak, aby byl schopen podpořit Objednatele při zajištění plnění požadavků stanovených příslušnými obecně závaznými právními předpisy (jakož i připravované Vyhlášky).

3. PŘEDMĚT SMLOUVY

3.1. Předmětem Smlouvy je závazek Poskytovatele poskytnout předem sjednané služby z oblasti kybernetické bezpečnosti v souladu s požadavky Vyhlášky, a to konkrétně v rozsahu dle přílohy č. 1 (dále jen „**Služby**").

3.2. Součástí Služeb podle této Smlouvy není/nejsou:

3.2.1. migrace či instalace nových verzí systémů.

3.2.2. dodávka HW vybavení.

3.3. Objednatel se zavazuje zaplatit Poskytovateli za řádně a včas poskytnuté Služby cenu dohodnutou v této Smlouvě, způsobem a ve lhůtě dle této Smlouvy.

3.4. Služby budou poskytovány Objednateli postupně po jednotlivých etapách, jak jsou tyto popsány v příloze této Smlouvy, přičemž se jedná o tyto etapy (uvedené termíny jsou pouze orientační):

3.4.1. Etapa 1: Provedení srovnávací analýzy současného stavu bezpečnosti informací (prosinec 2025 – leden 2026)

3.4.2. Etapa 2: Provedení hodnocení rizik a návrh bezpečnostních opatření (únor 2026 – květen 2026)

3.4.3. Etapa 3 – Podpora při zavedení ISMS (květen 2026 – srpen 2026).

3.5. Služby jsou Poskytovatelem poskytnuté řádně dokončením činností v rámci dané etapy a předáním výstupu z dané etapy Objednateli, jak je tento výstup definovaný v příloze Smlouvy u dané etapy. V případě, že výstup daná etapa nevyžaduje, tj. není tento výstup popsán v příloze Smlouvy, platí, že Služba je v rámci dané etapy poskytnuta splněním poslední z uvedených činností nebo splněním účelu dané etapy. V případě, že má být v jedné etapě zpracováno a předáno více výstupů, je pro účely splnění Služby v dané etapě rozhodný okamžik předání posledního z nich.

3.6. Objednatel bere na vědomí, že Objednatel neodpovídá za nesprávnost nebo neaktuálnost Služby ani výstupu či údaj v něm obsažených, pokud dojde k jakékoliv změně Vyhlášky či souvisejících právních předpisů. Poskytovatel odpovídá výhradně za to, že výstup a Služby budou v souladu s právními předpisy ve znění a ve stavu ke dni poskytnutí Služeb a v případě Vyhlášky ve znění dle přílohy této Smlouvy.

4. CENA A PODMÍNKY POSKYTOVÁNÍ SLUŽEB

4.1. Objednatel se zavazuje uhradit Poskytovateli za provedené Služby odměnu celkem ve výši **357.000,- Kč bez DPH** (dále jen „**Cena**"). Cena je dána součtem dílčích odměn za jednotlivé etapy, jak jsou tyto popsány v příloze.

4.2. Cenu se Objednatel zavazuje uhradit následovně:

4.2.1. Odměnu za Etapu 1 a Etapu 2 ve výši 187.000 Kč bez DPH se zavazuje uhradit Poskytovateli nejpozději do 31.12.2025 bez ohledu na to, jestli v termínu splatnosti budou Služby v uvedených etapách poskytnuty (tj. bude se jednat o zálohovou platbu) a

4.2.2. Odměnu za Etapu 3 se Objednatel zavazuje uhradit po poskytnutí Služeb v rámci této etapy.

4.3. Nárok Poskytovatele na úhradu odměny za jednotlivou etapu vzniká okamžikem poskytnutí Služeb v rámci dané etapy ve smyslu odst. 3.5, a to na základě Poskytovatelem vystaveného daňového dokladu (faktura). Pro vyloučení pochybností Smluvní strany stanoví, že podepsaný akceptační protokol není podmínkou nároku Poskytovatele na odměnu za danou etapu, resp. na Cenu.

4.4. Poskytovatel se zavazuje k vystavení faktury s datem uskutečnění zdanitelného plnění k poslednímu dni měsíce, ve kterém byly Služby poskytnuty, a to nejpozději do 15 kalendářních dnů od data uskutečnění zdanitelného plnění. Splatnost faktury činí 14 dnů. Objednatel se zavazuje uhradit fakturu, která bude zaslána na adresu fakturace@breclav.eu, ve lhůtě splatnosti.

4.5. Ke všem částkám uvedeným v této Smlouvě bude vždy připočtena DPH v zákonné výši.

4.6. Faktura musí splňovat všechny náležitosti daňového dokladu dle příslušných právních předpisů.

4.7. V případě, že Objednatel neuhradí jakoukoliv fakturu dle této Smlouvy, je Objednatel povinen uhradit Poskytovateli nad rámec dlužné částky i smluvní pokutu ve výši 0,1 % z dlužné částky s DPH za každý den takového prodlení.

4.8. Objednatel se zavazuje hradit veškeré platby ve prospěch účtu Poskytovatele uvedeného na faktuře.

5. TERMÍN A MÍSTO PLNĚNÍ

5.1. Poskytovatel se zavazuje zahájit plnění Služeb dle této Smlouvy bez zbytečného odkladu po podpisu Smlouvy oběma Smluvními stranami, nedohodnou-li se Smluvní strany jinak. Služby se Poskytovatel zavazuje poskytnout nejpozději do konce září 2026.

5.2. V případě, že bude Poskytovatel v prodlení s poskytnutím Služeb maximálně o 14 dní oproti termínu dle předchozího odstavce, informuje o tom Objednatele; takové prodlení není důvodem k odstoupení od Smlouvy ze strany Objednatele ani k uplatnění jiných nároků Objednatele.

5.3. Služby v rámci dané etapy jsou poskytnuty ve smyslu odstavce 3.5, pokud jsou všechny výstupy ze všech etap předány Objednateli. Po předání výstupu/výstupů z dané etapy Objednateli je Objednatel oprávněn vznést ke každému písemnému výstupu své připomínky, a to nejpozději do 5 pracovních dnů od předání takového výstupu Objednateli (nebo odeslání e-mailu obsahujícího výstup Objednateli). Pokud v uvedené lhůtě Objednatel nesdělí své připomínky, považuje se výstup za bezvadný a Služby za řádně poskytnuté a Objednatel je povinen podepsat akceptační protokol bez výhrad. Jsou-li k výstupu vzneseny oprávněné připomínky, zapracuje je Poskytovatel do výstupu v přiměřené lhůtě. Předáním výstupu se zapracovanými připomínkami vzniká Objednateli povinnost k podpisu akceptačního protokolu.

5.4. Místem plnění jsou prostory Poskytovatele na adrese U Uranie 954/18, Holešovice, 170 00 Praha 7 nebo sídlo či jiný prostor určený Poskytovatelem.

6. PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

6.1. Každá Smluvní strana se zavazuje informovat bez zbytečného odkladu druhou Smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být významné pro plnění závazků Smluvních stran dle této Smlouvy.

6.2. Poskytovatel je povinen realizovat předmět této Smlouvy řádně, pečlivě a v souladu s obecně závaznými právními předpisy.

6.3. Poskytovatel je povinen poskytovat Služby v dohodnutých termínech.

6.4. Poskytovatel je povinen neprodleně oznámit Objednateli překážky, které mu brání v poskytování Služeb a výkonu dalších činností souvisejících s plněním předmětu Smlouvy.

6.5. Poskytovatel je povinen upozorňovat Objednatele na případnou nevhodnost pokynů Objednatele.

6.6. Poskytovatel je oprávněn k poskytování Služeb využít subdodavatele.

6.7. Poskytovatel neodpovídá za vady Služeb v případě, že byla Služba provedena na základě chybných nebo nedostatečných vstupů, dokumentů či informací Objednatele nebo v případě následné změny těchto informací, podkladů či právních předpisů.

6.8. Poskytovatel neposkytuje na Služby záruku. Objednatel se může domáhat svých nároků z titulu odpovědnosti za vady poskytnutých Služeb, přičemž mu v případě vady poskytnutých Služeb náleží výhradně nárok na opravu nebo doplnění Služeb, resp. písemných výstupů, a to ve smyslu odst. 5.3. Jakékoliv další nároky Smluvní strany výslovně vylučují. Pro vyloučení pochybností Smluvní strany stanoví, že uplynutím lhůty dle odst. 5.3 zaniká právo Objednatele na úpravu, opravu či doplnění písemných výstupů.

7. SOUČINNOST

7.1. Objednatel se touto Smlouvou zavazuje poskytnout Poskytovateli veškerou součinnost pro poskytování Služeb (dále jen „součinnost“), a to součinnost popsanou v této Smlouvě (vč. jejích příloh) nebo součinnost, ke které vyzve Objednatele Poskytovatel, a která je nutná nebo vhodná pro řádné poskytování Služeb.

7.2. Součinnost se Objednatel zavazuje poskytnout neprodleně, nejpozději však ve lhůtě 7 dní ode dne výzvy Poskytovatele, nebude-li dohodnuta jiná lhůta mezi Smluvními stranami. Výzva může být učiněna i prostřednictvím e-mailu.

7.3. V případě prodlení Objednatele s poskytnutím součinnosti nevzniká prodlení na straně Poskytovatele s poskytováním Služeb. O prodlení Objednatele s poskytnutím součinnosti se automaticky prodlužují termíny plnění Poskytovatele dle této Smlouvy.

7.4. V případě prodlení Objednatele s poskytnutím součinnosti poskytne Poskytovatel Objednateli náhradní lhůtu k poskytnutí součinnosti alespoň v délce 10 dní. V případě, že součinnost Objednatel neposkytne ani v náhradní lhůtě, je Poskytovatel oprávněn požadovat a Objednatel je povinen uhradit smluvní pokutu ve výši 500,- Kč za každý den prodlení s poskytnutím součinnosti počínaje prvním dnem následujícím po konci náhradní lhůty. Současně, pokud Objednatel neposkytne Poskytovateli součinnost ani v náhradní lhůtě poskytnuté dle tohoto odstavce, je Poskytovatel oprávněn odstoupit od Smlouvy s účinkem k okamžiku doručení oznámení o odstoupení Objednateli.

7.5. Smluvní pokuta dle tohoto článku je splatná ve lhůtě 7 dní ode dne výzvy k její úhradě. Výzva může být učiněna i prostřednictvím e-mailu.

8. ODPOVĚDNOST

8.1. Poskytovatel odpovídá výlučně za újmu (zejm. škodu) vzniklou v příčinné souvislosti s úmyslným porušením povinností Poskytovatele dle této Smlouvy či dle zákona.

8.2. Povinnosti k náhradě škody se Poskytovatel zprostí, prokáže-li, že mu ve splnění povinnosti ze Smlouvy dočasně nebo trvale zabránila mimořádná nepředvídatelná, neodvratitelná a/nebo nepřekonatelná překážka vzniklá nezávisle na jeho vůli (vyšší moc). Poskytovatel se však povinnosti nahradit škodu nezprostí, pokud šlo o překážku, která (i) vznikla z jeho osobních poměrů, (ii) vznikla až v době, kdy byl s plněním smluvené povinnosti v prodlení, nebo (iii) kterou byl podle Smlouvy povinen překonat. Smluvní strany výslovně stanoví, že důvodem ke zproštění odpovědnosti Poskytovatele dle tohoto odstavce je např. dopravní nehoda Poskytovatele nebo některé z osob poskytující služby za Poskytovatele, výpadek elektrické energie nebo internetové konektivity nezávislý na vůli Poskytovatele apod. Pokud vznikne Objednateli újma v důsledku

těchto či obdobných situací, zprostí se Poskytovatel k náhradě takto vzniklé škody.

8.3. V každém případě je odpovědnost Poskytovatele omezena maximálně do výše 2.000.000,-Kč za dobu trvání Smlouvy, a to bez ohledu na to, jestli bude této částky dosaženo jedním nárokem nebo několika nároky v součtu. Pro odstranění pochybností se Objednatel veškerých nároků nad částku dle předchozí věty výslovně vzdává.

8.4. Smluvní strany si výslovně sjednávají, že se neaplikuje § 2952 občanského zákoníku. Strany se dohodly na tom, že se bude hradit pouze skutečná škoda, nikoliv ušlý zisk nebo jakékoli jiné nepřímé či nemajetkové újmy.

8.5. Poskytovatel neodpovídá za škodu, která vznikla v důsledku věcně nesprávného nebo jinak chybného nebo neúplného zadání, které obdržel od Objednatele.

8.6. Objednatel není oprávněn jednostranně započítat své pohledávky za Poskytovatelem vůči pohledávkám Poskytovatele za Objednatelem.

8.7. Případné obchodní zvyklosti, týkající se plnění této Smlouvy, nemají přednost před ujednáními v této Smlouvě, ani před ustanoveními zákona, byť by tato ustanovení neměla donucující účinky.

8.8. Smluvní strany se dohodly, že na vztah založený touto Smlouvou se nepoužijí §§ 1793 až 1795 občanského zákoníku.

9. LICENČNÍ UJEDNÁNÍ

9.1. Bude-li součástí Služeb nebo výsledkem činnosti Poskytovatele prováděné dle této Smlouvy autorské dílo podle zákona č. 121/2001 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „**autorské dílo**"), nabývá Objednatel dnem poskytnutí autorského díla Objednateli k užívání nevýhradní právo užít takovéto autorské dílo, avšak jen za účelem naplnění účelu vyplývajícího z této Smlouvy, a to po celou dobu trvání autorského práva k autorskému dílu bez omezení rozsahu množstevního, technologického, teritoriálního.

9.2. V případě, že dojde k úpravám nebo zásahům do autorského díla, nenese Poskytovatel za provedené změny jakoukoliv odpovědnost.

10. OCHRANA DŮVĚRNÝCH INFORMACÍ

10.1. Smluvní strany jsou si vědomy toho, že v rámci plnění Smlouvy:

- si mohou vzájemně úmyslně nebo i opominutím poskytnout informace, které budou považovány za důvěrné (dále jen „**důvěrné informace**"),
- mohou jejich zaměstnanci nebo třetí osoby získat vědomou činností druhé Smluvní strany nebo i jejím opominutím či jinak přístup k důvěrným informacím druhé Smluvní strany.

10.2. Předávající strana zůstává výlučným nositelem práv k veškerým důvěrným informacím a přijímající strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace, zejména bude o nich zachovávat mlčenlivost a zajistí, aby je ve stejném rozsahu zachovávaly i jiné osoby, kterým je poskytne v souladu s touto Smlouvou. S výjimkou plnění této Smlouvy se obě strany zavazují neduplikovat žádným způsobem důvěrné informace druhé strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohla být tato Smlouva řádně plněna. V případě plnění této Smlouvy se smluvní strany zavazují činit tak vždy jen v nezbytně nutném rozsahu. Obě smluvní strany se zároveň zavazují nepoužít důvěrné informace druhé strany jinak než za účelem plnění Smlouvy.

10.3. Nedohodnou-li se smluvní strany výslovně jinak, považují se za důvěrné implicitně všechny

informace, které jsou a nebo by mohly být součástí obchodního tajemství, tj. zejména, nikoliv však výlučně popisy nebo části popisů technologických procesů a vzorců, technických vzorců a technického know-how, informace o provozních metodách, procedurách a pracovních postupech, obchodní nebo marketingové plány, koncepce a strategie nebo jejich části, nabídky, kontrakty, smlouvy, dohody nebo jiná ujednání s třetími stranami, informace o výsledcích hospodaření, o vztazích s obchodními partnery, o pracovněprávních otázkách a všechny další informace, jejichž zveřejnění přijímající stranou by předávající straně mohlo způsobit škodu, nebo jejichž zveřejnění předávající strana výslovně zakázala. Tímto ustanovením nejsou dotčena práva a povinnosti smluvních stran dle čl. 9 této Smlouvy.

10.4. Poskytovatel se zavazuje dodržovat postupy zásad ochrany osobních údajů a listovních tajemství, ve smyslu zákona č. 110/2019 Sb., o ochraně osobních údajů a nařízení GDPR.

10.5. Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:

- se staly veřejně známými, aniž by to zavinila záměrně či opominutím přijímající strana,
- měla přijímající strana legálně k dispozici před uzavřením Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy o ochraně informací, nebo pokud nejsou chráněny ze zákona,
- jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany,

10.6. Ustanovení tohoto článku není dotčeno ukončením této Smlouvy z jakéhokoliv důvodu.

11. KOMUNIKACE SMLUVNÍCH STRAN

11.1. Veškerá komunikace mezi Smluvními stranami bude probíhat prostřednictvím oprávněných osob, pověřených zaměstnanců nebo statutárních orgánů Smluvních stran.

11.2. Každá ze Smluvních stran jmenuje oprávněnou osobu. Oprávněné osoby budou zastupovat Smluvní stranu v záležitostech souvisejících s plněním této Smlouvy. Není-li však stanoveno jinak, nejsou oprávněné osoby oprávněny ke změnám Smlouvy ani jejímu ukončení, ledaže získají speciální plnou moc.

11.3. Každá Smluvní strana je oprávněna změnit jí jmenovanou oprávněnou osobu, resp. jejího zástupce, je však povinna na takovou změnu druhou Smluvní stranu písemně upozornit (postačí forma e-mailové komunikace), nevyplývá-li tato změna z veřejné části obchodního rejstříku.

11.4. Kontaktní osoby:

Oprávněnou osobou na straně Objednatele je:

[redacted]

Oprávněné osoby na straně Poskytovatele budou stanoveny a oznámeny Objednateli bez zbytečného odkladu po zahájení plnění Služeb.

11.5. Vymezení kontaktních osob dle předchozího odstavce nemá vliv na možnost statutárních zástupců zapsaných v obchodním rejstříku zastupovat Smluvní strany v neomezeném rozsahu.

11.6. Komunikace mezi Smluvními stranami může probíhat prostřednictvím e-mailu mezi oprávněnými osobami nebo jinak písemně, není-li ve Smlouvě stanoveno jinak. Komunikace týkající se uplatnění vad, odstoupení od Smlouvy nebo jiného ukončení Smlouvy, jakož i uplatnění nároku na smluvní pokutu nebo úroku z prodlení musí být provedena výlučně písemně v listinné podobě nebo prostřednictvím datové schránky.

12. ÚČINNOST A TRVÁNÍ SMLOUVY

12.1. Tato Smlouva se uzavírá na dobu určitou, a to do doby řádného poskytnutí Služeb. Ukončení Smlouvy nemá vliv na trvání ustanovení, která mají ze své podstaty trvat i po skončení Smlouvy (právo na náhradu škody, povinnost mlčenlivosti, práva na smluvní pokuty apod.).

12.2. Tuto Smlouvu lze ukončit:

- dohodou Smluvních stran, jejíž součástí je i vypořádání vzájemných závazků a pohledávek,
- odstoupením od Smlouvy v případech uvedených v této Smlouvě nebo ze zákonem uvedených důvodů.

12.3. Objednatel je oprávněn odstoupit od této Smlouvy s účinkem k okamžiku doručení oznámení o odstoupení Poskytovateli v těchto případech:

- vstoupí-li Poskytovatel do likvidace,
- na majetek Poskytovatele bude prohlášen úpadek, Poskytovatel sám podá návrh na zahájení insolvenčního řízení nebo insolvenční návrh bude zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení,
- pozbude-li Poskytovatel jakékoliv oprávnění vyžadované právními předpisy pro poskytování Služeb,
- je-li Poskytovatel v prodlení s poskytnutím služeb déle než 14 dnů ve smyslu čl. 5.2 této Smlouvy.

12.4. Poskytovatel je oprávněn odstoupit od této Smlouvy s účinkem k okamžiku doručení oznámení o odstoupení Objednateli v těchto případech:

- je-li Objednatel v prodlení z kteroukoliv z plateb déle než 15 dní a toto nenapraví ani v náhradní přiměřené lhůtě od doručení písemné upomínky Poskytovatele;
- neposkytuje-li Objednatel potřebnou součinnost, a to ani poté, co byl Poskytovatelem k poskytnutí této součinnosti alespoň dvakrát písemně vyzván.

12.5. Odstoupením zanikají ke dni odstoupení práva a povinnosti stran z této Smlouvy ohledně části závazku nesplněné k tomuto dni. Odstoupení od Smlouvy se nedotýká práv a povinností pro splněnou část závazku a dále ustanovení, která by vzhledem ke své povaze trvala i po ukončení Smlouvy, zejména ustanovení o náhradě škody a ochraně důvěrných informací.

13. ŘEŠENÍ SPORŮ

13.1. Veškerá vzájemná práva a povinnosti Poskytovatele a Objednatele vyplývající z této Smlouvy se budou řídit právem České republiky. Veškeré spory, které vzniknou z uzavřených smluv nebo v souvislosti s nimi a které se nepodaří vyřešit přednostně smírnou cestou, budou rozhodovány obecným soudem Objednatele v souladu se zákonem č. 99/1963 Sb., občanským soudním řádem, ve znění pozdějších předpisů.

14. ZÁVĚREČNÁ USTANOVENÍ

14.1. Tato Smlouva a právní vztahy vzniklé z této Smlouvy se řídí českým právním řádem, zejména občanským zákoníkem.

14.2. Tuto Smlouvu lze měnit, doplňovat nebo rušit pouze písemně, není-li v této Smlouvě uvedeno jinak nebo nedohodnou-li se jinak Smluvní strany.

14.3. Práva a povinnosti smluvních stran z této Smlouvy přecházejí na jejich právní nástupce.

14.4. V případě, že se některé ustanovení této Smlouvy stane neplatným či nevymahatelným, zůstávají

ostatní ustanovení i nadále v platnosti, ledaže právní předpis stanoví jinak. Smluvní strany se zavazují takové neplatné či nevymahatelné ustanovení nahradit jiným, odpovídajícím účelu ustanovení neplatného či nevymahatelného.

14.5. Tato Smlouva je vyhotovena v elektronické podobě, každá ze stran obdrží oboustranně podepsaný elektronický originál této Smlouvy.

14.6. Tato Smlouva nabývá platnosti dnem podpisu Smlouvy oběma Smluvními stranami a účinnosti dnem zveřejnění v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Smluvní strany se dohodly, že uveřejnění Smlouvy dle zákona o registru smluv zajistí zasláním správci registru smluv Objednatel. Smluvní strany vysloveně souhlasí se zveřejněním této Smlouvy v jejím plném rozsahu, včetně příloh a dodatků v registru smluv vedeném Ministerstvem vnitra ve smyslu zákona o registru smluv.

14.7. V případě rozporu této Smlouvy a příloh má přednost znění Smlouvy.

14.8. Nedílnou součástí této Smlouvy jsou tyto přílohy:

Příloha 1 – Nabídka na: „PODPORU PŘI ZAVEDENÍ POŽADAVKŮ NA POSKYTOVATELE REGULOVANÉ SLUŽBY V REŽIMU NIŽŠÍCH POVINNOSTÍ“

Příloha 2 – Aktuální znění navrhované Vyhlášky, podle které postupuje Poskytovatel

NA DŮKAZ SVÉHO SOUHLASU S OBSAHEM TÉTO SMLOUVY K NÍ SMLUVNÍ STRANY PŘIPOJILY SVÉ UZNÁVANÉ ELEKTRONICKÉ PODPISY DLE ZÁKONA Č. 297/2016 SB., O SLUŽBÁCH VYTVÁŘEJÍCÍCH DŮVĚRU PRO ELEKTRONICKÉ TRANSAKCE, VE ZNĚNÍPOZDĚJŠÍCH PŘEDPISŮ.

Ing. Zdeněk Mareš

Digitálně podepsal Ing. Zdeněk Mareš
Datum: 2025.11.06 07:00:49 +01'00'

Ondřej Dedek

Digitálně podepsal Ondřej Dedek
Datum: 2025.11.13 11:40:32 +01'00'

AKTUALIZOVANÁ NABÍDKA NA:

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

MĚSTO BŘECLAV

V PRAZE DNE:

17. ZÁŘÍ 2025

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:	Mgr. Ondřej Dedek, jednatel
Webové stránky:	www.ngss.cz
Kontaktní osoby:	[redacted]

2. Obsah

Město Břeclav

Náměstí T. G. Masaryka 42/3

690 02 Břeclav

Vážený pane Hlavňovský,

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

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“). Zavedení kybernetické bezpečnosti naváže na provedenou srovnávací analýzu stavu bezpečnosti provedenou v Břeclavi. Nabízíme Vám realizovat práce zahrnující realizaci zavedení potřebných požadavků:

1. **Provedení hodnocení aktiv a přijetí bezpečnostních opatření** k určení možných rizik a návrhu jejich pokrytí.
2. **Implementace vybraných bezpečnostních opatření** zahrnuje návrh postupů, jejich popis v bezpečnostní dokumentaci a rozpracování do návrhu záznamů systému řízení bezpečnosti informací včetně ralizace základních postupů zajištění kontinuity činností..

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

S pozdravem
Martin Juhás, 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:

- 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** (audit/kontrola nebude v rámci nabízených služeb realizován).

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

Zavedení kybernetické bezpečnosti naváže na provedenou srovnávací analýzu stavu bezpečnosti provedenou v Břeclavi.

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.

Pro porovnání stavu bezpečnosti budou použity vybrané požadavky na poskytovatele regulované služby v režimu nižších povinností.

Posouzení stavu bude provedeno na úřadě Břeclav.

Posouzení stavu bezpečnosti informací ověří úroveň zabezpečení informací zpracovávaných společností. **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 společnosti a prostor, kde jsou informace zpracovávány a ukládány spolu s prohlídkou serveroven a technologických místností,
- vypracování závěrečné zprávy, která bude předána k připomínkám společnosti.

Jednotlivé oblasti jsou rozděleny následovně:

- Stanovení rozsahu řízení kybernetické bezpečnosti
- Zajišťování kybernetické bezpečnosti,
- Bezpečnostní opatření,
- Povinnosti vrcholného vedení,
- Bezpečnost lidských zdrojů,
- Řízení kontinuity činností,
- Řízení přístupu,
- Řízení identit a jejich oprávnění,
- Detekce a zaznamenávání kybernetických bezpečnostních událostí,
- Řešení kybernetických bezpečnostních incidentů,
- Bezpečnost komunikačních sítí,
- Aplikační bezpečnost,
- Kryptografické algoritmy,
- Stanovení významnosti dopadu kybernetického bezpečnostního incidentu,

- Hlášení kybernetických bezpečnostních incidentů,
- Zvládání kybernetických bezpečnostních incidentů,
- Informační povinnost,
- Protiopatření,
- Výstraha,
- Speciální úprava předání informací a dat od dodavatele,
- Prověřování rizik spojených s dodavatelem,
- Omezení rizik spojených s dodavatelem.

Výše uvedené oblasti mohou být upraveny na základě úpravy transpoziční legislativy k NIS2.

Výstupy:

- **Zprava z posouzení stavu bezpečnosti informací úřadu Břeclav 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 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 14 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.

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,
- postupy zajištění kontinuity činností včetně zpracování plánu obnovy,
- 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,

- zjištění ochrany osobních údajů a autorského práva,

- 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:

Návrh a hierarchie dokumentů je následující:

Typ dokumentu	Návrh dokumentu úřadu
Vrcholový dokument	• **Politika systému zajišťování minimální úrovně kybernetické bezpečnosti**
Dokumenty navazující na politiku	• **Směrnice řízení kybernetické bezpečnosti**
Dokumentace pro uživatele	• **Bezpečnostní uživatelská směrnice**

Vzory potřebných **záznamů** a další dokumentace s důrazem na vzory dokumentů **Plány obnovy, Závěrečná zpráva o kybernetickém bezpečnostním incidentu, Evidence nepodporovaných technických aktiv, Topologie infrastruktury., Segmentace infrastruktury, Přehled technických aktiv zejména síťových zařízení, aktivních prvků, koncových zařízení a serverů a kkntakty na osoby pověřené technickou a systémovou podporou.**

3.4. Etapa 4: Vyhodnocení účinnosti zavedených bezpečnostních opatření – volitelná část projektu

Cílem etapy je ověřit zavedení bezpečnostních procesů a opatření, včetně aktualizace přehledu bezpečnostních opatření.

V této etapě zavedení SŘBI se provede kontrola zajištění minimální úrovně kybernetické bezpečnosti cestou provedení kontroly odstranění neshod zjištěných při srovnávací analýze.

V rámci etapy je vhodné provést:

- provedení **hodnocení stavu zajištění minimální úrovně kybernetické bezpečnosti** :
  - příprava vyhodnocení – příprava podkladů, upřesnění rámce a průběhu hodnocení stavu a příprava jeho účastníků na straně úřadu,
  - provedení hodnocení – shromáždění relevantních informací z oblastí kybernetické bezpečnosti a provedení rozhovorů ke zjištění aktuálního stavu kybernetické bezpečnosti,
  - zpracování zprávy z hodnocení – bude zjištěna úroveň shody aktuálního stavu zajištění minimální úrovně kybernetické bezpečnosti u úřadu.
- Zpracování **dokumentovaného vyhodnocení účinnosti zavedených bezpečnostních opatření**. Cílem je přezkoumat zajištění minimální úrovně kybernetické bezpečnosti a předložit ho vedení úřadu. Přezkoumání bude zpracováno pracovníky úřadu za součinnosti dodavatele ve struktuře popsané ve výstupech.
- Aktualizace **Plánu zavedení bezpečnostních opatření**, které se upraví na základě výsledků hodnocení stavu kybernetické bezpečnosti.

Výstupy:

- **Zpráva z hodnocení stavu zajištění minimální úrovně kybernetické bezpečnosti úřadu** obsahující shrnutí zjištění, zhodnocení stavu bezpečnosti informací s uvedením neshod vůči požadovanému stavu;
- **Vyhodnocení účinnosti zavedených bezpečnostních opatření** obsahující vyhodnocení stavu SŘBI v předepsaném formátu:
  - Shrnutí vyhodnocení stavu bezpečnostních opatření za uplynulý rok,
  - posouzení stavu plánu zavádění bezpečnostních opatřeních,
  - identifikace možných změn a okolností, které mohou mít vliv na zajišťování minimální úrovně kybernetické bezpečnosti v budoucím období,
  - posouzení dopadů kybernetických bezpečnostních incidentů na poskytované služby a kybernetickou bezpečnost,
  - doporučení potřebných rozhodnutí, bezpečnostních opatření a cílů na následující rokí.
- Aktualizovaný **Plán zavedení bezpečnostních opatření.**

4. Nabídková cena

Popis	Cena bez DPH
Etapa 1 – Posouzení stavu bezpečnosti informací	68.000,- Kč
Etapa 2 – Provedení identifikace a hodnocení aktiv	119.000,- Kč
Etapa 3 – Implementace vybraných bezpečnostních opatření	170.000,- Kč
Celkem	**357.000,- Kč**

Volitelná část projektu:

Etapa 4 – Provedení interního auditu a přezkoumání SŘBI	85.000,-

V případě potřeby je možné čerpat i individuální konzultace v ceně 1 800,- Kč/hod.

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

5. Navrhovaný harmonogram zpracování

Zahájení	Ukončení	Etapa	Název etapy
prosinec 25/ leden 26	únor 26	Etapa 1	Provedení srovnávací analýzy současného stavu bezpečnosti informací
únor 26	květen 26	Etapa 2	Provedení hodnocení rizik a návrh bezpečnostních opatření
květen 26	srpen 26	Etapa 3	Podpora při zavedení ISMS
srpen 26	září 26	Etapa 4	Podpora při provedení interního auditu
Celkem ve všech etapách			12/2025-01/2026 – 09/2026

Harmonogram je možné upravit po vzájemné dohodě mezi NGSS a úřadem. Týká se zejména etapy 1, kdy je možné s pracemi začít ve 2.pol. prosince 2025.

6. Naše zkušenosti

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

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

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

Reference od 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."

Bc. Andrea Svobodová, Manažer kvality, 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 získaní certifikace."

Filip Pěgřím, Sage Automotive Interiors, Strakonice Fabrics, s.r.o., Manažer bezpečnosti informací a maintenance & investition manager

„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."

Ing. Jaroslav Bureš, MBA, Předseda představenstva, Liberecká IS, a.s.

„Díky spolupráci se společností NGSS, jsme detailně zhodnotili stav bezpečnosti informací v kyberprostředí 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 vděčni za profesionální přístup a spolehlivou a odbornou pomoc."

Tomáš Plesník, Vedoucí pracoviště – Divize IT služeb, Ústav výpočetní techniky Masarykovy univerzity (ÚVT 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 analýz dopadu GDPR."

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

7. 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.**

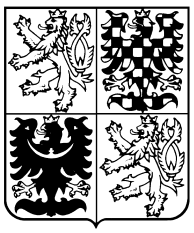
Dalším významným pilířem našich služeb je služba **SOC** (security operations center), která zahrnuje mj. role pro **SŘBI** podporu a poradenství, outsourcing role pověřence pro ochranu osobních údajů (**DPO** – Data Privacy Officer), produktově nezávislou analyticko-operativní schopnost při řešení incidentů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

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



Sbírka zákonů a mezinárodních smluv

ČESKÁ REPUBLIKA

Zpřístupněna dne 14. října 2025

Vyhláška č. 410/2025 Sb.

Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností

410

VYHLÁŠKA

ze dne 26. září 2025

o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 13 odst. 3 a § 15 odst. 3 zákona č. 264/2025 Sb., o kybernetické bezpečnosti, (dále jen „zákon“):

ČÁST PRVNÍ

ÚVODNÍ USTANOVENÍ

§ 1

Předmět úpravy

Tato vyhláška zapracovává příslušný předpis Evropské unie[1]) a pro poskytovatele regulované služby v režimu nižších povinností (dále jen „povinná osoba“) upravuje

a) obsah, způsob zavádění a provádění bezpečnostních opatření a

b) stanovení významnosti dopadu kybernetického bezpečnostního incidentu.

§ 2

Vymezení pojmů

Pro účely této vyhlášky se rozumí

a) uživatelem fyzická nebo právnická osoba anebo orgán veřejné moci, který využívá aktiva,

b) privilegovaným uživatelem uživatel nebo jiná osoba, jejíž činnost na technickém aktivu může mít významný dopad na bezpečnost regulované služby,

c) administrátorem privilegovaný uživatel nebo osoba zajišťující správu, provoz, užívání, údržbu a bezpečnost technického aktiva,

d) bezpečnostní politikou soubor zásad a pravidel, která určují způsob zajištění ochrany aktiv.

ČÁST DRUHÁ

BEZPEČNOSTNÍ OPATŘENÍ

§ 3

Systém zajišťování minimální kybernetické bezpečnosti

(1) Povinná osoba při zajišťování kybernetické bezpečnosti

a) zavede a provádí bezpečnostní opatření, která jsou přiměřená bezpečnostním potřebám, a

b) zavede a provádí alespoň bezpečnostní opatření podle odstavců 2 až 6, § 4 až 6 a § 10.

(2) Povinná osoba

a) stanoví přehled bezpečnostních opatření podle přílohy č. 1 k této vyhlášce, který obsahuje přehled všech bezpečnostních opatření, která

1. byla povinnou osobou zavedena, včetně popisu jejich zavedení,
2. budou povinnou osobou zavedena, včetně termínů pro jejich zavedení, priority jejich zavedení a určení osoby odpovědné za jejich zavedení, a
3. nebyla zavedena, včetně odůvodnění jejich nezavedení,

b) provede a dokumentuje alespoň jednou ročně aktualizaci přehledu bezpečnostních opatření, včetně vyhodnocení účinnosti zavedených bezpečnostních opatření,

c) uchovává jednotlivé přehledy bezpečnostních opatření a jejich aktualizace alespoň po dobu 4 let.

(3) Povinná osoba v rámci řízení bezpečnostní politiky a bezpečnostní dokumentace

a) stanoví bezpečnostní politiku a bezpečnostní dokumentaci k bezpečnostním opatřením požadovaným touto vyhláškou,

b) pravidelně přezkoumává a aktualizuje pravidla a postupy stanovené v bezpečnostní politice a bezpečnostní dokumentaci a

c) vynucuje dodržování pravidel a postupů stanovených v bezpečnostní politice a bezpečnostní dokumentaci.

(4) Povinná osoba v rámci řízení aktiv stanoví pravidla pro používání a manipulaci technických aktiv.

(5) Povinná osoba při uzavírání smlouvy s dodavatelem do stanoveného rozsahu podle § 12 zákona zohlední hrozby a zranitelnosti spojené s tímto dodavatelem, celkovou kvalitu produktů a postupů v oblasti kybernetické bezpečnosti tohoto dodavatele, včetně postupů bezpečného vývoje a na základě toho zajistí, aby smlouvy s tímto dodavatelem obsahovaly relevantní požadavky na smluvní ujednaní uvedené v příloze č. 2 k této vyhlášce.

(6) Povinná osoba v souvislosti s plánovanou akvizicí, vývojem a údržbou technických aktiv stanoví bezpečnostní požadavky v oblasti kybernetické bezpečnosti a vymáhá jejich dodržování, přičemž vychází z požadavků na bezpečnostní opatření podle této vyhlášky.

§ 4

Požadavky na vrcholné vedení

Statutární orgán povinné osoby nebo jiná osoba anebo skupina osob v obdobném řídícím postavení povinné osoby (dále jen „vrcholné vedení“) s ohledem na zajišťování minimální kybernetické bezpečnosti

a) určí osobu pověřenou kybernetickou bezpečností, které svěří pravomoci potřebné k řízení a rozvoji kybernetické bezpečnosti, dohledu nad stavem kybernetické bezpečnosti a komunikaci s vrcholným vedením, přičemž pro výkon této činnosti
   1. absolvuje bez zbytečného odkladu odborné školení podle § 5 odst. 2 písm. d), nebo
   2. prokáže odbornou znalost v kybernetické bezpečnosti,
b) absolvuje prokazatelně školení podle § 5 odst. 2 písm. a),
c) zajistí dostupnost zdrojů potřebných pro zajišťování kybernetické bezpečnosti v souladu s přehledem bezpečnostních opatření,
d) se prokazatelně seznamuje se stavem plnění bezpečnostních opatření uvedeným v přehledu bezpečnostních opatření podle § 3 odst. 2 písm. a),
e) prosazuje neustálé zlepšování zajišťování kybernetické bezpečnosti a za tímto účelem podporuje osobu pověřenou kybernetickou bezpečností a jiné relevantní osoby a
f) stanoví prioritu obnovy primárních aktiv.

§ 5

Bezpečnost lidských zdrojů

(1) Povinná osoba v rámci bezpečnosti lidských zdrojů
   a) stanoví politiku bezpečného chování uživatelů, v jejímž rámci zohledňuje relevantní témata uvedená v příloze č. 3 k této vyhlášce,
   b) stanoví pravidla rozvoje bezpečnostního povědomí vrcholného vedení, uživatelů, administrátorů a osoby pověřené kybernetickou bezpečností, včetně pravidel pro tvorbu hesel,
   c) zajistí kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osoby pověřené kybernetickou bezpečností a
   d) stanoví pravidla a postupy pro řešení případů porušení bezpečnostní politiky.

(2) Povinná osoba v souladu s pravidly rozvoje bezpečnostního povědomí zajistí
   a) poučení vrcholného vedení o jeho povinnostech a o bezpečnostní politice, zejména v oblasti zajišťování kybernetické bezpečnosti, formou vstupních a pravidelných školení,
   b) vstupní školení v oblasti kybernetické bezpečnosti,
   c) pravidelná školení v oblasti kybernetické bezpečnosti a
   d) potřebná odborná teoretická i praktická školení administrátorů a osoby pověřené kybernetickou bezpečností v souladu s jejich pracovní náplní.

(3) Povinná osoba vede přehledy o provedených školeních a seznamy školených osob podle odstavce 2.

§ 6

Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

a) stanoví prioritu technických aktiv, pořadí a postupy jejich obnovy a zohlední přitom stanovenou prioritu relevantního primárního aktiva podle § 4 písm. f),

b) stanoví povinnosti a odpovědnost konkrétních osob za jednotlivé činnosti pro zajištění kontinuity činností a k obnově podle písmene a) a

c) vytváří pravidelné zálohy informací, dat, konfigurací a nastavení technických aktiv nezbytných zejména pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu.

§ 7

Řízení přístupu

(1) Povinná osoba řídí přístup k aktivům a v rámci něj

a) přidělí každému uživateli a administrátorovi přistupujícímu k aktivům přístupová práva a oprávnění na úroveň nezbytně nutnou k výkonu jejich práce a jedinečný identifikátor daného typu účtu, přičemž od sebe odděluje uživatelské a administrátorské účty jedné osoby,

b) řídí identifikátory, přístupová práva a oprávnění účtů technických aktiv,

c) zavádí bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení a jiných obdobných technických aktiv, popřípadě i bezpečnostní opatření spojená s využitím technických aktiv, která povinná osoba nemá ve své správě,

d) provádí pravidelné přezkoumání nastavení veškerých přístupových práv a oprávnění,

e) zajistí bezodkladné odebrání nebo změnu přístupových práv a oprávnění při změně pozice nebo zařazení uživatelů nebo administrátorů a

f) zajistí deaktivaci účtu a bezodkladné odebrání nebo změnu přístupových práv a oprávnění při ukončení nebo změně smluvního vztahu, na jehož základě došlo ke zřízení přístupu k aktivům.

(2) Povinná osoba v rámci zajištění fyzické bezpečnosti zamezí neoprávněnému přístupu ke svým aktivům a předchází poškození, odcizení, zneužití aktiv, neoprávněným zásahům do nich a narušení bezpečnosti poskytování regulované služby.

§ 8

Řízení identit a jejich oprávnění

(1) Povinná osoba pro řízení identit, přístupových práv a oprávnění používá nástroj, který zajišťuje

a) řízení počtu možných neúspěšných pokusů o přihlášení,

b) opětovné ověření identity po stanovené době nečinnosti,

c) odolnost uložených a přenášených autentizačních údajů a

d) řízení přístupových práv, oprávnění pro čtení a zápis informací a dat a změnu oprávnění.

(2) Povinná osoba pro ověření identity administrátorů, uživatelů a technických aktiv využívá autentizační mechanismus, který je založený na vícefaktorové autentizaci s alespoň dvěma různými typy faktorů, nebo využívá autentizační mechanismus, který je založen na aktuálně odolné kontinuální autentizaci založené na modelu nulové důvěry.

(3) Povinná osoba do doby využívání autentizačního mechanismu podle odstavce 2 využívá autentizaci pomocí kryptografických klíčů nebo certifikátů.

(4) Povinná osoba do doby využívání autentizačního mechanismu podle odstavce 3 využívá nástroj založený na autentizaci pomocí identifikátoru účtu a hesla, kdy tento nástroj musí vynucovat pravidla

a) délky hesla alespoň

1. 12 znaků pro účty uživatelů,
2. 17 znaků pro účty administrátorů,
3. 22 znaků pro účty technických aktiv,

b) bezodkladné změny výchozího hesla pro ověření identity technických aktiv, přičemž nové heslo musí být vytvořeno náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků,

c) neomezující použití malých a velkých písmen, číslic a speciálních znaků,

d) povinné změny hesla v intervalu alespoň jednou za 18 měsíců a

e) neumožňující uživatelům a administrátorům

1. zvolit si jednoduchá a často používaná hesla,
2. tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacích jmen, adres elektronické pošty, názvů systémů nebo obdobným způsobem a
3. opětovného použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel.

(5) Povinná osoba při řízení identit dále zajistí

a) důvěrnost při vytváření výchozích autentizačních údajů a při obnově přístupu,

b) změnu výchozího hesla nebo hesla sloužícího k obnově přístupu po jeho prvním použití,

c) zneplatnění hesla nebo identifikátoru sloužícího k obnově přístupu nejpozději do 24 hodin od jeho vytvoření,

d) bezodkladnou změnu přístupového hesla v případě důvodného podezření na jeho kompromitaci a

e) zabezpečení administrátorských účtů technických aktiv zejména určených pro případ obnovy po kybernetickém bezpečnostním incidentu a využívá tyto účty pouze v nezbytně nutných případech.

§ 9

Detekce a zaznamenávání kybernetických bezpečnostních událostí

(1) Povinná osoba při detekci kybernetických bezpečnostních událostí zajistí

a) ověření a kontrolu přenášených dat na perimetru komunikační sítě, včetně blokování nežádoucí komunikace,

b) použití nástroje pro nepřetržitou a automatickou ochranu před škodlivým kódem na technických aktivech, zejména na

1. serverech a
2. koncových stanicích,

c) řízení automatického spouštění obsahu, zejména u vyměnitelných zařízení a datových nosičů,

d) nepřetržité poskytování informací o relevantních detekovaných kybernetických bezpečnostních událostech a včasné varování relevantních osob a

e) pravidelnou a bezodkladnou aktualizaci nástrojů pro nepřetržitou a automatickou ochranu před škodlivým kódem a dalších detekčních nástrojů a jejich pravidel.

(2) Povinná osoba za účelem detekce kybernetických bezpečnostních událostí zaznamenává

a) bezpečnostní a relevantní provozní události detekované podle odstavce 1 a bezpečnostní a relevantní provozní události technických aktiv na základě svých bezpečnostních potřeb a

b) u událostí podle písmene a) následující informace o události:

1. datum a čas, včetně specifikace časového pásma,
2. typ činnosti,
3. jednoznačnou identifikaci technického aktiva a identifikaci účtu původce a
4. úspěšnost nebo neúspěšnost činnosti.

(3) Povinná osoba uchovává záznamy bezpečnostních a relevantních provozních událostí po dobu, kterou si stanoví na základě svých bezpečnostních potřeb.

§ 10

Řešení kybernetických bezpečnostních incidentů

Povinná osoba při řešení kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů

a) zajistí, že uživatelé, administrátoři, osoby pověřené kybernetickou bezpečností a další zaměstnanci budou oznamovat neobvyklé chování technických aktiv a podezření na jakékoliv zranitelnosti,

b) vytvoří metodiku pro posuzování kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, včetně posuzování významnosti dopadu kybernetického bezpečnostního incidentu v souladu s § 14,

c) zajistí detekci kybernetických bezpečnostních událostí,

d) zajistí posuzování kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů v souladu s metodikou podle písmene b),

e) zajistí hlášení kybernetického bezpečnostního incidentu s významným dopadem podle § 15 zákona,

f) zajistí vytvoření závěrečné zprávy o vyřešení kybernetického bezpečnostního incidentu s významným dopadem podle § 16 zákona.

§ 11

Bezpečnost komunikačních sítí

Povinná osoba pro ochranu bezpečnosti komunikační sítě, a to zejména jejího síťového perimetru,

a) zajistí segmentaci komunikační sítě, včetně oddělení provozního a zálohovacího prostředí,

b) omezí odchozí a příchozí komunikaci na perimetru komunikační sítě na dobu nezbytně nutnou pro řádné zajištění poskytování regulované služby,

c) užívá aktuálně odolné a bezpečné komunikační protokoly,

d) v případě užití vzdáleného připojení do interní komunikační sítě nebo vzdálené správy technických aktiv regulované služby

1. omezí tato připojení na nezbytně nutná,

2. zavede bezpečnostní opatření, která zajistí důvěrnost a integritu těchto vzdálených připojení a vzdálené správy, a

3. má přehled o uživatelích a administrátorech, kteří tato vzdálená připojení nebo vzdálenou správu užívají.

§ 12

Aplikační bezpečnost

Povinná osoba při zajišťování aplikační bezpečnosti regulované služby

a) zajistí bezodkladné aplikování schválených bezpečnostních aktualizací vydaných pro technická aktiva,

b) u technických aktiv, která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována

1. vede jejich evidenci,

2. zavede bezpečnostní opatření, která zaručí obdobnou nebo vyšší úroveň bezpečnosti, a

3. omezí jejich komunikaci v komunikační síti na nezbytně nutnou,

c) provádí pravidelné skenování zranitelností relevantních technických aktiv a aplikuje přiměřená bezpečnostní opatření na základě zjištěných výsledků.

§ 13

Kryptografické algoritmy

(1) Povinná osoba při zajištění bezpečnosti technických aktiv a jejich komunikace

a) používá aktuálně odolné kryptografické algoritmy,

b) prosazuje bezpečné nakládání s kryptografickými algoritmy a

c) zohledňuje doporučení a metodiky v oblasti kryptografických algoritmů vydané Národním úřadem pro kybernetickou a informační bezpečnost.

(2) Povinná osoba zajišťuje bezpečnou

a) hlasovou, audiovizuální a textovou komunikaci, a to včetně e-mailové komunikace, a

b) nouzovou komunikaci v rámci organizace.

ČÁST TŘETÍ

STANOVENÍ VÝZNAMNOSTI DOPADU KYBERNETICKÉHO BEZPEČNOSTNÍHO INCIDENTU

§ 14

(1) Povinná osoba pro potřeby vyhodnocení významnosti dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby stanoví

a) únosnou míru újmy způsobené kybernetickým bezpečnostním incidentem, v jehož důsledku ještě není ohrožen život nebo zdraví osob nebo schopnost povinné osoby dostát svým závazkům,

b) oblasti pro posouzení významnosti dopadu kybernetických bezpečnostních incidentů zohledňující zejména

1. provozní dopad kybernetického bezpečnostního incidentu na povinnou osobu a její schopnost poskytovat regulovanou službu,
2. množství uživatelů regulované služby a jiných orgánů a osob zasažených kybernetickým bezpečnostním incidentem,
3. časové, lidské a technické zdroje, které jsou potřebné k obnově poskytování zasažené regulované služby,
4. typ a umístění aktiv dotčených kybernetickým bezpečnostním incidentem,
5. citlivost informací a dat zasažených kybernetickým bezpečnostním incidentem a újmu, jakou může narušení bezpečnosti těchto informací a dat způsobit povinné osobě nebo jinému orgánu nebo osobě, a
6. přímou příčinu kybernetického bezpečnostního incidentu, je-li povinné osobě známo, zda se jedná o lidskou chybu, technickou závadu nebo úmyslné jednání.

(2) Dopad kybernetického bezpečnostního incidentu na poskytování regulované služby je považován za významný, pokud

a) přesáhne povinnou osobou stanovenou únosnou míru újmy způsobenou kybernetickým bezpečnostním incidentem podle odstavce 1 písm. a) a současně

b) je oblast pro posouzení významnosti dopadu podle odstavce 1 písm. b) posouzena jako významná.

ČÁST ČTVRTÁ

ÚČINNOST

§ 15

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. listopadu 2025.

Ředitel:
Ing. Kintr v. r.

Příloha č. 1

Přehled bezpečnostních opatření

Tato příloha představuje přehled bezpečnostních opatření ve formě tabulky (Tab. č. 1), která má povinné osobě sloužit jako nástroj k vyhodnocení účinnosti zavedených bezpečnostních opatření za stanovené období.

Tab. č. 1: Přehled bezpečnostních opatření

Vyhodnocení účinnosti zajišťování kybernetické bezpečnosti					
Bezpečnostní opatření podle vyhlášky	**Stav bezpečnostního opatření**	**Popis bezpečnostního opatření**	**Termín zavedení bezpečnostního opatření**	**Priorita zavedení bezpečnostního opatření**	**Odpovědnost za bezpečnostní opatření**

Přehled bezpečnostních opatření je složen ze šesti sloupců, kdy specifika jednotlivých sloupců a příklady jejich vyplnění jsou uvedeny v tabulkách níže (Tab. č. 2 až 7). V Tabulce č. 3 „Stav bezpečnostního opatření“ jsou místo příkladů uvedeny „Přípustné hodnoty“.

Tab. č. 2: Bezpečnostní opatření podle vyhlášky

Název sloupce v Tab. č. 1	Bezpečnostní opatření podle vyhlášky.
Popis sloupce	Příslušné bezpečnostní opatření požadované vyhláškou uvedené například formou odkazu na dotčené ustanovení vyhlášky.
Popis hodnot	Uvedené hodnoty musí odkazovat na konkrétní ustanovení právního předpisu, přičemž je doporučeno, aby byly jednotlivé části uvedeny v logické návaznosti.

Tab. č. 3: Stav bezpečnostního opatření

Název sloupce v Tab. č. 1	Stav bezpečnostního opatření.
Popis sloupce	Popis stavu bezpečnostního opatření ve chvíli, kdy je provedeno vyhodnocení účinnosti zajišťování kybernetické bezpečnosti.
Popis hodnot	Tento sloupec bude obsahovat právě jednu z přípustných hodnot „Zavedeno“, „V procesu“ nebo „Nezavedeno“. Hodnotu „Zavedeno“ lze zapsat v případě, kdy bylo bezpečnostní opatření v hodnoceném období zavedeno v požadovaném rozsahu. Hodnotu „V procesu“ lze zapsat v případě, kdy je bezpečnostní opatření (nebo jeho část) v hodnoceném období zaváděno, popřípadě jsou činěny doložitelné kroky k jeho zavedení (například výběrové řízení, smlouva, testovací provoz atd.) Hodnotu „Nezavedeno“ lze zapsat pouze v případě, kdy opatření zavedeno nebylo.

Tab. č. 4: Popis bezpečnostního opatření

Název sloupce v Tab. č. 1	Popis bezpečnostního opatření.
Popis sloupce	Stručný popis zavedení bezpečnostního opatření v návaznosti na stav, v jakém se aktuálně nachází, a s přihlédnutím k prostředí povinné osoby.
Popis hodnot	Popis jednotlivých bezpečnostních opatření by měl stručně reflektovat situaci u povinné osoby (například podle názvů příslušných částí bezpečnostní dokumentace) a stav bezpečnostního opatření podle Tab. č. 2. V případě bezpečnostních opatření, která jsou označena jako „V procesu“ je nutné popsat prozatímní stav, případně uvést odkaz na dokumentaci, která proces zavádění dokládá. Pokud je bezpečnostní opatření označeno jako „Nezavedeno“, je nutné odůvodnit, proč zavedeno nebylo.

Tab. č. 5: Termín zavedení bezpečnostního opatření

Název sloupce v Tab. č. 1	Termín zavedení bezpečnostního opatření.
Popis sloupce	Plánovaný termín zavedení bezpečnostního opatření v plném rozsahu.
Popis hodnot	Tato hodnota bude vyplněna pouze v případě, je-li stav bezpečnostního opatření označen jako „V procesu“ nebo „Nezavedeno“, ale jeho zavedení je v budoucnu plánováno nebo závisí na dalších okolnostech. Měla by být uvedena buď konkrétním datem nebo kvartálem či měsícem konkrétního roku.

Tab. č. 6: Priorita zavedení bezpečnostního opatření

Název sloupce v Tab. č. 1	Priorita zavedení bezpečnostního opatření.
Popis sloupce	Prioritizace zavádění bezpečnostních opatření s ohledem na dopad na poskytování regulované služby.
Popis hodnot	Hodnotu „nízká“ nebo „1“ je možné zapsat v případě, kdy by absence zavedení bezpečnostního opatření neměla dopad na poskytování regulované služby nebo dané bezpečnostní opatření není pro poskytování regulované služby relevantní. Hodnotu „střední“ nebo „2“ je možné zapsat v případě, kdy by absence zavedení bezpečnostního opatření měla minimální a krátkodobý dopad na poskytování regulované služby. Hodnotu „vysoká“ nebo „3“ je možné zapsat v případě, kdy by absence zavedení bezpečnostního opatření měla za následek vážný a dlouhodobý dopad na poskytování regulované služby. Hodnotu „kritická“ nebo „4“ je možné zapsat v případě, kdy by absence zavedení bezpečnostního opatření měla okamžité a nevratné důsledky pro poskytování regulované služby nebo jsou známy úspěšné pokusy o překonání bezpečnostních opatření.

Tab. č. 7: Odpovědnost za bezpečnostní opatření

Název sloupce v Tab. č. 1	Odpovědnost za bezpečnostní opatření.
Popis sloupce	Osoba pověřená za zavedení daného bezpečnostního opatření.
Popis hodnot	Je nutné zaznamenat údaje tak, aby bylo možné jednoznačně určit osobu pověřenou za zavedení bezpečnostního opatření. V případě potřeby je možné uvést také konkrétní organizační složku, do níž daná osoba spadá.

Příloha č. 2

Požadavky na smluvní ujednání s dodavateli

Povinná osoba uzavírá pouze takové smlouvy, které stanoví způsoby realizace bezpečnostních opatření a určují obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.

Povinné osoby mohou uzavírat jen takové smlouvy, které budou zohledňovat následující relevantní ustanovení:

a) ustanovení o bezpečnosti informací z pohledu důvěrnosti (včetně ustanovení o mlčenlivosti), integrity a dostupnosti,
b) ustanovení o auditu dodavatele související s plněním smlouvy,
c) ustanovení o řetězení dodavatelů,
d) ustanovení upravující tzv. exit strategii, podmínky ukončení smluvního vztahu z pohledu bezpečnosti informací,
e) ustanovení o sankcích za porušení smluvních povinností,
f) ustanovení o oprávnění užívat data,
g) ustanovení o autorství programového kódu, případně o programových licencích,
h) ustanovení o důvěrnosti smluvního vztahu,
i) ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele (nebo odsouhlasení pro dodavatelský vztah relevantních částí bezpečnostních politik) povinnou osobou,
j) ustanovení o řízení změn,
k) ustanovení o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,
l) ustanovení upravující zajištění řízení kontinuity činností,
m) náležitosti smlouvy o úrovni služeb (SLA) a způsobu a úrovni realizace bezpečnostních opatření,
n) ustanovení o dodržování pravidel bezpečného vývoje.

Povinná osoba může požadovat při uzavírání smluv s dodavateli i další ujednání zohledňující specifické požadavky plynoucí ze zajištění provozních a bezpečnostních potřeb souvisejících s regulovanou službou, která nejsou uvedena v této příloze.

Příloha č. 3

Témata pro rozvoj bezpečnostního povědomí

a) Techniky zabezpečení zařízení.
b) Firewall, antivirový program a jejich omezení.
c) Škodlivé programy a jejich projevy.
d) Rizika stahování programů a aplikací.
e) Aktualizace software.
f) Rizika povolení a zakázání spouštění maker.
g) Rizika spustitelných souborů.
h) Zásady zabezpečení uživatelských účtů.
i) Používání, tvorba a správa hesel.
j) Vícefaktorová autentizace.
k) Techniky sociálního inženýrství.
l) On-line identita, digitální stopa a její minimalizace.
m) Zásady práce v počítačové síti.
n) Používání vzdáleného připojení (VPN).
o) Bezpečná elektronická komunikace.
p) Bezpečnost webových stránek.
q) Zálohování, ukládání a šifrování dat.
r) Bezpečné používání přenosných technických nosičů dat.
s) Využívání služeb cloud computingu.
t) Pravidla a postupy pro oznamování neobvyklého chování technických aktiv a podezření na jakékoliv zranitelnosti.
u) Základní postup při reakci na kybernetickou bezpečnostní událost nebo kybernetický bezpečnostní incident.
v) Zásady bezpečného používání pracovních zařízení pro soukromé účely.
w) Zásady bezpečného používání soukromých zařízení pro pracovní účely (tzv. BYOD).
x) Osobní odpovědnost zaměstnance při dodržování zásad kybernetické bezpečnosti.
y) Aktuální hrozby v kybernetické bezpečnosti.

[1]) Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 20/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).

ISSN 3029-5092

Vydavatel: Ministerstvo vnitra, Nad Štolou 3, poštovní schránka 21, 170 34 Praha 7 • **Redakce Sbírky zákonů a mezinárodních smluv**: Ministerstvo vnitra, nám. Hrdinů 1634/3, poštovní schránka 155/SB, 140 21, Praha 4, telefon: 974 817 289, e-mail: sbirka@mvcr.cz • Sazba: Tiskárna Ministerstva vnitra, Bartůňkova 1159/4, poštovní schránka 10, 149 00 Praha 11-Chodov • **Právně závazná elektronická verze Sbírky zákonů a mezinárodních smluv je k dispozici na www.e-sbirka.cz** • Tištěnou verzi částky Sbírky zákonů a mezinárodních smluv lze objednat u Tiskárny Ministerstva vnitra, telefon: 974 887 312, e-mail: info@tmv.cz, www.tmv.cz • Předplatné je od 1. 1. 2024 ukončeno.